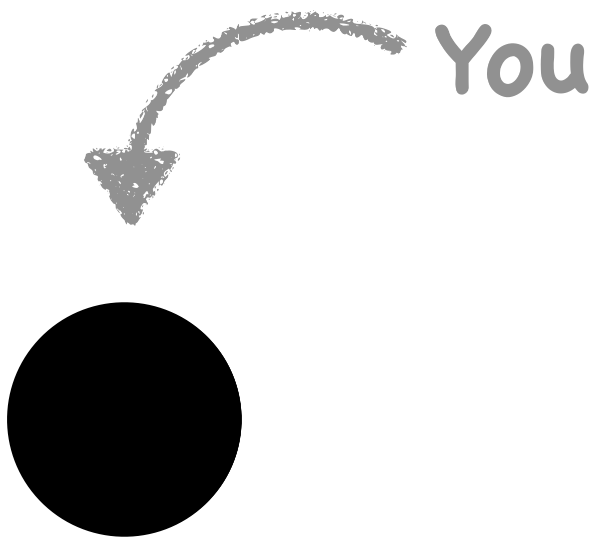
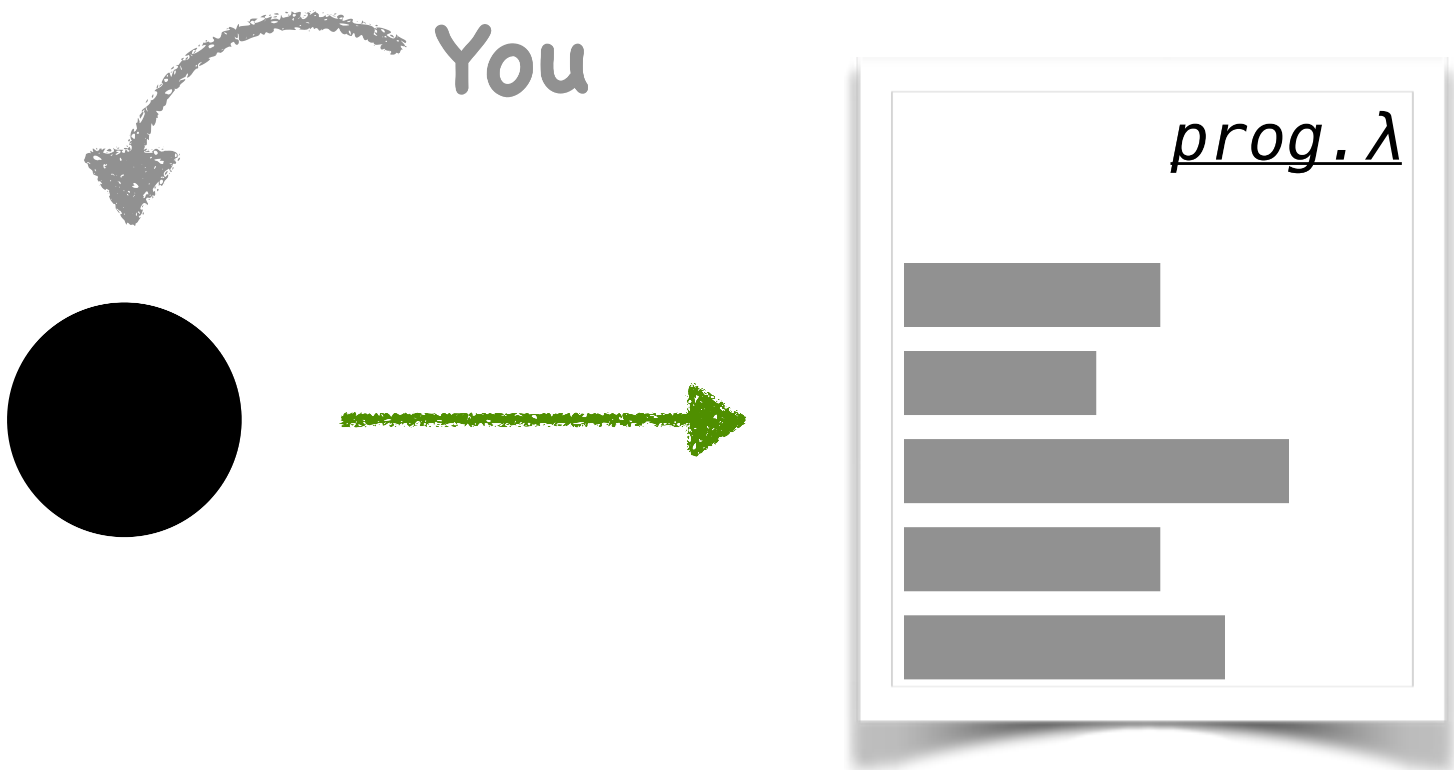
