

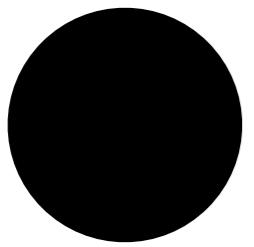
# Constructive Galois Connections

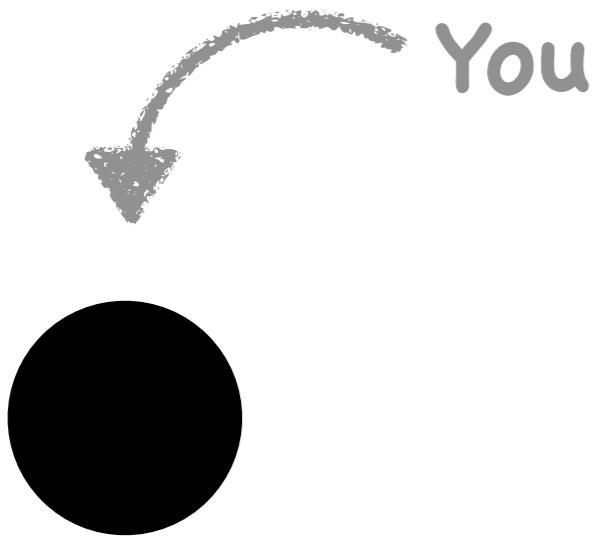
**David Daraïs**

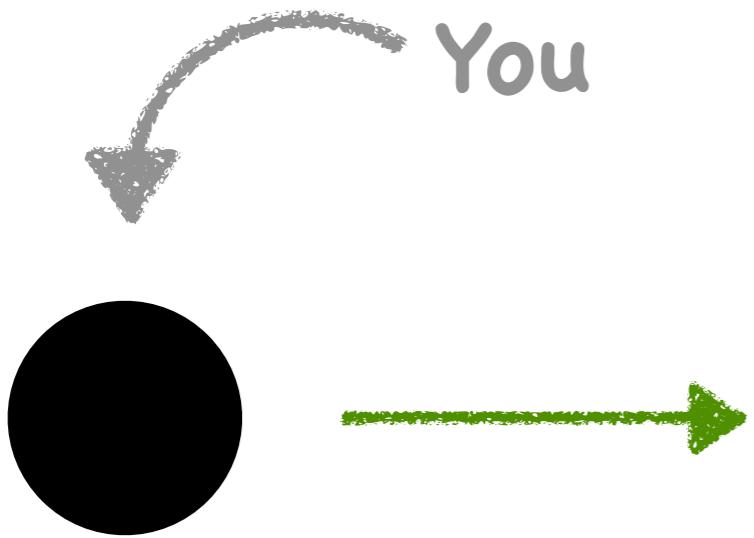
University of Maryland

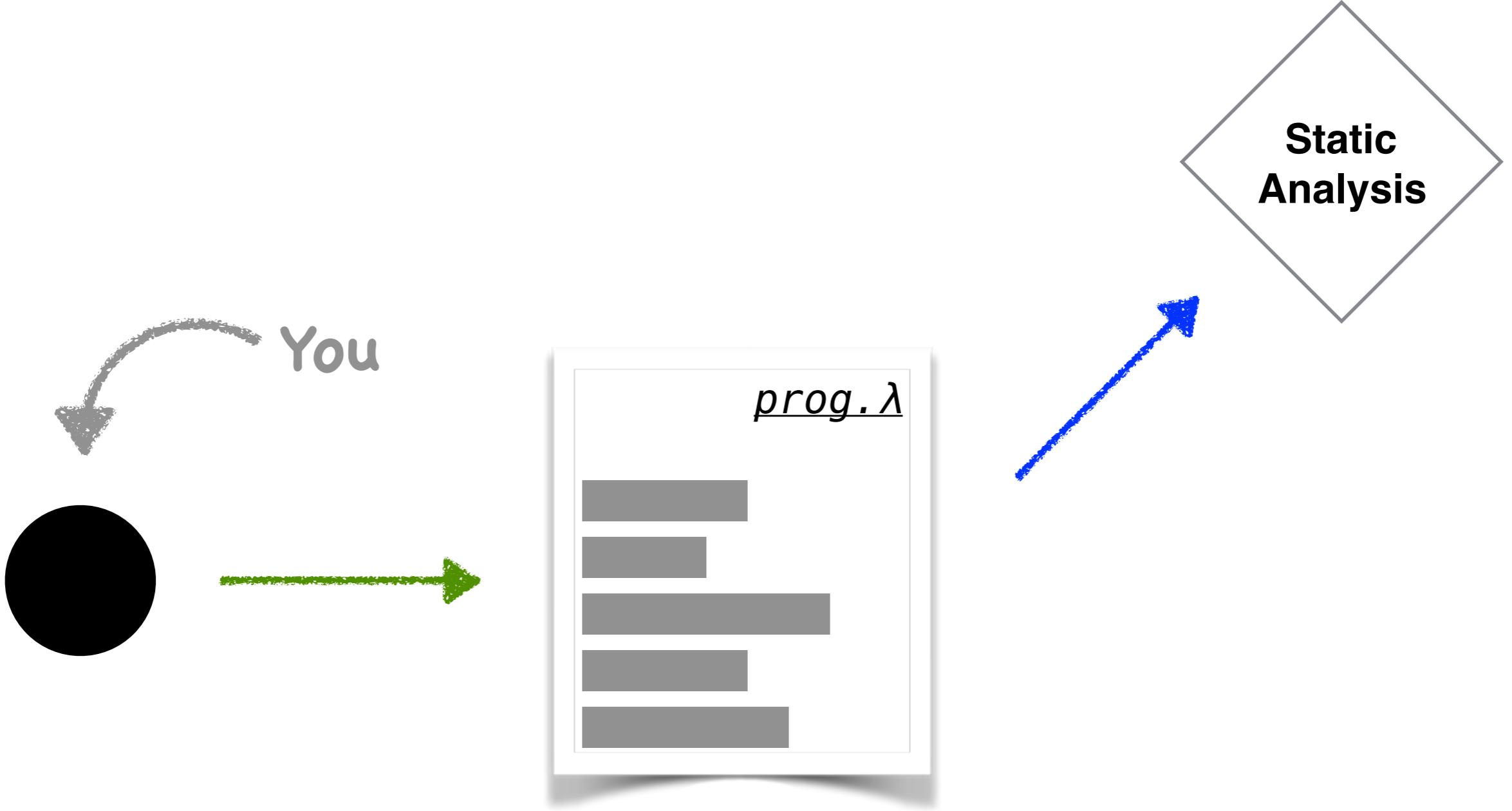
David Van Horn

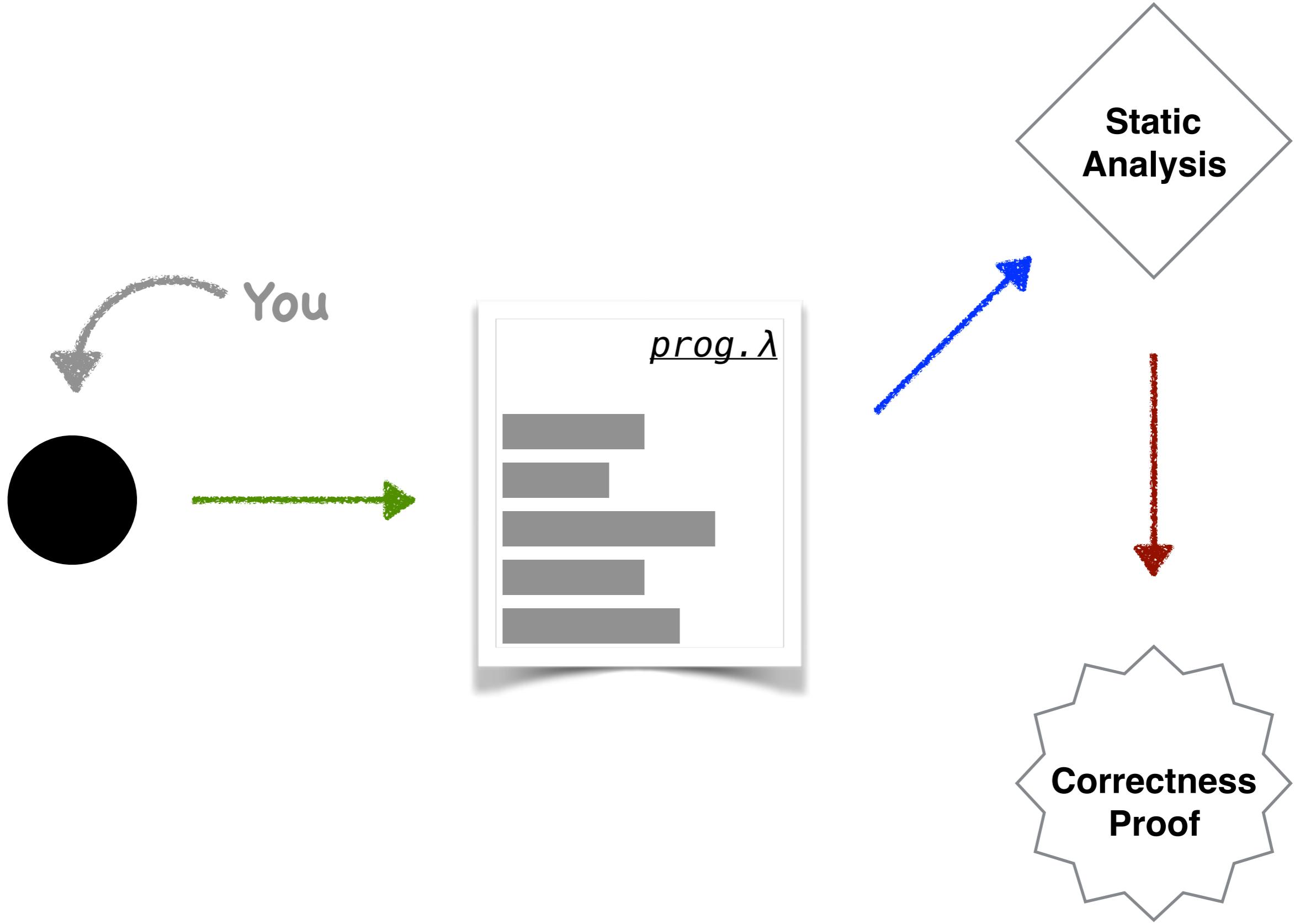
University of Maryland

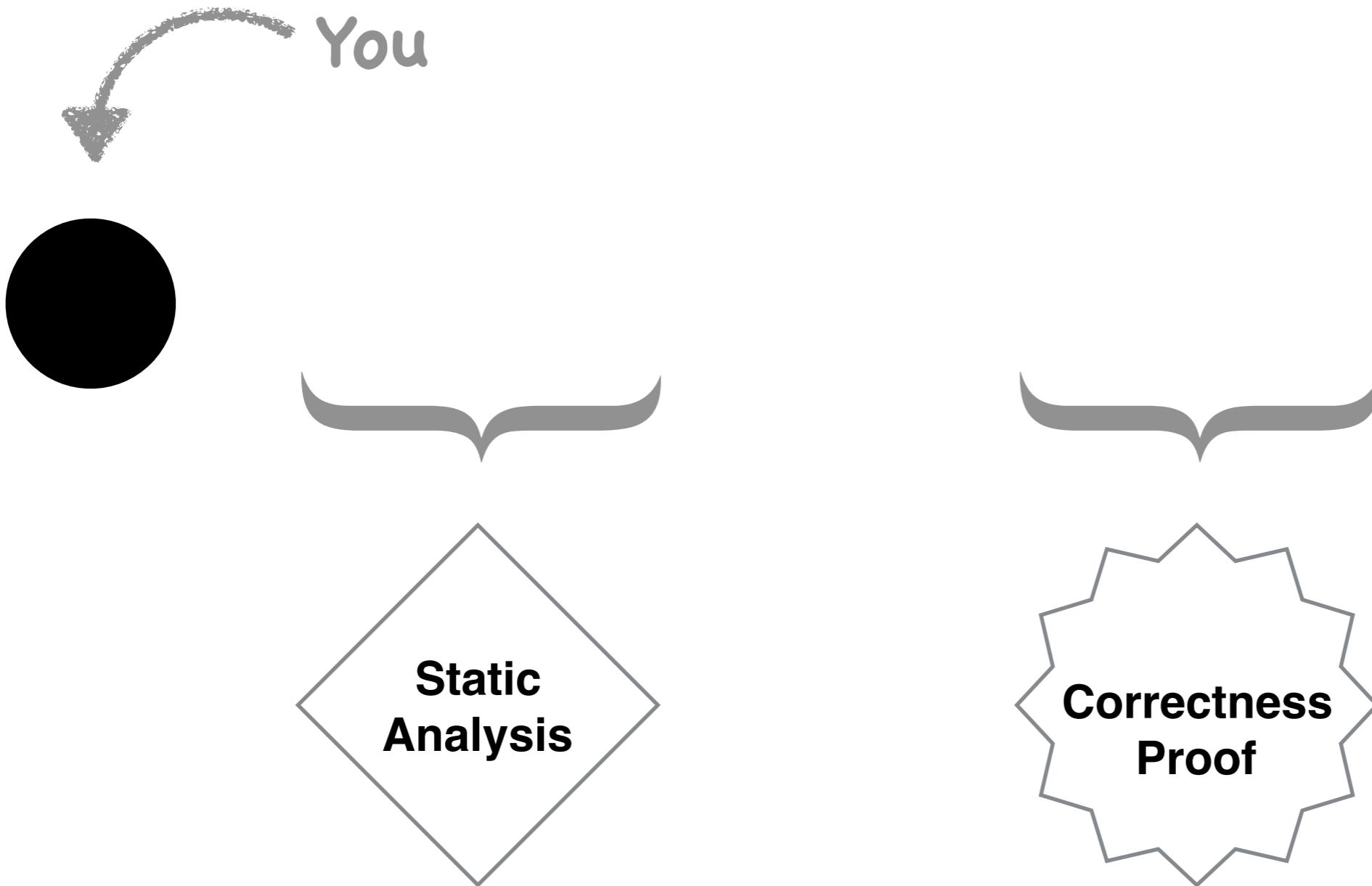


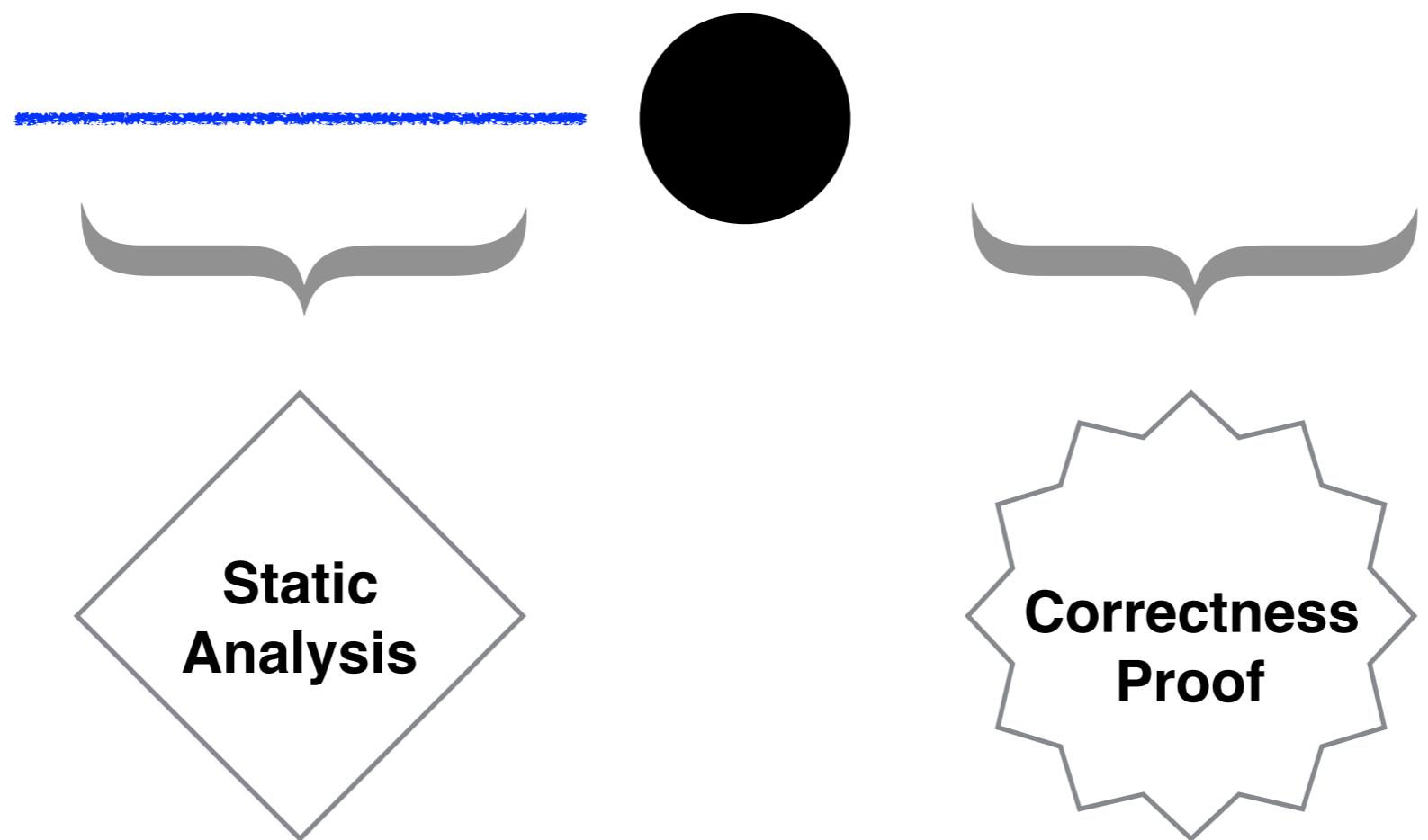


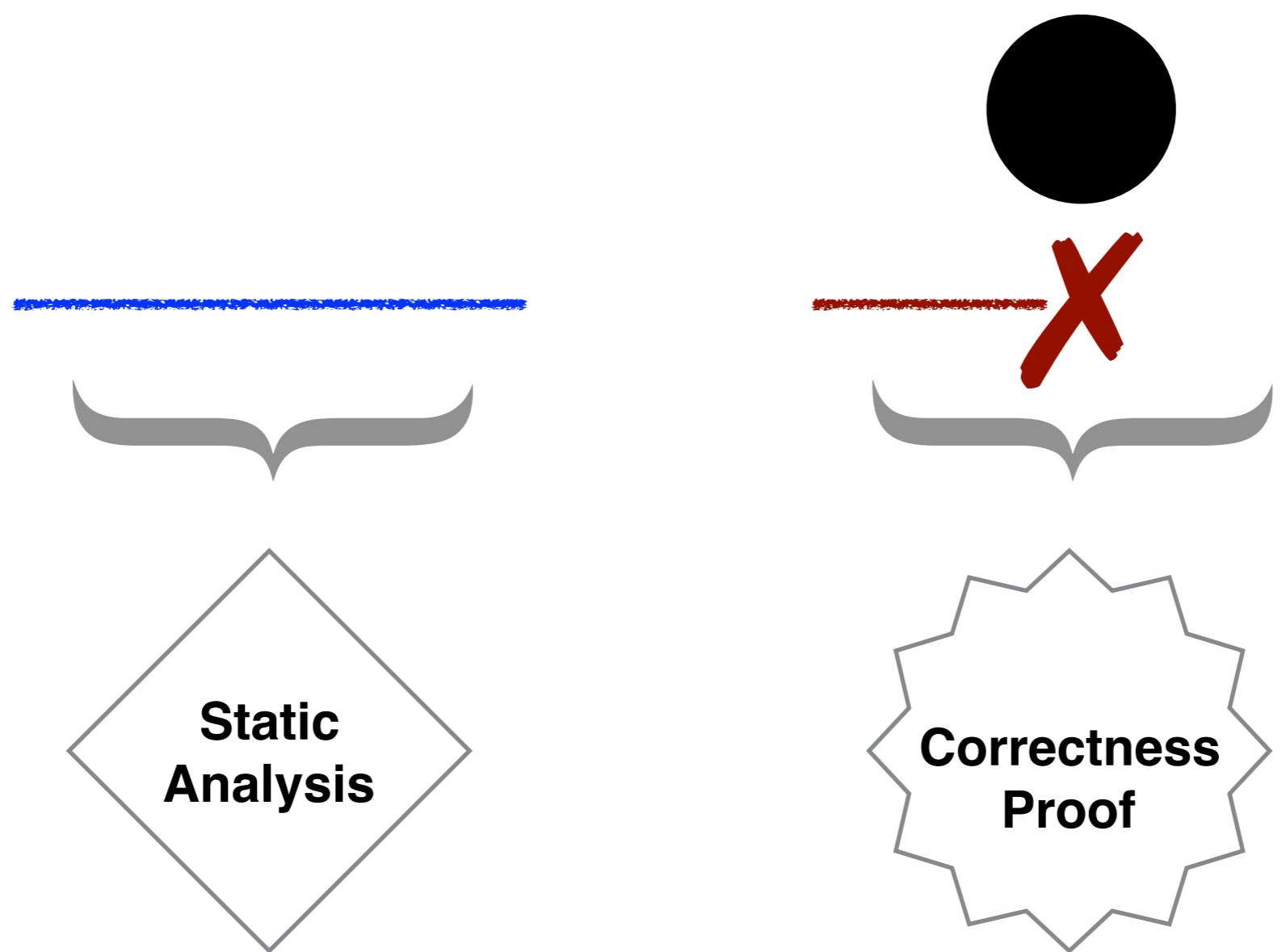


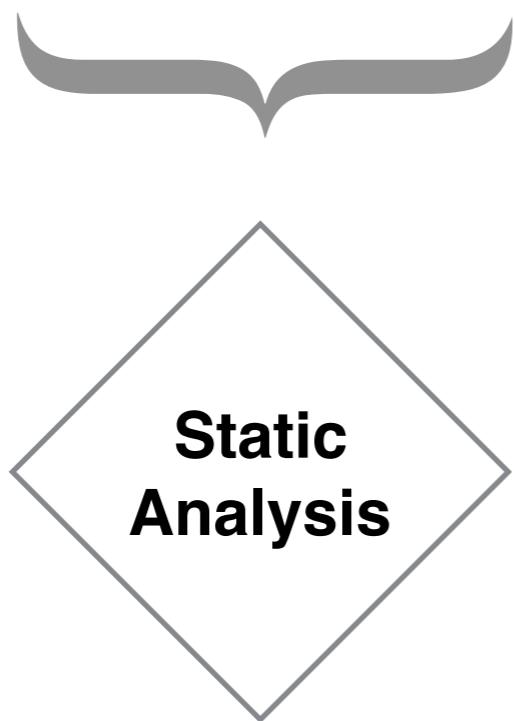
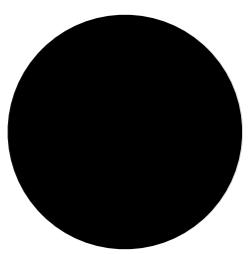




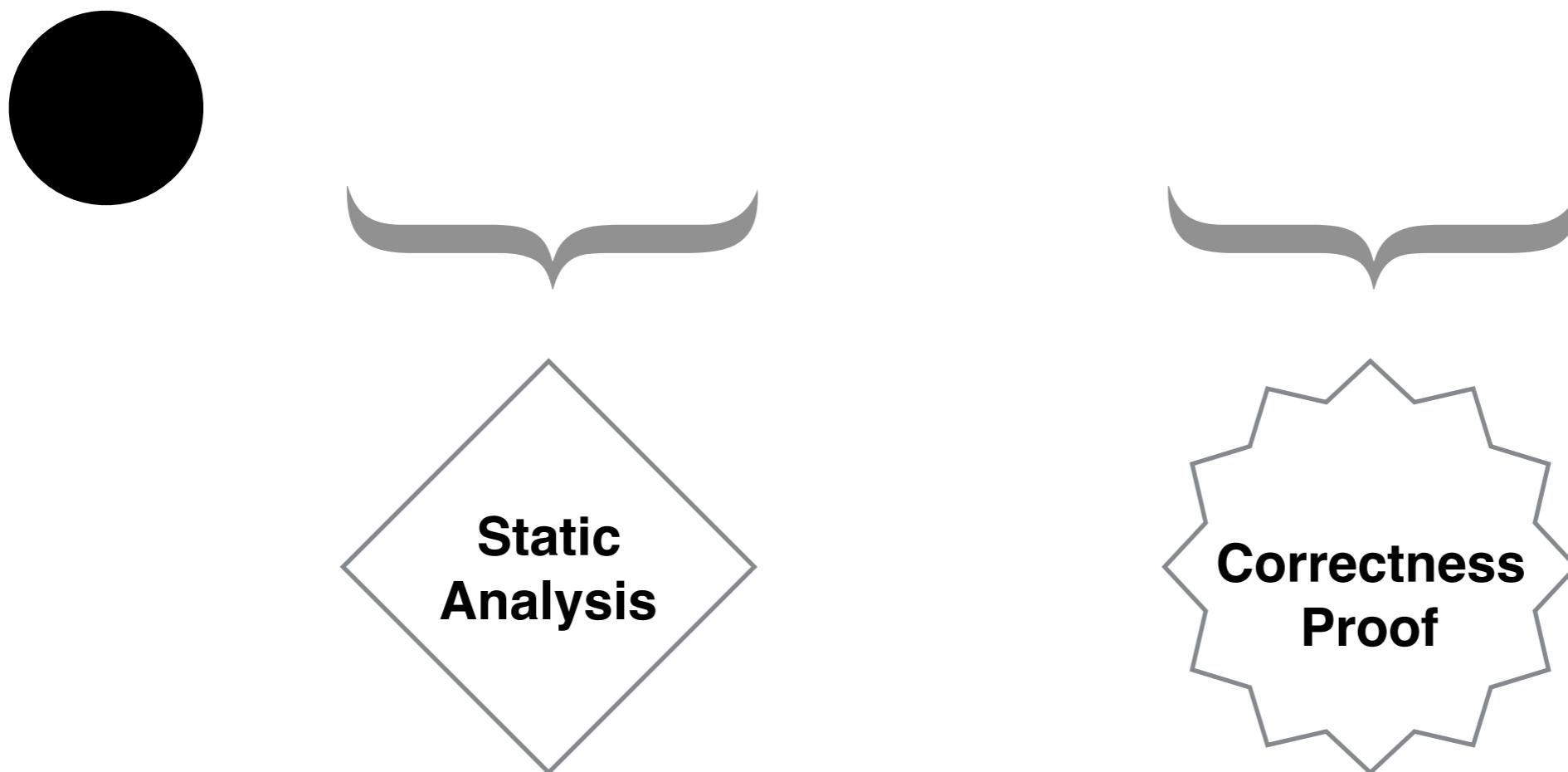




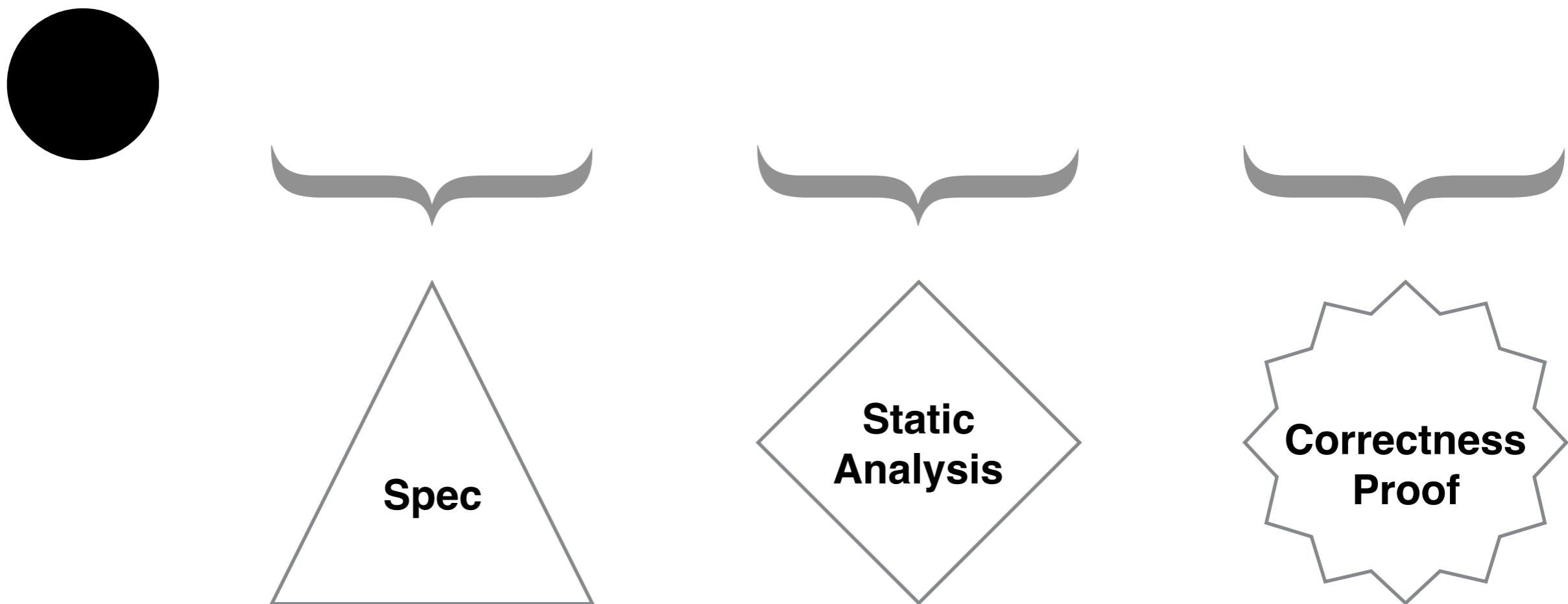




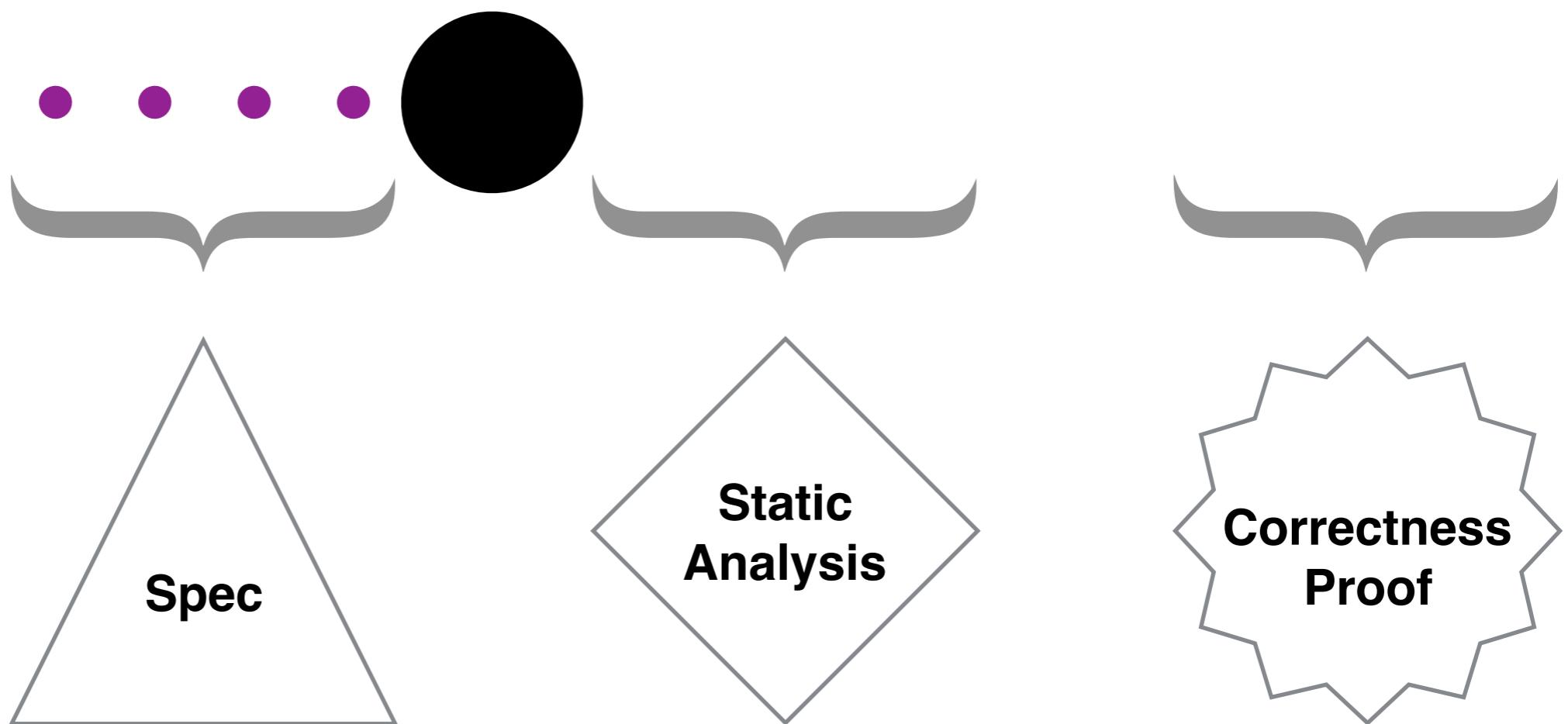
# Abstract Interpretation



# Abstract Interpretation

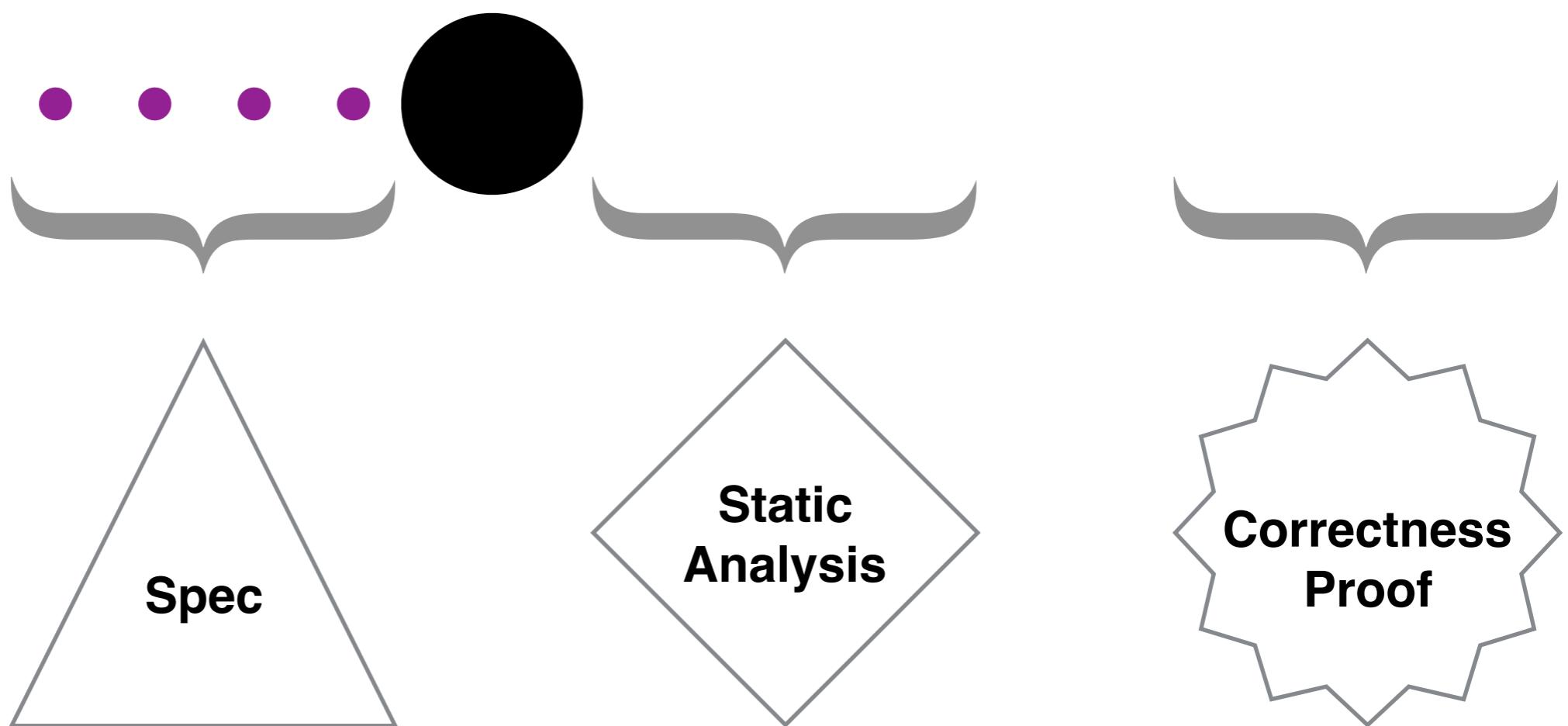


# Abstract Interpretation



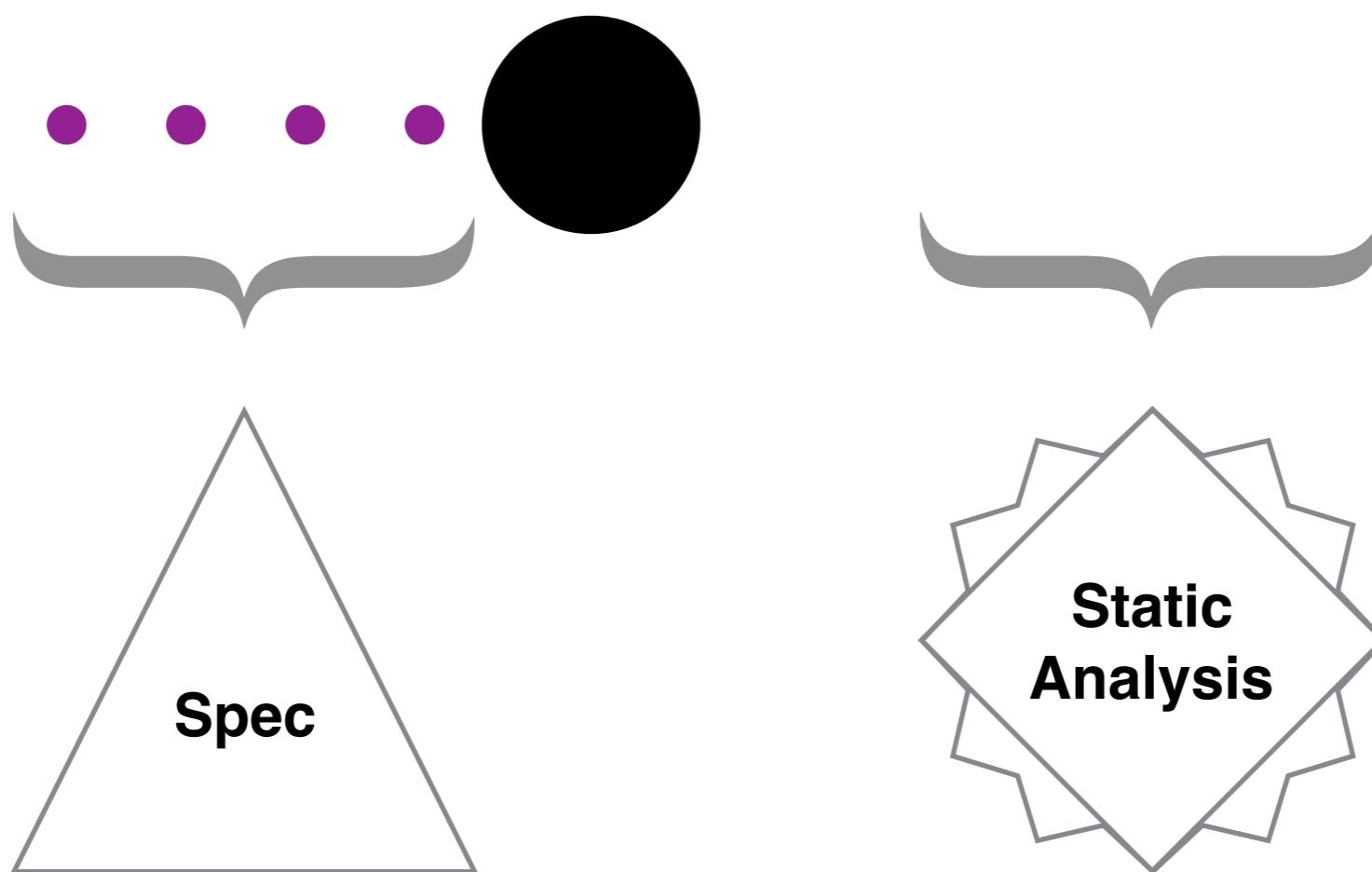
Abstract  
Interpretation

Calculational  
Design



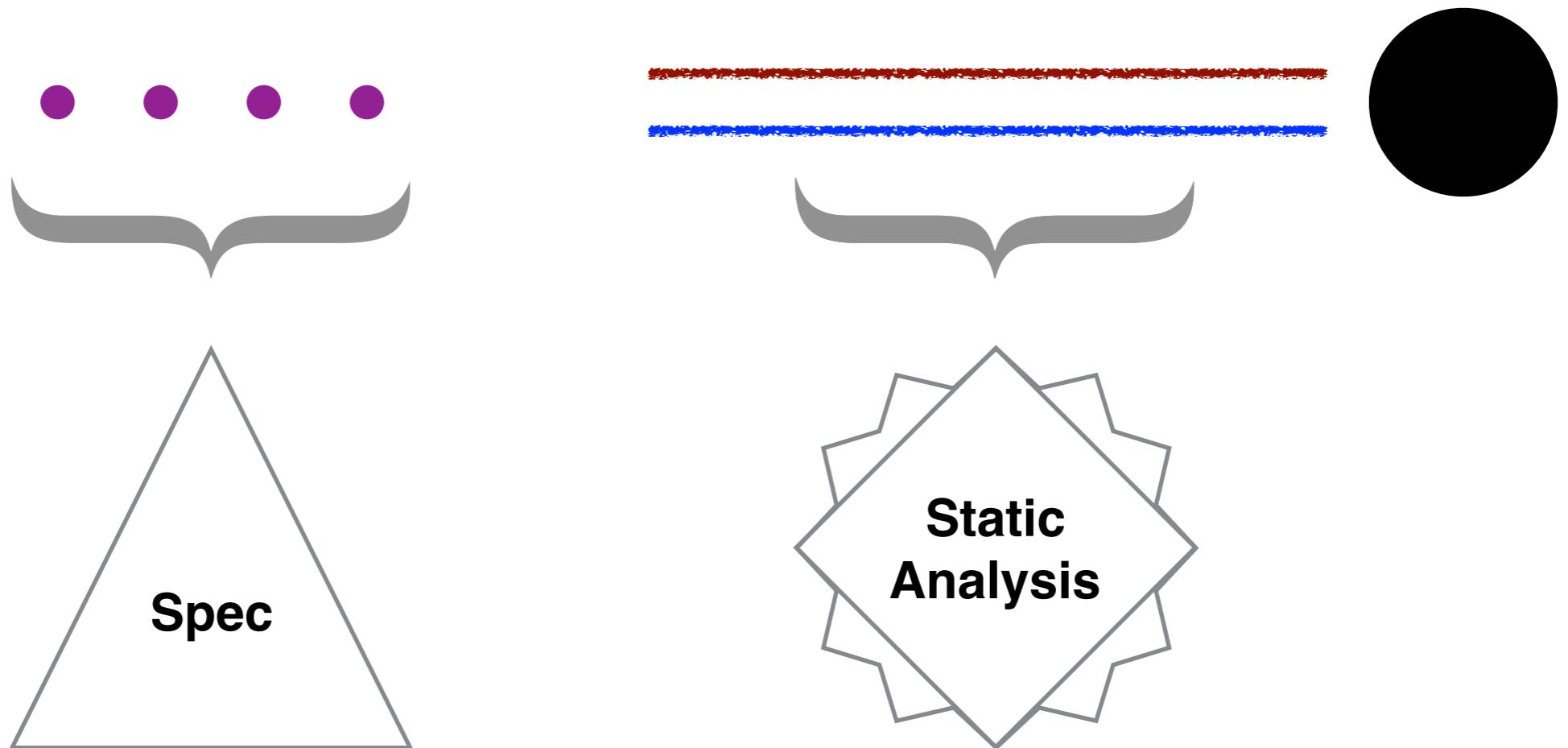
Abstract  
Interpretation

Calculational  
Design



Abstract  
Interpretation

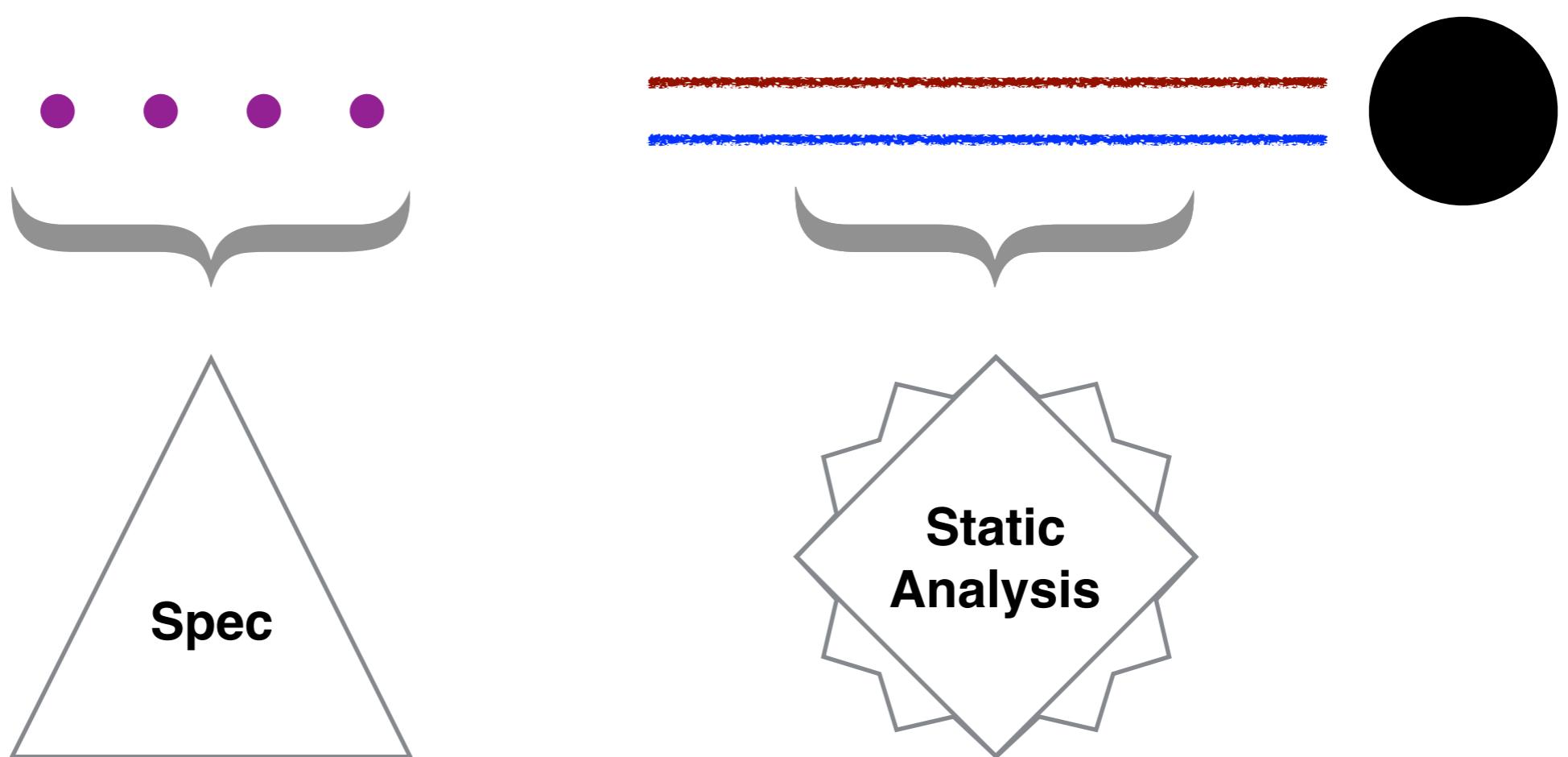
Calculational  
Design



Abstract  
Interpretation

Calculational  
Design

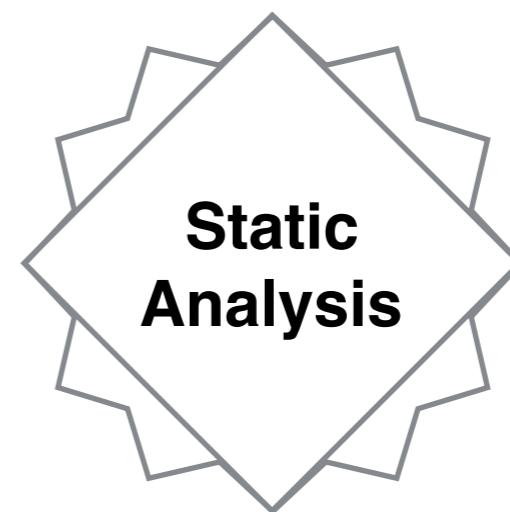
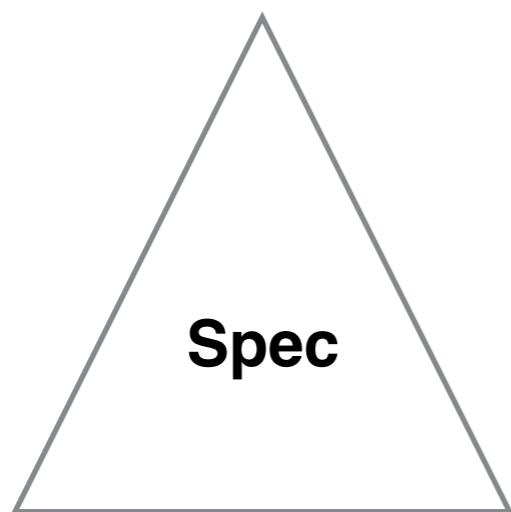
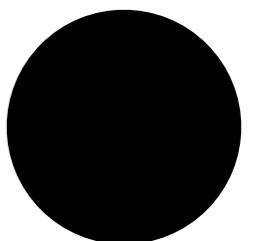
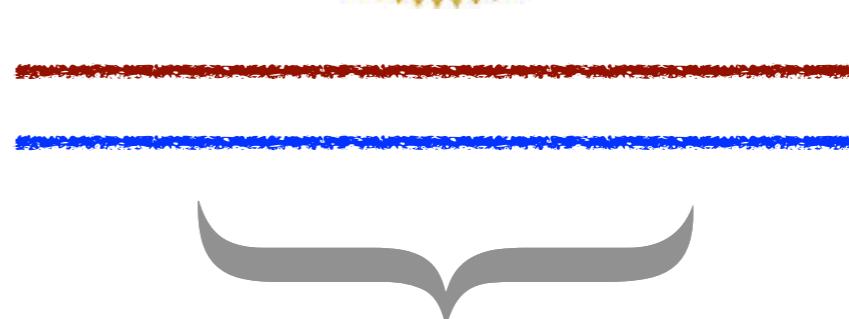
Proof  
Assistants



Abstract  
Interpretation

Calculational  
Design

Proof  
Assistants



# The Dream

*Abstract  
Interpreters*



Synthesized from spec

Correct by construction

Certified Implementation

# The Calculational Design of a Generic Abstract Interpreter

Patrick COUSOT

*LIENS, Département de Mathématiques et Informatique  
École Normale Supérieure, 45 rue d'Ulm, 75230 Paris cedex 05, France*

**Abstract.** We present in extenso the calculation-based development of a generic compositional reachability static analyzer for a simple imperative programming language by abstract interpretation of its formal rule-based/structured small-step operational semantics.

## Contents

<b>1. Introduction</b>	<b>3</b>
<b>2. Definitions</b>	<b>4</b>
<b>3. Values</b>	<b>5</b>
3.1 Machine integers . . . . .	5
3.2 Errors . . . . .	5
<b>4. Properties of Values</b>	<b>5</b>
<b>5. Abstract Properties of Values</b>	<b>6</b>
5.1 Galois connection based abstraction . . . . .	6
5.2 Componentwise abstraction of sets of pairs . . . . .	7
5.3 Initialization and simple sign abstraction . . . . .	7
5.4 Initialization and interval abstraction . . . . .	8
5.5 Algebra of abstract properties of values . . . . .	9
<b>6. Environments</b>	<b>10</b>
6.1 Concrete environments . . . . .	10
6.2 Properties of concrete environments . . . . .	10
6.3 Nonrelational abstraction of environment properties . . . . .	10
6.4 Algebra of abstract environments . . . . .	12
<b>7. Semantics of Arithmetic Expressions</b>	<b>13</b>
7.1 Abstract syntax of arithmetic expressions . . . . .	13
7.2 Machine arithmetics . . . . .	13
7.3 Operational semantics of arithmetic expressions . . . . .	13
7.4 Forward collecting semantics of arithmetic expressions . . . . .	14
7.5 Backward collecting semantics of arithmetic expressions . . . . .	14
<b>8. Abstract Interpretation of Arithmetic Expressions</b>	<b>15</b>
8.1 Lifting Galois connections at higher-order . . . . .	15

The emphasis in these notes [has been the]  
correctness of the design **by calculus**.

The **mechanized verification** [of this technique]  
can be foreseen with **automatic extraction** of a  
**correct program** from its **correctness proof**.

*–Patrick Cousot [Monograph 1999]*

N° d'ordre: 3262

## THÈSE

présentée

**devant l'Université de Rennes 1**

pour obtenir

le grade de : DOCTEUR DE L'UNIVERSITÉ DE RENNES 1  
Mention INFORMATIQUE

par

David PICARDIE