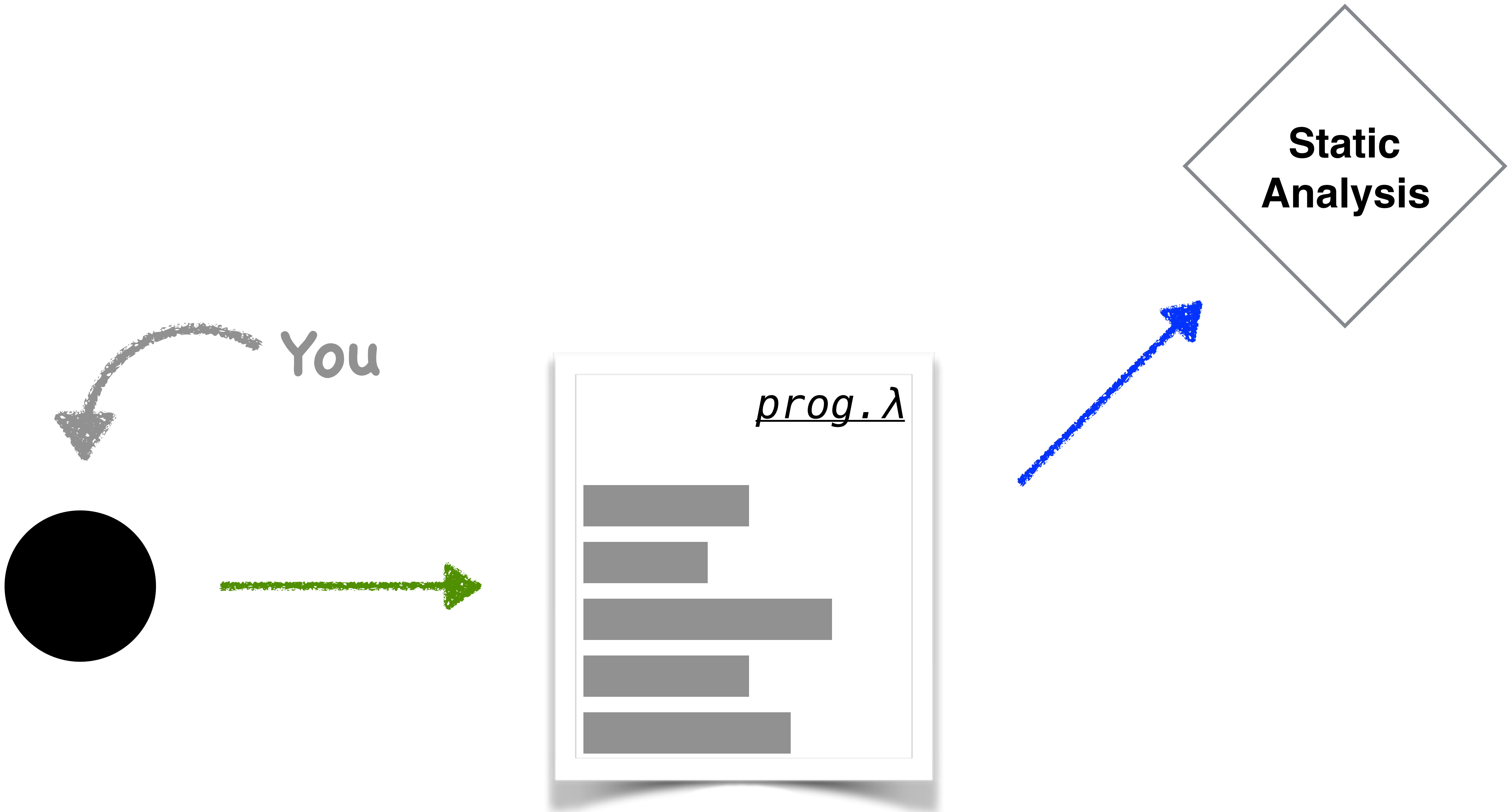
Constructive Galois Connections

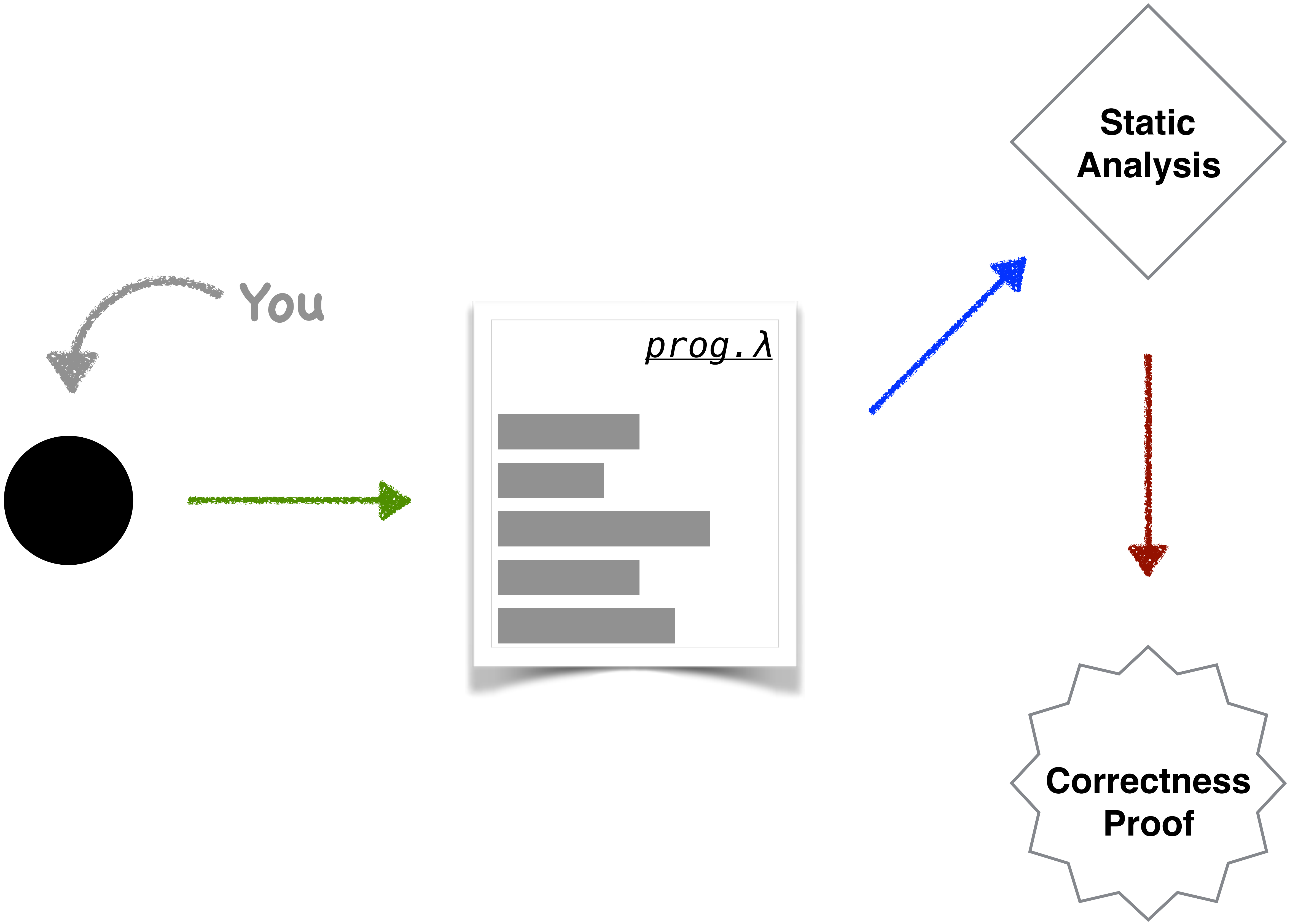
David Darais
University of Maryland

David Van Horn