Équipe d'accueil : Lande (Irisa,Rennes)  
École Doctorale : Matisse  
Composante universitaire : IFSIC

Titre de la thèse :

*Interprétation abstraite en logique intuitionniste :  
extraction d'analyseurs Java certifiés*

Soutenue le 6 décembre 2005 devant la commission d'examen

M. :	Jean-Pierre	Banâtre	Président
M. :	Patrick	Cousot	Rapporteurs
M. :	Xavier	Leroy	
Mme. :	Christine	Paulin-Mohring	Examinateurs
M. :	David	Schmidt	
M. :	Thomas	Jensen	Directeurs
M. :	David	Cachera	

[Our] framework [loses] an important property of the standard framework: **the ability to derive a correct approximation from [its specification]**.

Several examples of such derivations are given by Cousot. **It seems interesting to find a framework for [deriving approximations], while remaining easily formalizable in Coq.**

*–David Pichardie [PhD Thesis 2005]*

```
...  
if (b) {x = 10} else {x = 20}  
...
```

```
...  
if (b) {x = 10} else {x = 20}  
...
```

$$x \in [10, 20]$$

```
...  
if (b) {x = 10} else {x = 20}  
...
```

$\wp(\mathbb{Z})$

$\mathbb{Z} \times \mathbb{Z}$

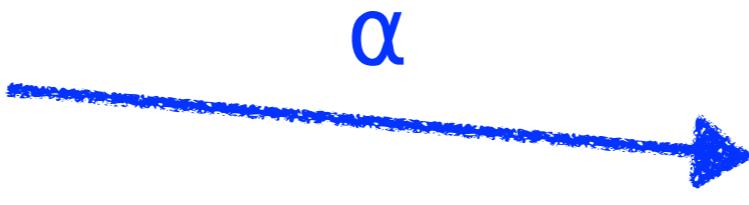
$x \in [10, 20]$

```
...  
if (b) {x = 10} else {x = 20}  
...
```

$\wp(\mathbb{Z})$

$\mathbb{Z} \times \mathbb{Z}$

$x \in \{10, 20\}$



$x \in [10, 20]$

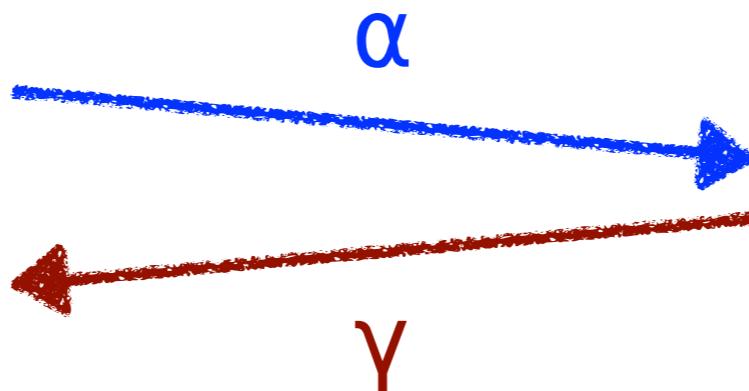
```
...  
if (b) {x = 10} else {x = 20}  
...
```

$\wp(\mathbb{Z})$

$\mathbb{Z} \times \mathbb{Z}$

$x \in \{10, 20\}$

$x \in \{10, \dots, 20\}$



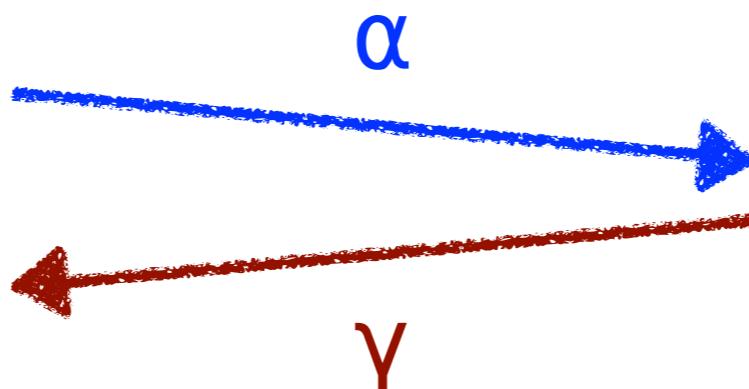
$x \in [10, 20]$

```
...  
if (b) {x = 10} else {x = 20}  
...
```

$\wp(\mathbb{Z})$

$\mathbb{Z} \times \mathbb{Z}$

$x \in \{10, 20\}$   
 $x \in \{10, \dots, 20\}$



$x \in [10, 20]$

*Uncomputable*

*Computable*

$\wp(\mathbb{Z})$  $\mathbb{Z} \times \mathbb{Z}$ 

*Classical  
Reasoning*



*Program  
Extraction*

### calculate.cousot

```
 $\alpha(\text{eval}[n])(\rho^\#)$ 
l defn of  $\alpha$  
=  $\alpha^I(\text{eval}[n](\gamma^R(\rho^\#)))$ 
l defn of eval[n] 
=  $\alpha^I(\{i \mid \rho \vdash n \mapsto i\})$ 
l defn of  $\_\vdash\_\mapsto\_\$  
=  $\alpha^I(\{i\})$ 
l defn of eval#[n] 
 $\triangleq \text{eval}^\#[n](\rho^\#)$ 
```

### calculate.cousot

```
α(eval[n])(ρ#)
l defn of α §
= αI(eval[n](γR(ρ#)))
l defn of eval[n] §
= αI({i | ρ ⊢ n ↣ i})
l defn of _⊤_ ↣ _ §
= αI({i})
l defn of eval#[n] §
△ eval#[n](ρ#)
```

### calculate.agda

```
▷ ⟨ α[ ⇌R ↞ ⇌I ] · eval[ Num n ] · ρ# ⟩
▷ ⟨ (αI * · (eval[ Num n ] * · (γR · ρ#)) ) ⟩
▷ [focus-right [·] of αI * ]
    l defn[eval[ Num n ]] §
▷ ⟨ αI * · (return · n) ⟩
▷ l right-unit[*] §
▷ ⟨ pure · eval#[ Num n ] · ρ# ⟩
```

# Four Stories

- |                         |             |
|-------------------------|-------------|
| Direct Verification     | x calculate |
| Abstract Interpretation | x mechanize |

# Four Stories

Direct Verification	$\times$ calculate
Abstract Interpretation	$\times$ mechanize
Kleisli GCs	$\checkmark$ calculate $\frac{1}{2}$ mechanize
Constructive GCs	$\checkmark$ calculate $\checkmark$ mechanize

# Direct Verification

# Direct Verification

**succ** :  $\mathbb{N} \rightarrow \mathbb{N}$

# Direct Verification

$\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$        $P = \{\mathsf{E}, 0\}$

# Direct Verification

$\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$

$P := \{E, 0\}$

$\text{succ}^\# : P \rightarrow P$

$\text{succ}^\#(E) = 0$

$\text{succ}^\#(0) = E$

# Direct Verification

$\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$

$P = \{E, 0\}$

$\text{succ}^\# : P \rightarrow P$

$\text{succ}^\#(E) = 0$

$\text{succ}^\#(0) = E$

$\llbracket \_ \rrbracket : P \rightarrow \wp(\mathbb{N})$

$\llbracket E \rrbracket = \{ n \mid \text{even}(n) \}$

$\llbracket 0 \rrbracket = \{ n \mid \text{odd}(n) \}$

# Direct Verification

$\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$

$P = \{E, 0\}$

$\text{succ}^\# : P \rightarrow P$

$\text{succ}^\#(E) = 0$

$\text{succ}^\#(0) = E$

$\llbracket \_ \rrbracket : P \rightarrow \wp(\mathbb{N})$

$\llbracket E \rrbracket = \{ n \mid \text{even}(n) \}$

$\llbracket 0 \rrbracket = \{ n \mid \text{odd}(n) \}$

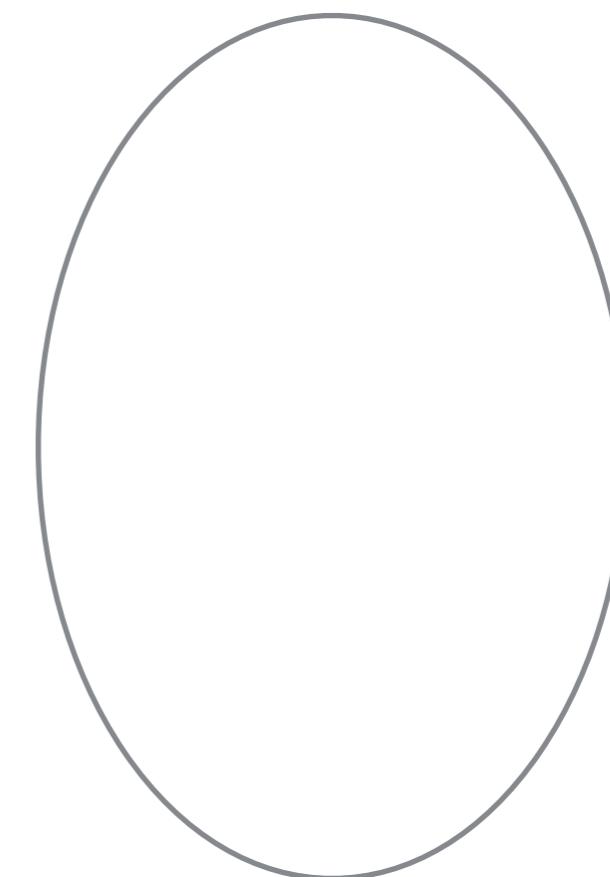
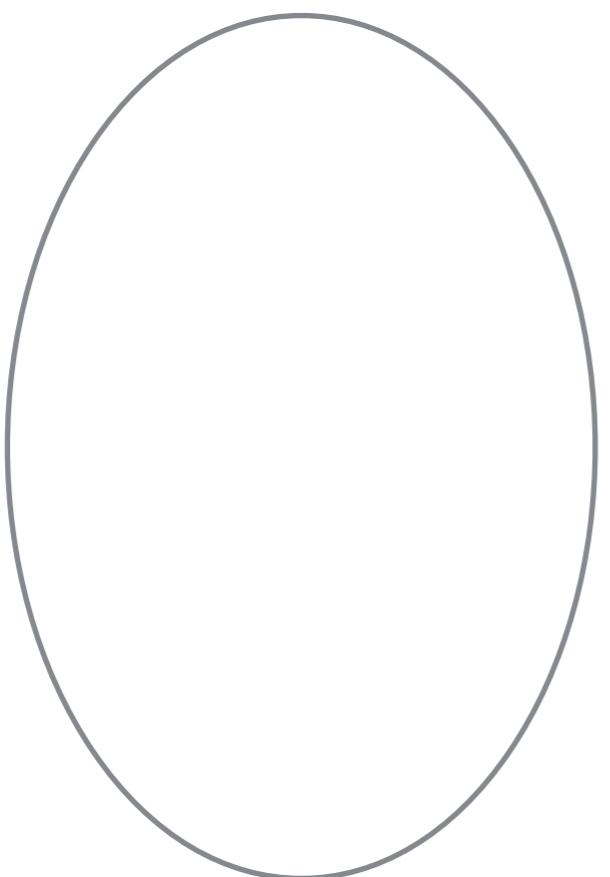
sound :  $n \in \llbracket p \rrbracket \implies \text{succ}(n) \in \llbracket \text{succ}^\#(p) \rrbracket$

# Four Stories

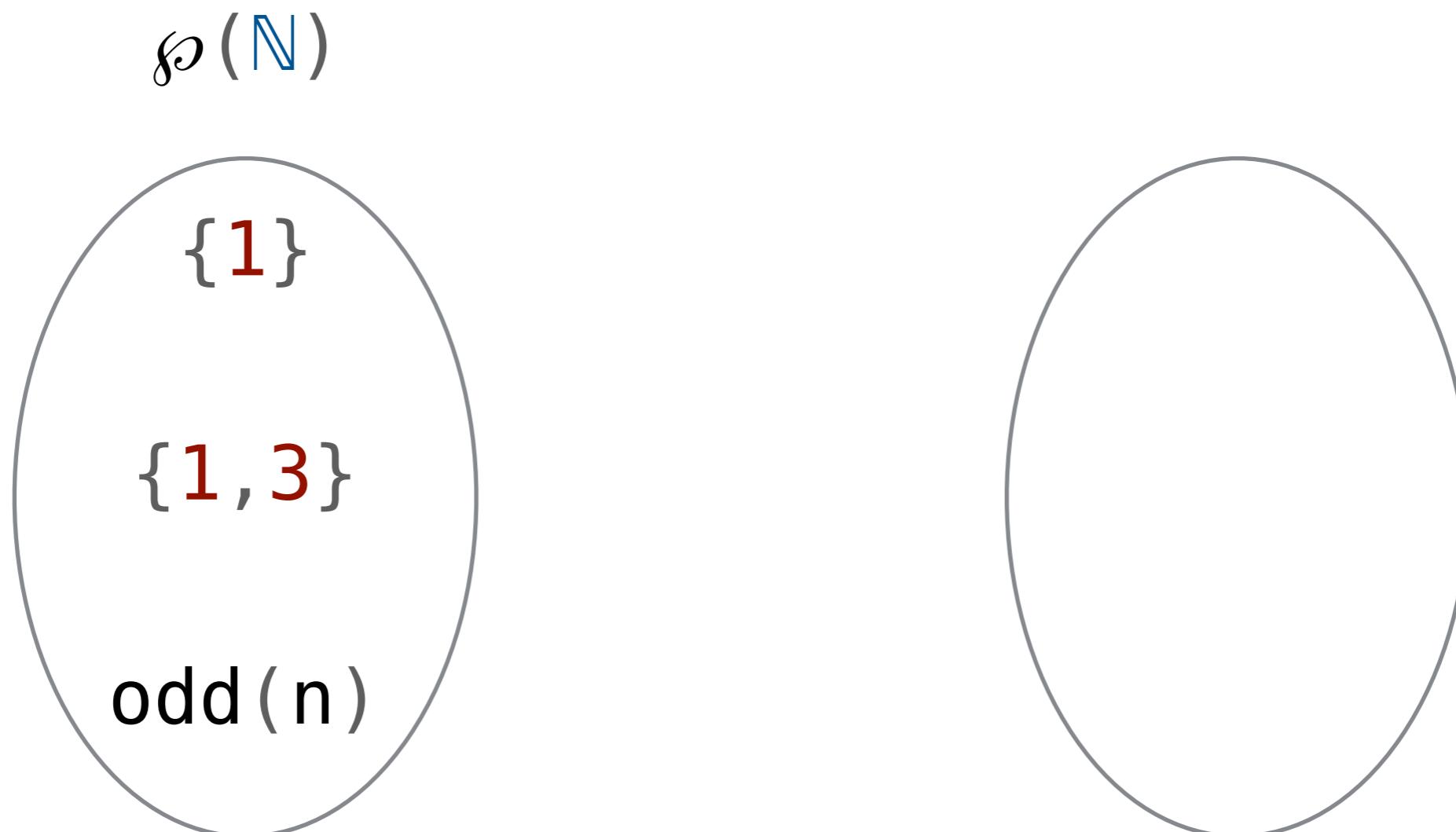
Direct Verification	$\times$ calculate
Abstract Interpretation	$\times$ mechanize
Kleisli GCs	$\checkmark$ calculate $\frac{1}{2}$ mechanize
Constructive GCs	$\checkmark$ calculate $\checkmark$ mechanize