University of Maryland

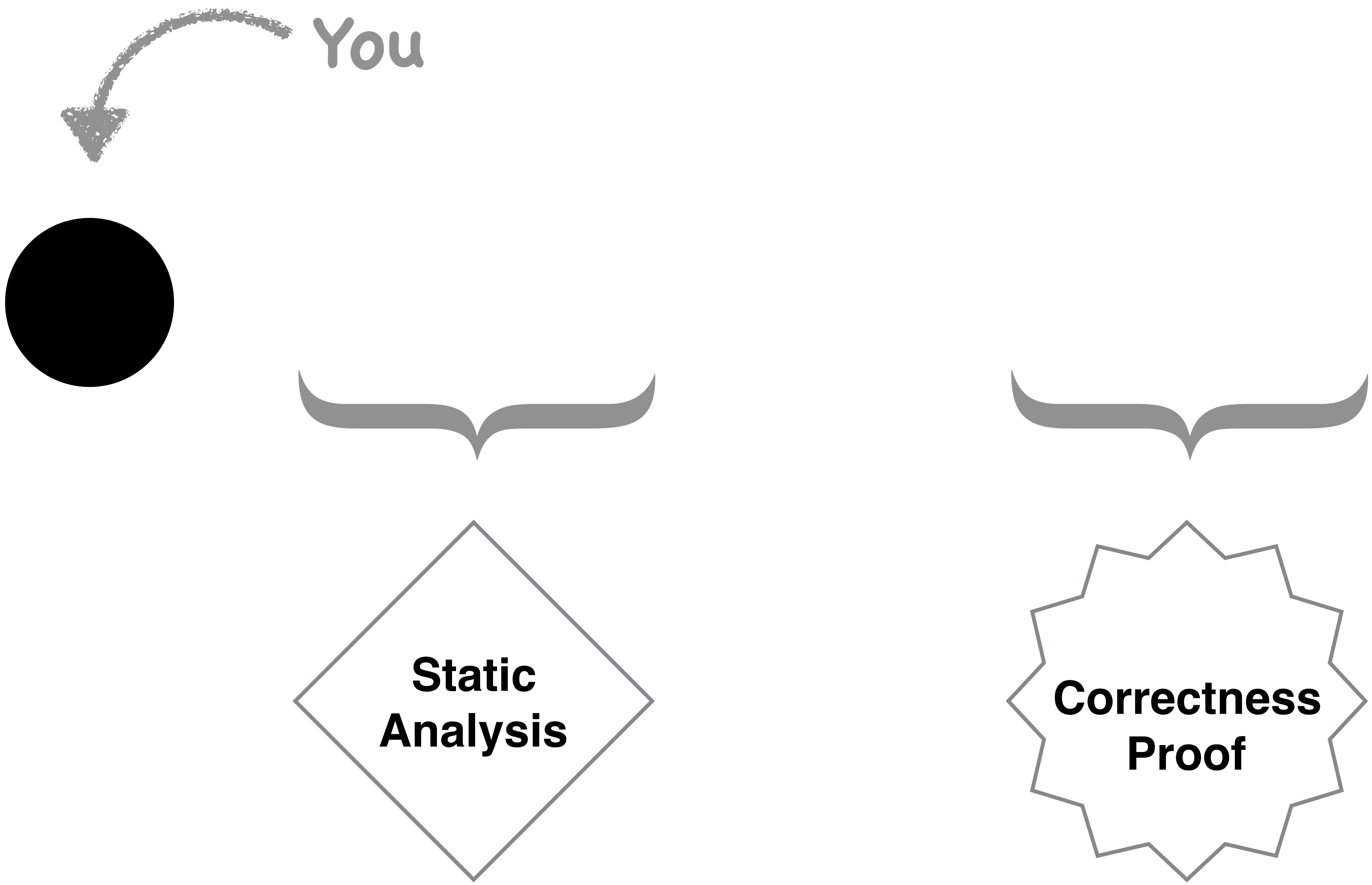

You

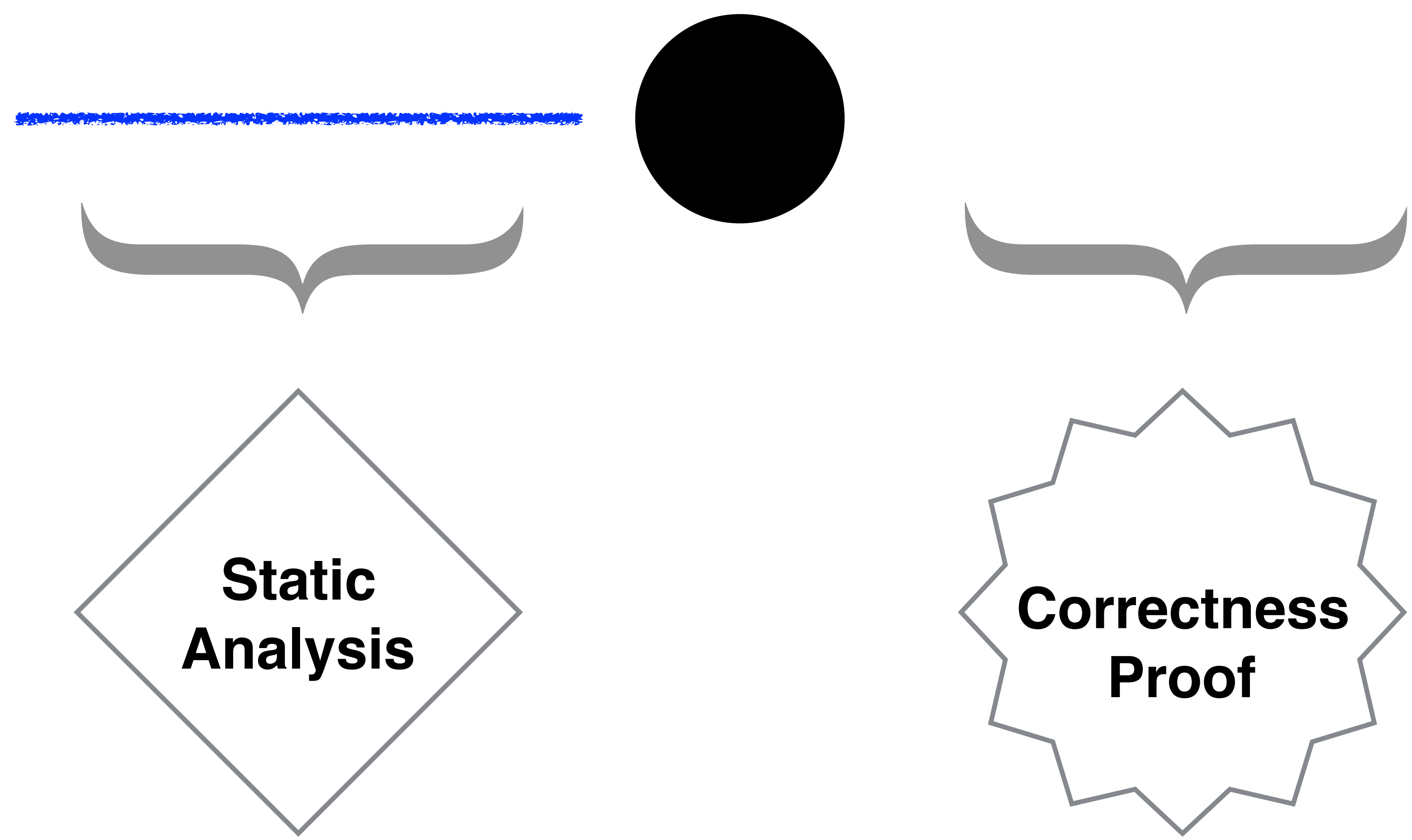