# Abstract Interpretation

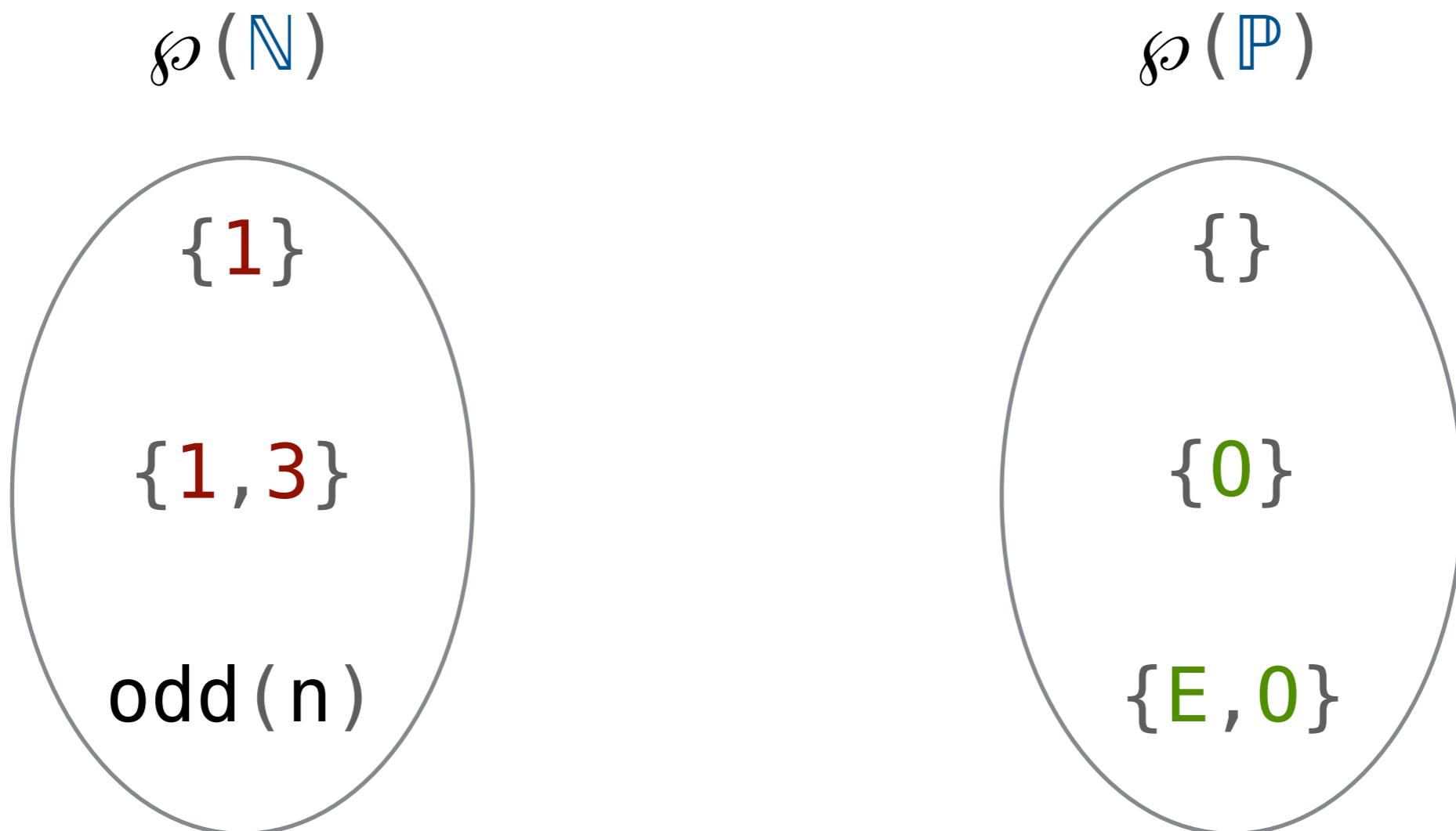
# Abstract Interpretation



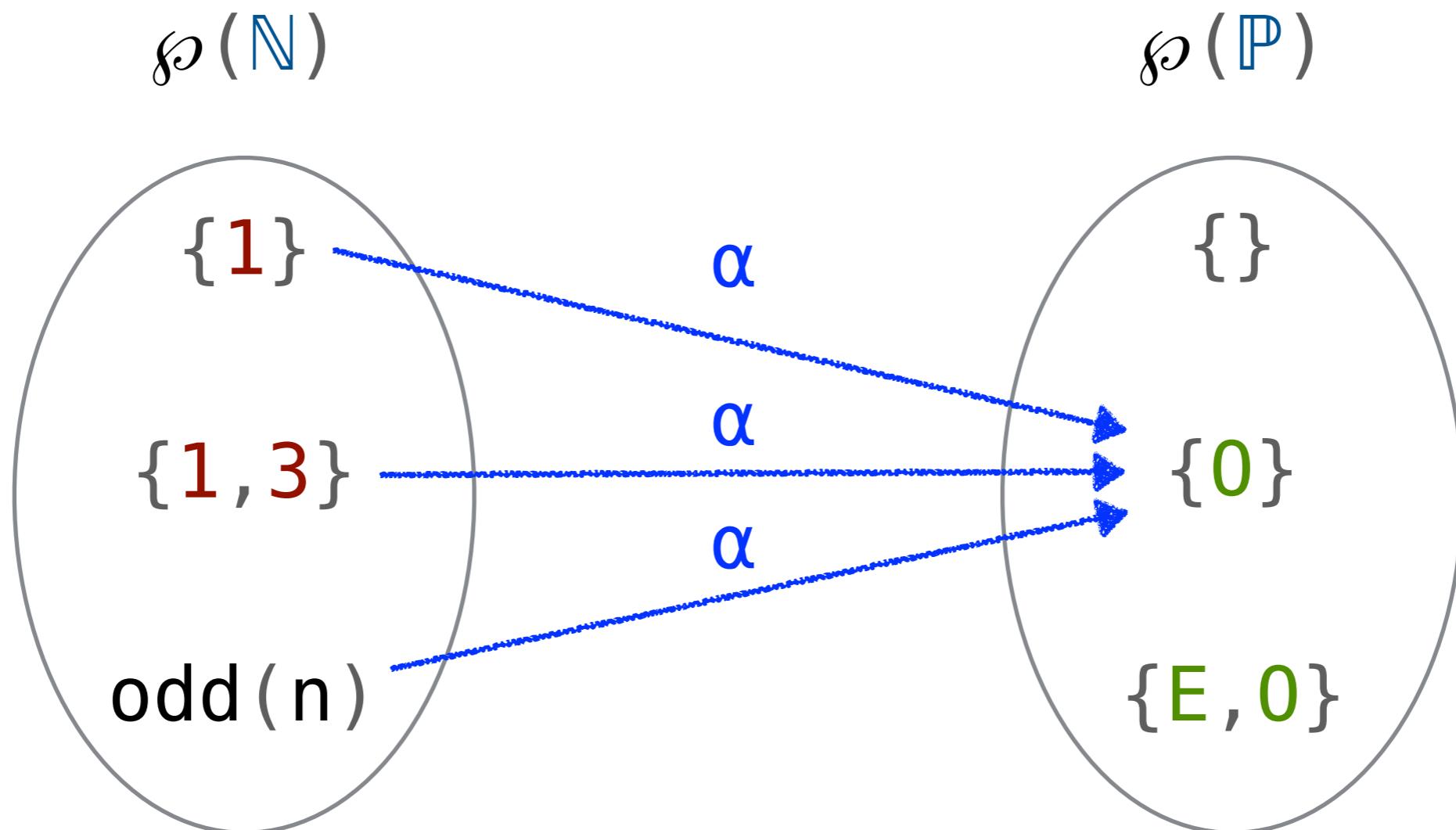
# Abstract Interpretation



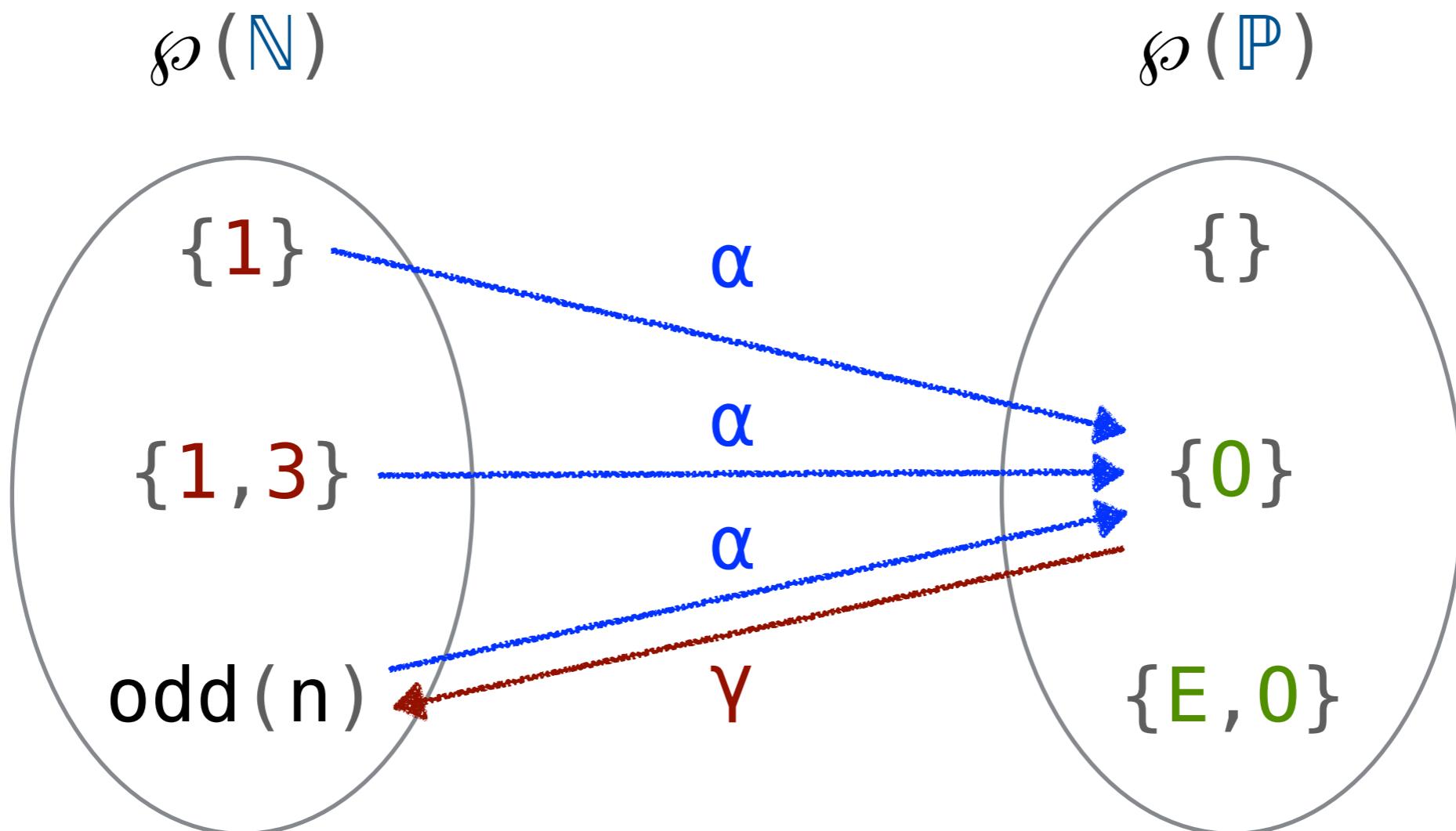
# Abstract Interpretation



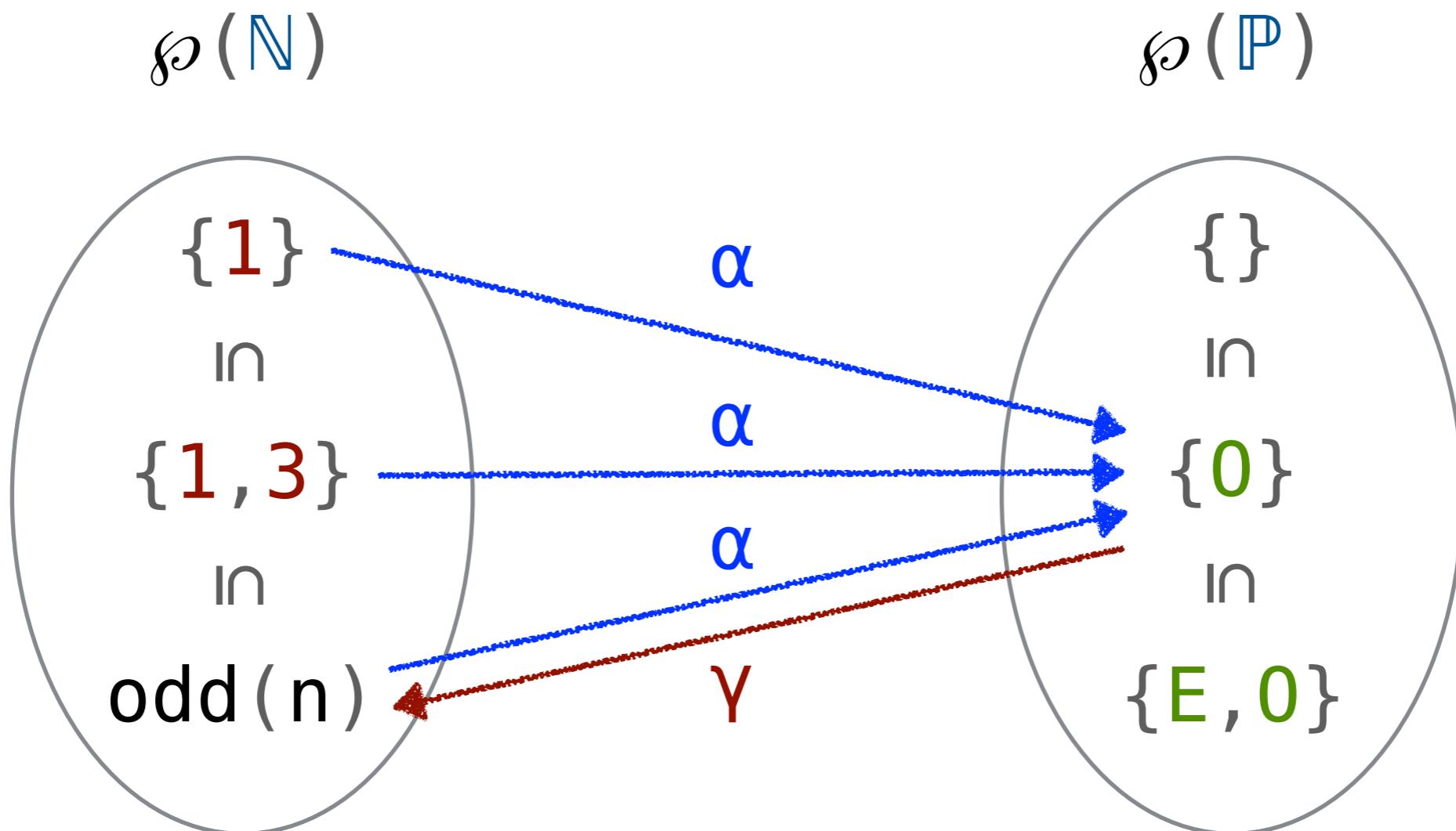
# Abstract Interpretation



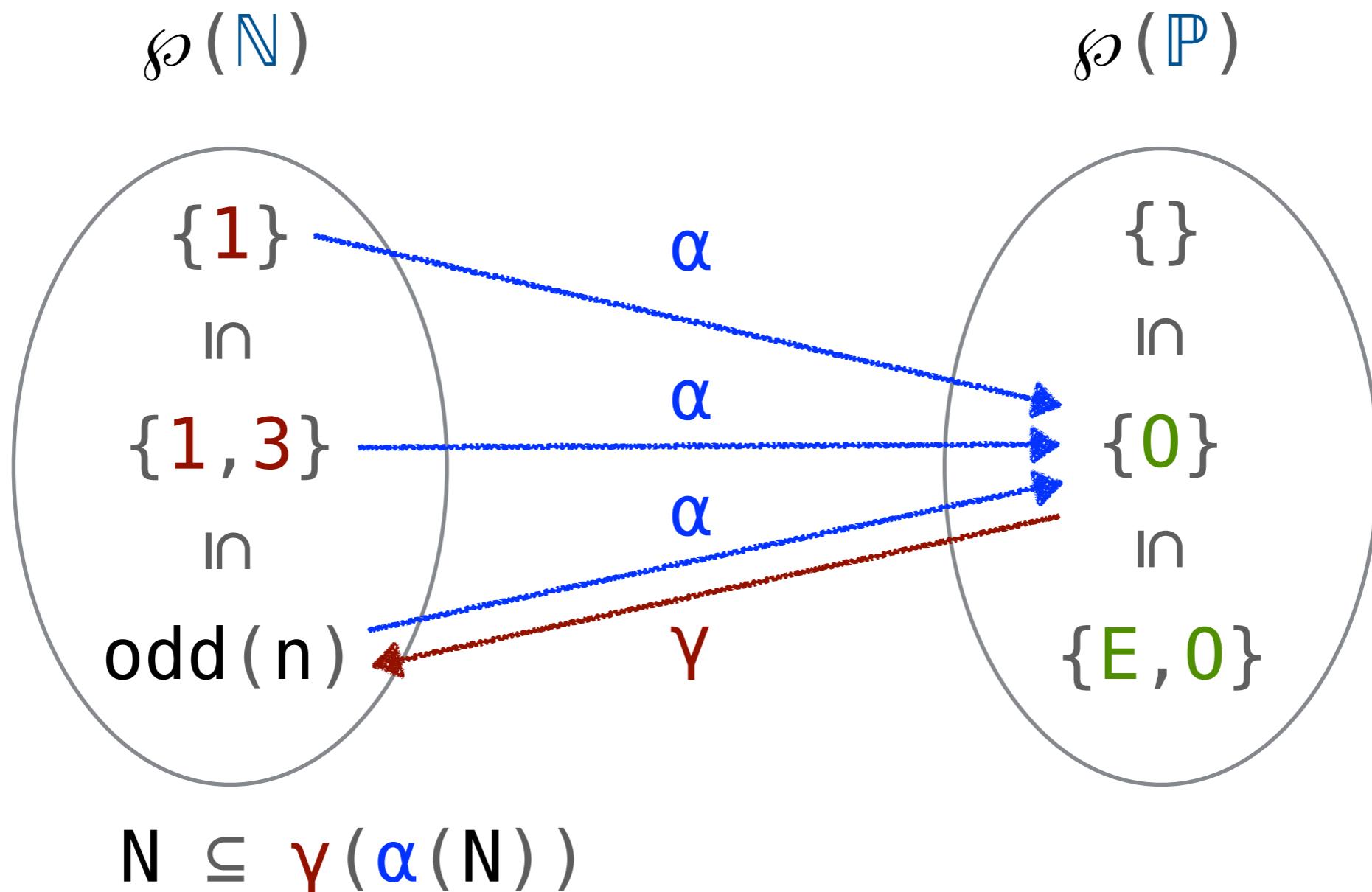
# Abstract Interpretation



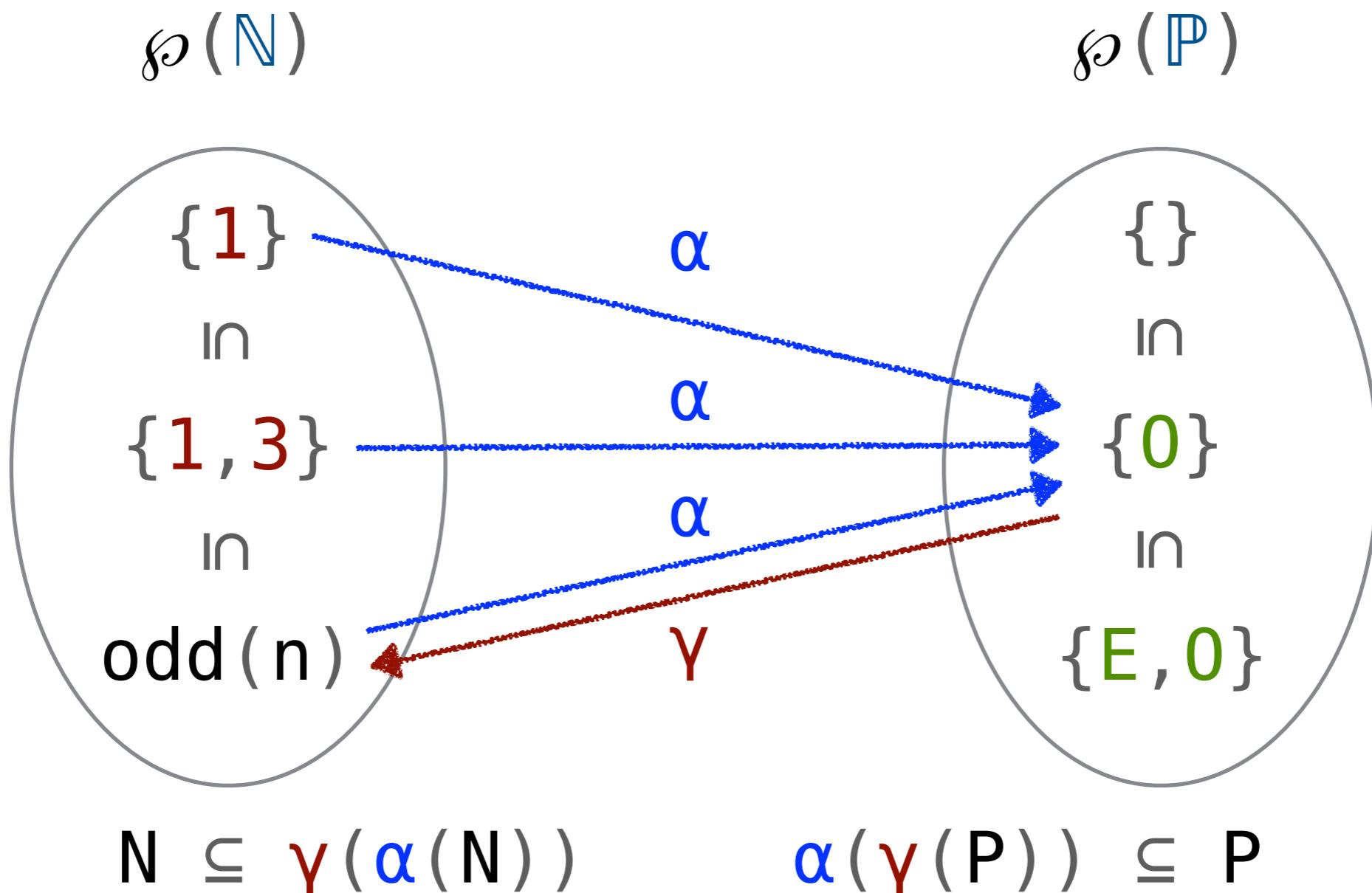
# Abstract Interpretation



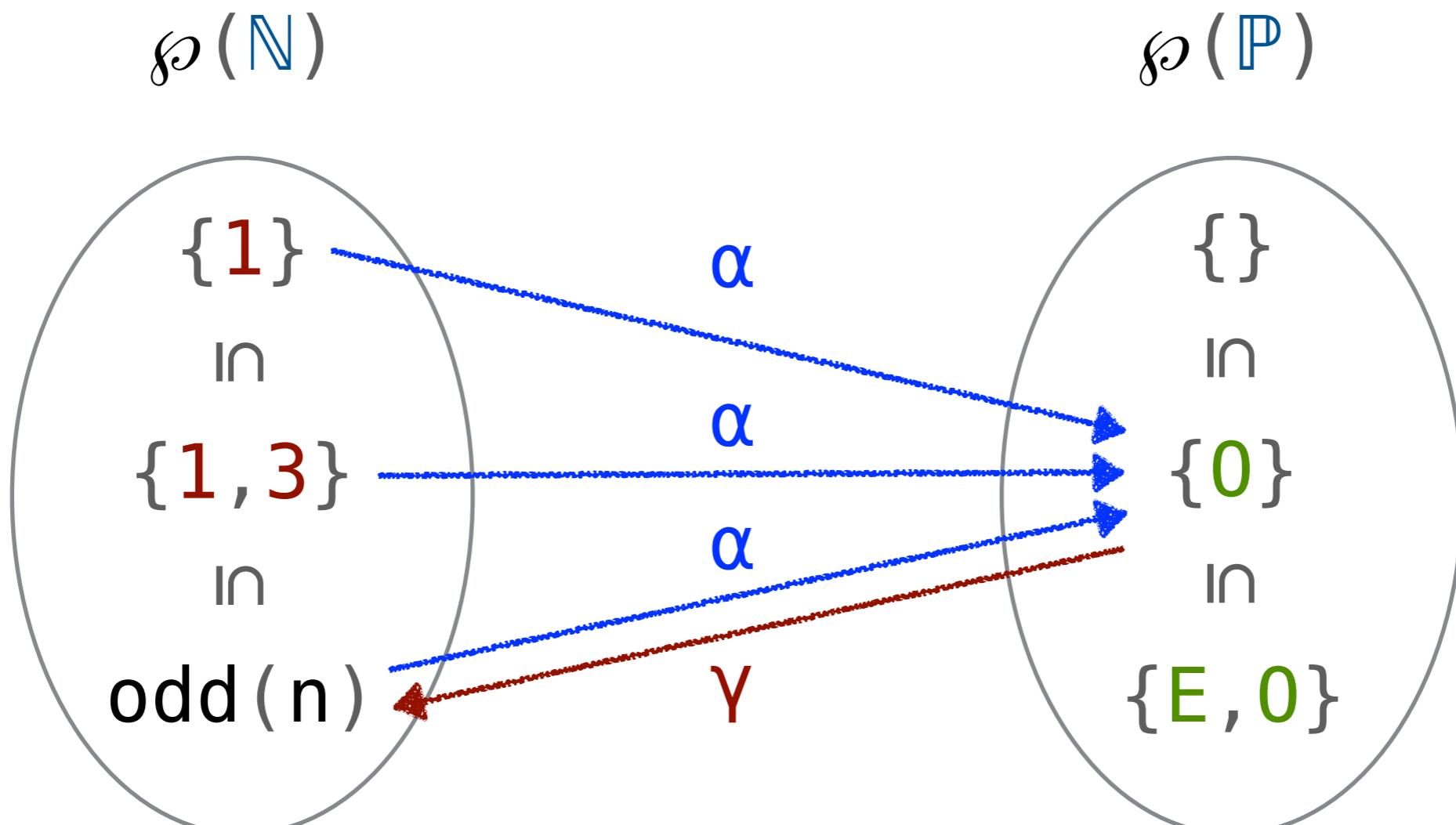
# Abstract Interpretation



# Abstract Interpretation



# Abstract Interpretation



$$N \subseteq \gamma(\alpha(N)) \quad \wedge \quad \alpha(\gamma(P)) \subseteq P$$

---

$$N \subseteq \gamma(P) \iff \alpha(N) \subseteq P$$

# Abstract Interpretation

$$\begin{aligned} N &\in \wp(\mathbb{N}) \\ P &\in \wp(\mathbb{N}) \end{aligned}$$

"P is sound for N"

$$\alpha(N) \subseteq P$$

# Abstract Interpretation

$$N \in \wp(\mathbb{N})$$

$$P \in \wp(\mathbb{N})$$

"P is sound for N"

$$\alpha(N) \subseteq P$$

$$f^N \in \wp(\mathbb{N}) \rightarrow \wp(\mathbb{N})$$

$$f^P \in \wp(\mathbb{P}) \rightarrow \wp(\mathbb{P})$$

" $f^P$  is sound for  $f^N$ "

# Abstract Interpretation

$$N \in \wp(\mathbb{N})$$

$$P \in \wp(\mathbb{N})$$

"P is sound for N"

$$\alpha(N) \subseteq P$$

$$f^N \in \wp(\mathbb{N}) \rightarrow \wp(\mathbb{N})$$

$$f^P \in \wp(\mathbb{P}) \rightarrow \wp(\mathbb{P})$$

"f<sup>P</sup> is sound for f<sup>N</sup>"

$$\vec{\alpha}(f^N) \subseteq f^P$$

# Abstract Interpretation

$$N \in \wp(\mathbb{N})$$

$$P \in \wp(\mathbb{N})$$

"P is sound for N"

$$\alpha(N) \subseteq P$$

$$f^N \in \wp(\mathbb{N}) \rightarrow \wp(\mathbb{N})$$

$$f^P \in \wp(\mathbb{P}) \rightarrow \wp(\mathbb{P})$$

"f<sup>P</sup> is sound for f<sup>N</sup>"

$$\alpha \circ f^N \circ \gamma \subseteq f^P$$

# Abstract Interpretation

$$\begin{aligned}\alpha : \wp(\mathbb{N}) &\rightarrow \wp(\mathbb{P}) \\ \alpha(\mathbb{N}) &= \{\text{parity}(n) \mid n \in \mathbb{N}\}\end{aligned}$$

# Abstract Interpretation

$$\begin{aligned}\alpha : \wp(\mathbb{N}) &\rightarrow \wp(\mathbb{P}) \\ \alpha(\mathbb{N}) &= \{\text{parity}(n) \mid n \in \mathbb{N}\}\end{aligned}$$

$$\begin{aligned}\gamma : \wp(\mathbb{P}) &\rightarrow \wp(\mathbb{N}) \\ \gamma(\mathbb{P}) &= \{n \mid p \in \mathbb{P} \wedge n \in \llbracket p \rrbracket\}\end{aligned}$$

# Abstract Interpretation

$$\begin{aligned}\alpha : \wp(\mathbb{N}) &\rightarrow \wp(\mathbb{P}) \\ \alpha(\mathbb{N}) &= \{\text{parity}(n) \mid n \in \mathbb{N}\}\end{aligned}$$

$$\begin{aligned}\alpha(\mathbb{N}) &\approx \text{map}(\text{parity})(\mathbb{N}) \\ \text{map} : (\mathbb{N} \rightarrow \mathbb{P}) &\rightarrow \wp(\mathbb{N}) \rightarrow \wp(\mathbb{P})\end{aligned}$$

$$\begin{aligned}\gamma : \wp(\mathbb{P}) &\rightarrow \wp(\mathbb{N}) \\ \gamma(\mathbb{P}) &= \{n \mid p \in \mathbb{P} \wedge n \in \llbracket p \rrbracket\}\end{aligned}$$

# Abstract Interpretation

$$\alpha : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{P})$$

$$\alpha(\mathbb{N}) = \{\text{parity}(n) \mid n \in \mathbb{N}\}$$

$$\alpha(\mathbb{N}) \approx \text{map}(\text{parity})(\mathbb{N})$$

$$\text{map} : (\mathbb{N} \rightarrow \mathbb{P}) \rightarrow \wp(\mathbb{N}) \rightarrow \wp(\mathbb{P})$$

$$\gamma : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{N})$$

$$\gamma(P) = \{n \mid p \in P \wedge n \in \llbracket p \rrbracket\}$$

$$\gamma(P) \approx P^*$$