You
prog.λ

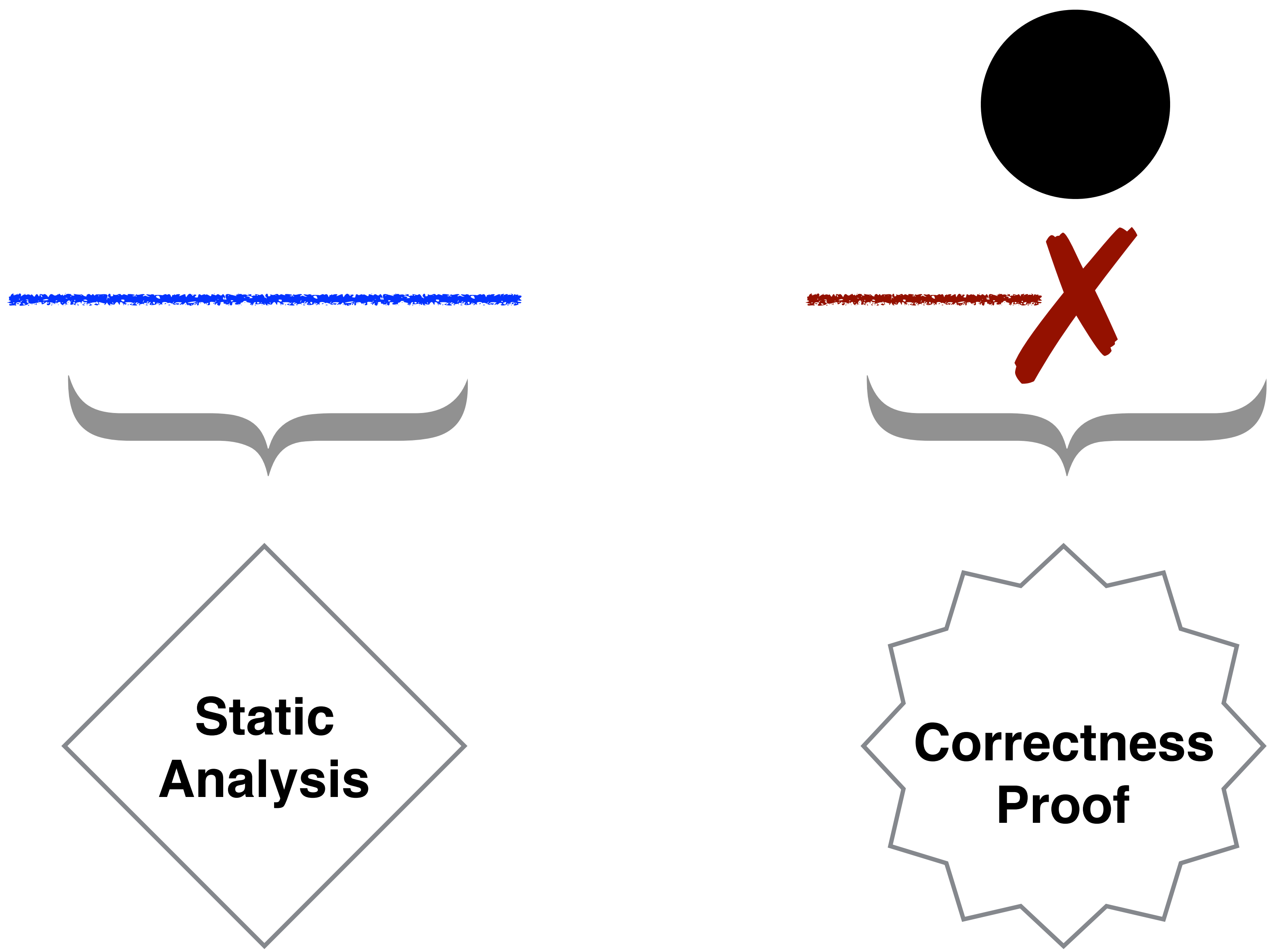

You
prog.λ
Static
Analysis

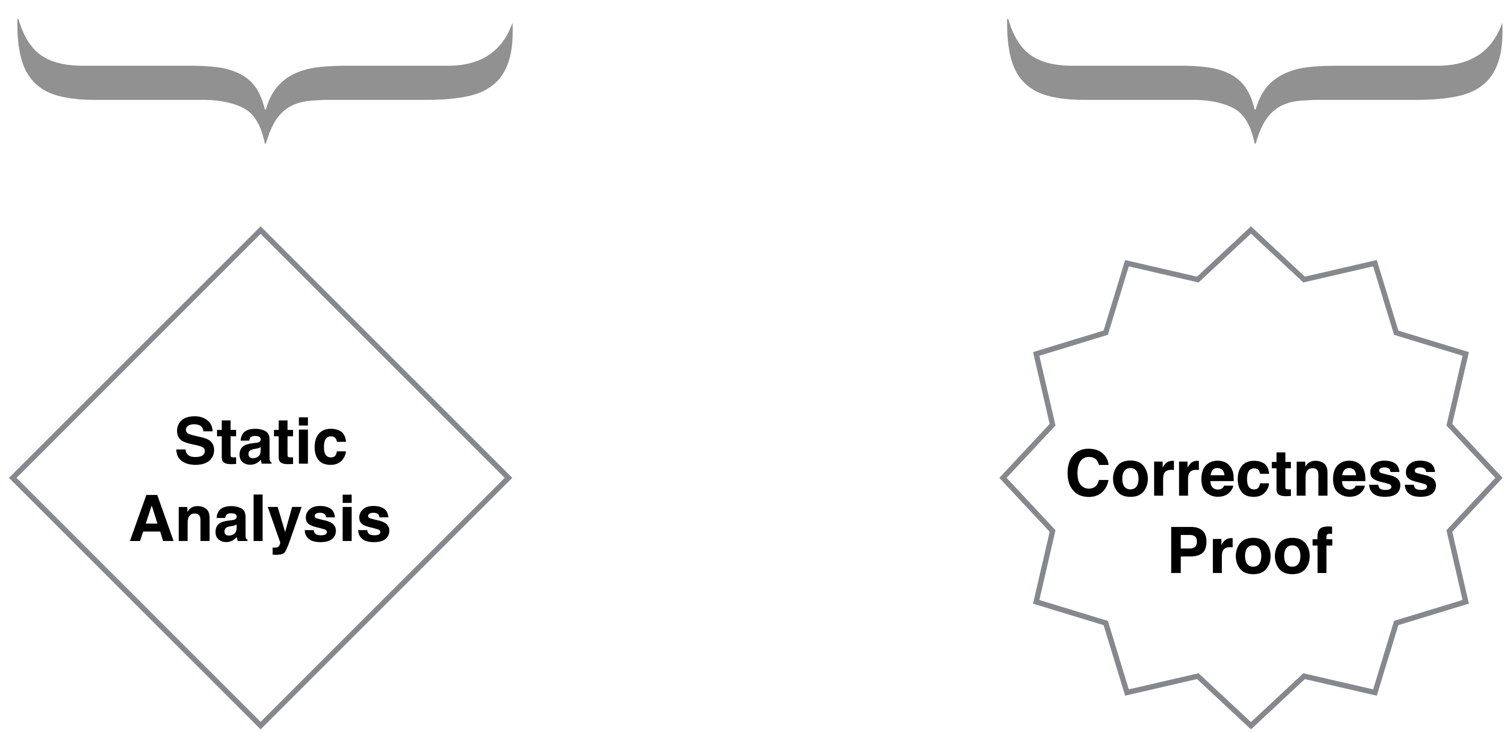


You
prog.λ
Static Analysis
Correctness Proof

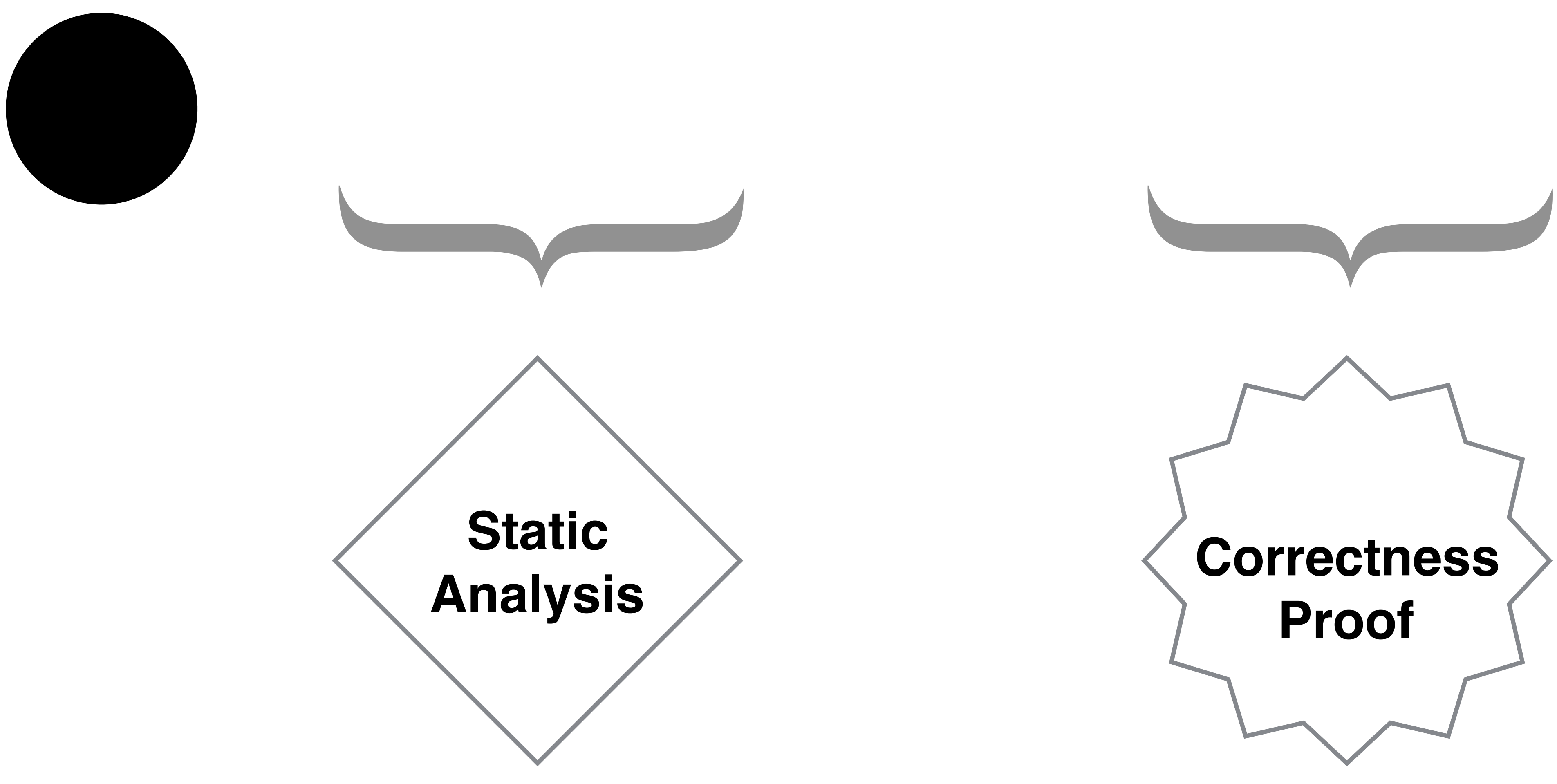