$$\underline{*} : (\mathbb{P} \rightarrow \wp(\mathbb{N})) \rightarrow \wp(\mathbb{P}) \rightarrow \wp(\mathbb{N})$$

# Abstract Interpretation

$$\alpha : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{P})$$

$$\gamma : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{N})$$

$$\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$$

$$\text{succ}^\# : \mathbb{P} \rightarrow \mathbb{P}$$

# Abstract Interpretation

$$\alpha : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{P})$$

$$\gamma : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{N})$$

$$\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$$

$$\text{succ}^\# : \mathbb{P} \rightarrow \mathbb{P}$$

$$f^N : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{N})$$

$$f^N(\mathbb{N}) = ?$$

$$f^P : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{P})$$

$$f^P(\mathbb{P}) = ?$$

# Abstract Interpretation

$$\alpha : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{P})$$

$$\gamma : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{N})$$

$$\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$$

$$\text{succ}^\# : \mathbb{P} \rightarrow \mathbb{P}$$

$$\uparrow \text{succ} : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{N})$$

$$\uparrow \text{succ}(\mathbb{N}) = \{\text{succ}(n) \mid n \in \mathbb{N}\}$$

$$\uparrow \text{succ}^\# : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{P})$$

$$\uparrow \text{succ}^\#(\mathbb{P}) = \{\text{succ}^\#(p) \mid p \in \mathbb{P}\}$$

# Abstract Interpretation

$$\alpha : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{P})$$

$$\gamma : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{N})$$

$$\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$$

$$\text{succ}^\# : \mathbb{P} \rightarrow \mathbb{P}$$

$$\uparrow \text{succ} : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{N})$$

$$\uparrow \text{succ}(\mathbb{N}) = \{\text{succ}(n) \mid n \in \mathbb{N}\}$$

$$\uparrow \text{succ}^\# : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{P})$$

$$\uparrow \text{succ}^\#(\mathbb{P}) = \{\text{succ}^\#(p) \mid p \in \mathbb{P}\}$$

$$\text{sound} : \alpha(\uparrow \text{succ}(\gamma(\mathbb{P}))) \subseteq \uparrow \text{succ}^\#(\mathbb{P})$$

# Abstract Interpretation

$$\alpha : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{P})$$

$$\gamma : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{N})$$

$$\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$$

$$\text{succ}^\# : \mathbb{P} \rightarrow \mathbb{P}$$

$$\uparrow \text{succ} : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{N})$$

$$\uparrow \text{succ}(\mathbb{N}) = \{\text{succ}(n) \mid n \in \mathbb{N}\}$$

$$\uparrow \text{succ}^\# : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{P})$$

$$\uparrow \text{succ}^\#(\mathbb{P}) = \{\text{succ}^\#(p) \mid p \in \mathbb{P}\}$$

$$\text{sound} : \alpha(\uparrow \text{succ}(\gamma(\mathbb{P}))) \subseteq \uparrow \text{succ}^\#(\mathbb{P})$$

$$\text{optimal} : \alpha(\uparrow \text{succ}(\gamma(\mathbb{P}))) = \uparrow \text{succ}^\#(\mathbb{P})$$

# Abstract Interpretation

optimal :  $\alpha(\uparrow\text{succ}(\gamma(P))) = \uparrow\text{succ}^\#(P)$

# Abstract Interpretation

```
calc : α(↑succ(γ(P))) = ... ≡ ↑succ#(P)
```

# Abstract Interpretation

```
calc : α(↑succ(γ(P))) = ... ≡ ↑succ#(P)
```

```
α(↑succ(γ({E})))
```

# Abstract Interpretation

```
calc : α(↑succ(γ(P))) = ... ≡ ↑succ#(P)
```

$$\begin{aligned} & \alpha(\uparrow\text{succ}(\gamma(\{E\}))) \\ &= \alpha(\uparrow\text{succ}(\{n \mid \text{even}(n)\})) \end{aligned}$$

# Abstract Interpretation

```
calc : α(↑succ(γ(P))) = ... ≡ ↑succ#(P)
```

$$\begin{aligned} & \alpha(\uparrow\text{succ}(\gamma(\{E\}))) \\ &= \alpha(\uparrow\text{succ}(\{n \mid \text{even}(n)\})) \\ &= \alpha(\{\text{succ}(n) \mid \text{even}(n)\}) \end{aligned}$$

# Abstract Interpretation

```
calc : α(↑succ(γ(P))) = ... ≡ ↑succ#(P)
```

$$\begin{aligned} & \alpha(\uparrow\text{succ}(\gamma(\{E\}))) \\ &= \alpha(\uparrow\text{succ}(\{n \mid \text{even}(n)\})) \\ &= \alpha(\{\text{succ}(n) \mid \text{even}(n)\}) \\ &= \alpha(\{n \mid \text{odd}(n)\}) \end{aligned}$$

# Abstract Interpretation

```
calc : α(↑succ(γ(P))) = ... ≡ ↑succ#(P)
```

$$\begin{aligned} & \alpha(\uparrow\text{succ}(\gamma(\{E\}))) \\ &= \alpha(\uparrow\text{succ}(\{n \mid \text{even}(n)\})) \\ &= \alpha(\{\text{succ}(n) \mid \text{even}(n)\}) \\ &= \alpha(\{n \mid \text{odd}(n)\}) \\ &= \{0\} \end{aligned}$$

# Abstract Interpretation

```
calc : α(↑succ(γ(P))) = ... ≡ ↑succ#(P)
```

$$\begin{aligned} & \alpha(\uparrow\text{succ}(\gamma(\{E\}))) \\ &= \alpha(\uparrow\text{succ}(\{n \mid \text{even}(n)\})) \\ &= \alpha(\{\text{succ}(n) \mid \text{even}(n)\}) \\ &= \alpha(\{n \mid \text{odd}(n)\}) \\ &= \{0\} \\ &\stackrel{\Delta}{=} \uparrow\text{succ}^{\#}(\{E\}) \end{aligned}$$

# Abstract Interpretation

calc :  $\alpha(\uparrow\text{succ}(\gamma(P))) = \dots \triangleq \uparrow\text{succ}^\#(P)$

$$\uparrow\text{succ}^\#(\{E\}) \triangleq \{0\}$$

# Abstract Interpretation

$$\wp(\textcolor{blue}{P}) \rightarrow \dots \rightarrow \wp(\textcolor{blue}{P})$$

```
calc : α(↑succ(γ(P))) = ... ≡ ↑succ#(P)
```

$$\uparrow\text{succ}^{\#}(\{E\}) \triangleq \{0\}$$

# Abstract Interpretation

$$\wp(\textcolor{blue}{P}) \rightarrow \dots \rightarrow \wp(\textcolor{blue}{P})$$

calc :  $\alpha(\uparrow\text{succ}(\gamma(P))) = \dots \triangleq \uparrow\text{succ}^\#(P)$

$$\uparrow\text{succ}^\#(\{\textcolor{green}{E}\}) \triangleq \{\textcolor{green}{0}\}$$

$\wp(P) \coloneqq (\textcolor{blue}{P} \rightarrow \text{prop}) \approx \text{“specification”}$

$\wp(P) \coloneqq [\textcolor{blue}{P}] \approx \text{“constructed”}$

# Abstract Interpretation

$$\wp(\textcolor{blue}{P}) \rightarrow \dots \rightarrow \wp(\textcolor{blue}{P})$$

calc :  $\alpha(\uparrow\text{succ}(\gamma(P))) = \dots \triangleq \uparrow\text{succ}^\#(P)$

$$\uparrow\text{succ}^\#(\{\textcolor{green}{E}\}) \triangleq \{\textcolor{green}{0}\}$$

$\wp(\textcolor{blue}{P}) \doteq (\textcolor{blue}{P} \rightarrow \text{prop}) \approx \text{“specification”}$

$\wp(\textcolor{blue}{P}) \doteq [\textcolor{blue}{P}] \approx \text{“constructed”}$

# Abstract Interpretation

$$\wp(\mathbb{P}) \rightarrow \dots \rightarrow \wp(\mathbb{P})$$

calc :  $\alpha(\uparrow\text{succ}(\gamma(\mathbb{P}))) = \dots \triangleq \uparrow\text{succ}^\#(\mathbb{P})$

$$\uparrow\text{succ}^\#(\{\mathbb{E}\}) \triangleq \{0\}$$

$\wp(\mathbb{P}) \doteq (\mathbb{P} \rightarrow \text{prop}) \approx \text{"specification"}$

$\wp(\mathbb{P}) \doteq [\mathbb{P}] \approx \text{"constructed"}$

# Abstract Interpretation

$$\wp(\mathbb{P}) \rightarrow \dots \rightarrow \wp(\mathbb{P})$$

calc :  $\alpha(\uparrow\text{succ}(\gamma(\mathbb{P}))) = \dots \triangleq \uparrow\text{succ}^\#(\mathbb{P})$

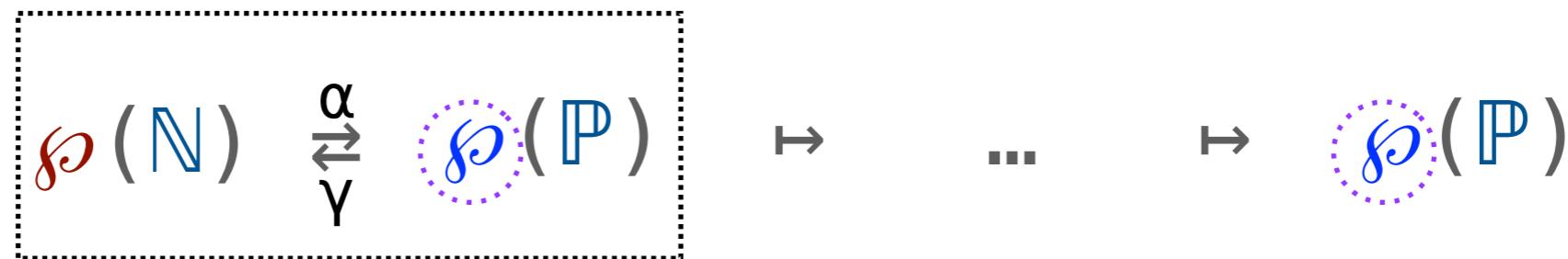
$$\uparrow\text{succ}^\#(\{\mathbb{E}\}) \triangleq \{0\}$$

$\wp(\mathbb{P}) \doteq (\mathbb{P} \rightarrow \text{prop}) \approx \text{"specification"}$

$\wp(\mathbb{P}) \doteq [\mathbb{P}] \approx \text{"constructed"}$

**no extraction**

# Abstract Interpretation



calc :  $\alpha(\uparrow \text{succ}(\gamma(P))) = \dots \triangleq \uparrow \text{succ}^\#(P)$

$$\uparrow \text{succ}^\#(\{E\}) \triangleq \{0\}$$

$\wp(P) \doteq (P \rightarrow \text{prop}) \approx \text{"specification"}$

$\wp(P) \doteq [P] \approx \text{"constructed"}$

# Abstract Interpretation

$$\boxed{\wp(\mathbb{N}) \xrightarrow[\gamma]{\alpha} \wp(\mathbb{P})} \rightarrow \dots \rightarrow \wp(\mathbb{P})$$

calc :  $\alpha(\uparrow \text{succ}(\gamma(P))) = \dots \triangleq \uparrow \text{succ}^\#(P)$

$$\uparrow \text{succ}^\#(\{E\}) \triangleq \{0\}$$

$\wp(P) \doteq (P \rightarrow \text{prop}) \approx \text{"specification"}$

$\wp(P) \doteq [P] \approx \text{"constructed"}$

**no extraction**

# Four Stories

Direct Verification	$\times$ calculate
Abstract Interpretation	$\times$ mechanize
Kleisli GCs	$\checkmark$ calculate $\frac{1}{2}$ mechanize
Constructive GCs	$\checkmark$ calculate $\checkmark$ mechanize

# Kleisli GCs

$$\alpha : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{P})$$

$$\gamma : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{N})$$

$$\uparrow \text{succ} : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{N})$$

$$\uparrow \text{succ}^\# : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{P})$$

# Kleisli GCs

$$\begin{array}{ll} \alpha : \mathbb{N} \rightarrow \mathbb{P} \rightarrow \text{prop} & \uparrow \text{succ} : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \text{prop} \\ \gamma : \mathbb{P} \rightarrow \mathbb{N} \rightarrow \text{prop} & \uparrow \text{succ}^\# : \mathbb{P} \rightarrow \mathbb{P} \rightarrow \text{prop} \end{array}$$

$$\wp(X) := X \rightarrow \text{prop}$$

# Kleisli GCs

$$\alpha : \mathbb{N} \rightarrow \wp(\mathbb{P})$$

$$\gamma : \mathbb{P} \rightarrow \wp(\mathbb{N})$$

$$\uparrow \text{SUCC} : \mathbb{N} \rightarrow \wp(\mathbb{N})$$

$$\uparrow \text{SUCC}^\# : \mathbb{P} \rightarrow \wp(\mathbb{P})$$

# Kleisli GCs

$$\begin{array}{l} \alpha : \mathbb{N} \rightarrow \wp(\mathbb{P}) \\ \gamma : \mathbb{P} \rightarrow \wp(\mathbb{N}) \end{array}$$

$$\begin{array}{l} \uparrow \text{SUCC} : \mathbb{N} \rightarrow \wp(\mathbb{N}) \\ \uparrow \text{SUCC}^\# : \mathbb{P} \rightarrow \wp(\mathbb{P}) \end{array}$$

$$N \subseteq \gamma(\alpha(N)) \quad \wedge \quad \alpha(\gamma(P)) \subseteq P$$

=====

$$N \subseteq \gamma(P) \iff \alpha(N) \subseteq P$$

# Kleisli GCs

$$\begin{array}{l} \alpha : \mathbb{N} \rightarrow \wp(\mathbb{P}) \\ \gamma : \mathbb{P} \rightarrow \wp(\mathbb{N}) \end{array}$$

$$\begin{array}{l} \uparrow \text{SUCC} : \mathbb{N} \rightarrow \wp(\mathbb{N}) \\ \uparrow \text{SUCC}^\# : \mathbb{P} \rightarrow \wp(\mathbb{P}) \end{array}$$

$$\text{id} \sqsubseteq \gamma \circ \alpha \wedge \alpha \circ \gamma \sqsubseteq \text{id}$$

=====

$$\text{id}(\mathbb{N}) \subseteq \gamma(\mathbb{P}) \iff \alpha(\mathbb{N}) \subseteq \text{id}(\mathbb{P})$$

# Kleisli GCs

$$\begin{array}{l} \alpha : \mathbb{N} \rightarrow \wp(\mathbb{P}) \\ \gamma : \mathbb{P} \rightarrow \wp(\mathbb{N}) \end{array}$$

$$\begin{array}{l} \uparrow \text{SUCC} : \mathbb{N} \rightarrow \wp(\mathbb{N}) \\ \uparrow \text{SUCC}^\# : \mathbb{P} \rightarrow \wp(\mathbb{P}) \end{array}$$

$$\begin{array}{c} \text{ret} \sqsubseteq \gamma \circledast \alpha \wedge \alpha \circledast \gamma \sqsubseteq \text{ret} \\ \hline \hline \\ \text{ret}(n) \subseteq \gamma(p) \iff \alpha(n) \subseteq \text{ret}(p) \end{array}$$

# Kleisli GCs

$$\begin{array}{l} \alpha : \mathbb{N} \rightarrow \wp(\mathbb{P}) \\ \gamma : \mathbb{P} \rightarrow \wp(\mathbb{N}) \end{array}$$

$$\begin{array}{l} \uparrow \text{SUCC} : \mathbb{N} \rightarrow \wp(\mathbb{N}) \\ \uparrow \text{SUCC}^\# : \mathbb{P} \rightarrow \wp(\mathbb{P}) \end{array}$$

$$\begin{array}{c} \text{ret} \sqsubseteq \gamma \circledast \alpha \wedge \alpha \circledast \gamma \sqsubseteq \text{ret} \\ \hline \hline \\ \text{ret}(n) \subseteq \gamma(p) \iff \alpha(n) \subseteq \text{ret}(p) \end{array}$$

$$\text{sound} : \alpha \circ \uparrow \text{SUCC} \circ \gamma \sqsubseteq \uparrow \text{SUCC}^\#$$

# Kleisli GCs

$$\alpha : \mathbb{N} \rightarrow \wp(\mathbb{P})$$

$$\gamma : \mathbb{P} \rightarrow \wp(\mathbb{N})$$

$$\uparrow\text{SUCC} : \mathbb{N} \rightarrow \wp(\mathbb{N})$$

$$\uparrow\text{SUCC}^\# : \mathbb{P} \rightarrow \wp(\mathbb{P})$$

$$\text{ret} \sqsubseteq \gamma \circ \alpha \wedge \alpha \circ \gamma \sqsubseteq \text{ret}$$

=====

$$\text{ret}(n) \subseteq \gamma(p) \iff \alpha(n) \subseteq \text{ret}(p)$$

$$\text{sound} : \alpha \circ \uparrow\text{SUCC} \circ \gamma \sqsubseteq \uparrow\text{SUCC}^\#$$

# Four Stories

Direct Verification	$\times$ calculate
Abstract Interpretation	$\times$ mechanize
Kleisli GCs	$\checkmark$ calculate $\frac{1}{2}$ mechanize
Constructive GCs	$\checkmark$ calculate $\checkmark$ mechanize

# Constructive GCs

$$\begin{array}{l} \alpha : \mathbb{N} \rightarrow \wp(\mathbb{P}) \\ \gamma : \mathbb{P} \rightarrow \wp(\mathbb{N}) \end{array}$$

$\wedge$

$$\begin{array}{l} \text{ret} \sqsubseteq \gamma \circledast \alpha \\ \alpha \circledast \gamma \sqsubseteq \text{ret} \end{array}$$

---

# Constructive GCs

$$\begin{array}{c} \alpha : \mathbb{N} \rightarrow \wp(\mathbb{P}) \\ \gamma : \mathbb{P} \rightarrow \wp(\mathbb{N}) \end{array} \quad \wedge \quad \begin{array}{c} \text{ret} \sqsubseteq \gamma \circledast \alpha \\ \alpha \circledast \gamma \sqsubseteq \text{ret} \end{array}$$

---

$$\exists(\eta : \mathbb{N} \rightarrow \mathbb{P}). \alpha(x) = \text{ret}(\eta(x))$$

# Constructive GCs

$$\begin{array}{l} \alpha : \mathbb{N} \rightarrow \wp(\mathbb{P}) \\ \gamma : \mathbb{P} \rightarrow \wp(\mathbb{N}) \end{array}$$

$\wedge$

$$\begin{array}{l} \text{ret} \sqsubseteq \gamma \circledast \alpha \\ \alpha \circledast \gamma \sqsubseteq \text{ret} \end{array}$$

---

$$\exists(\eta : \mathbb{N} \rightarrow \mathbb{P}). \alpha(x) = \text{ret}(\eta(x))$$



constructive

# Constructive GCs

$$\begin{array}{c} \alpha : \mathbb{N} \rightarrow \wp(\mathbb{P}) \\ \gamma : \mathbb{P} \rightarrow \wp(\mathbb{N}) \end{array} \quad \wedge \quad \begin{array}{c} \text{ret} \sqsubseteq \gamma \circledast \alpha \\ \alpha \circledast \gamma \sqsubseteq \text{ret} \end{array}$$

---

$$\exists(\eta : \mathbb{N} \rightarrow \mathbb{P}). \alpha(x) = \text{ret}(\eta(x))$$

The “specification effect” in  $\alpha$  is always benign

# Constructive GCs

$$\begin{aligned}\alpha &: \mathbb{N} \rightarrow \wp(\mathbb{P}) \\ \gamma &: \mathbb{P} \rightarrow \wp(\mathbb{N})\end{aligned}$$

# Constructive GCs

$$\begin{aligned}\eta &: \mathbb{N} \rightarrow \mathbb{P} \\ \mu &: \mathbb{P} \rightarrow \wp(\mathbb{N})\end{aligned}$$

# Constructive GCs

$$\begin{aligned}\eta &: \mathbb{N} \rightarrow \mathbb{P} \\ \mu &: \mathbb{P} \rightarrow \wp(\mathbb{N})\end{aligned}$$

$$\text{ret} \sqsubseteq \gamma \otimes \alpha \wedge \alpha \otimes \gamma \sqsubseteq \text{ret}$$

$$\text{=====}$$
$$\text{ret}(n) \subseteq \gamma(p) \iff \alpha(n) \subseteq \text{ret}(p)$$

# Constructive GCs

$$\begin{aligned}\eta &: \mathbb{N} \rightarrow \mathbb{P} \\ \mu &: \mathbb{P} \rightarrow \wp(\mathbb{N})\end{aligned}$$

$$\text{ret} \sqsubseteq \mu \circledast \uparrow(\eta) \quad \wedge \quad \uparrow(\eta) \circledast \mu \sqsubseteq \text{ret}$$

$$\text{ret}(n) \subseteq \mu(p) \iff \uparrow(\eta)(n) \subseteq \text{ret}(p)$$

# Constructive GCs

$$\begin{aligned}\text{parity} &: \mathbb{N} \rightarrow \mathbb{P} \\ \llbracket \_ \rrbracket &: \mathbb{P} \rightarrow \wp(\mathbb{N})\end{aligned}$$

# Constructive GCs

$$\begin{aligned}\text{parity} &: \mathbb{N} \rightarrow \mathbb{P} \\ \llbracket \_ \rrbracket &: \mathbb{P} \rightarrow \wp(\mathbb{N})\end{aligned}$$

$n \in \llbracket \text{parity}(n) \rrbracket$

# Constructive GCs

$$\begin{aligned}\text{parity} &: \mathbb{N} \rightarrow \mathbb{P} \\ \llbracket \_ \rrbracket &: \mathbb{P} \rightarrow \wp(\mathbb{N})\end{aligned}$$
$$n \in \llbracket p \rrbracket \rightarrow \text{parity}(n) \sqsubseteq p$$

# Constructive GCs

$$\begin{aligned}\text{parity} &: \mathbb{N} \rightarrow \mathbb{P} \\ \llbracket \_ \rrbracket &: \mathbb{P} \rightarrow \wp(\mathbb{N})\end{aligned}$$

$$n \in \llbracket p \rrbracket \iff \text{parity}(n) \sqsubseteq p$$

# Constructive GCs

$$\begin{aligned}\text{parity} &: \mathbb{N} \rightarrow \mathbb{P} \\ \llbracket \_ \rrbracket &: \mathbb{P} \rightarrow \wp(\mathbb{N})\end{aligned}$$
$$\text{sound} : n \in \llbracket p \rrbracket \implies \text{parity}(\text{succ}(n)) \sqsubseteq \text{succ}^\sharp(p)$$

# Results

# Results

- Metatheory complete w.r.t. subset of classical GC

# Results

- Metatheory complete w.r.t. subset of classical GC
- Kleisli-adjunction analogous to classical GCs

# Results

- Metatheory complete w.r.t. subset of classical GC
- Kleisli-adjunction analogous to classical GCs
- Case Study: Calculational AI [*Cousot 1999*]

# Results

- Metatheory complete w.r.t. subset of classical GC
- Kleisli-adjunction analogous to classical GCs
- Case Study: Calculational AI [*Cousot 1999*]
- Case Study: AGT [*Garcia, Clark and Tanter 2016*]

# Results

- Metatheory complete w.r.t. subset of classical GC
- Kleisli-adjunction analogous to classical GCs
- Case Study: Calculational AI [*Cousot 1999*]
- Case Study: AGT [*Garcia, Clark and Tanter 2016*]
- Sound, optimal and *computable* AIs by construction

# Results

- Metatheory complete w.r.t. subset of classical GC
- Kleisli-adjunction analogous to classical GCs
- Case Study: Calculational AI [*Cousot 1999*]
- Case Study: AGT [*Garcia, Clark and Tanter 2016*]
- Sound, optimal and *computable* AIs by construction
- Metatheory and case studies all verified in Agda

# Constructive GCs

$$\begin{array}{l} \eta : \mathbb{N} \rightarrow \mathbb{P} \\ \mu : \mathbb{P} \rightarrow \wp(\mathbb{N}) \end{array}$$

$$n \in \mu(p) \iff \eta(n) \sqsubseteq p$$

- ✓ calculate
- ✓ mechanize