You
Static
Analysis
Correctness
Proof


Static Analysis
Correctness Proof

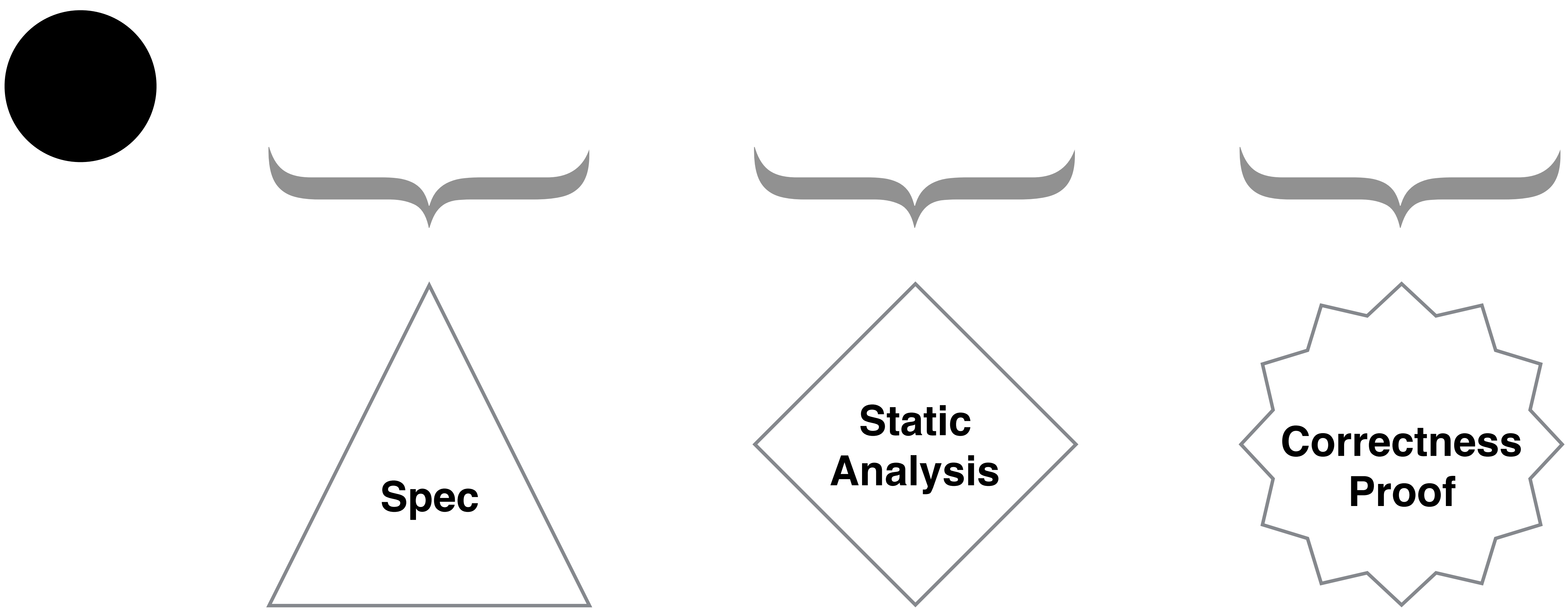

Static Analysis
Correctness Proof


Static Analysis
Correctness Proof

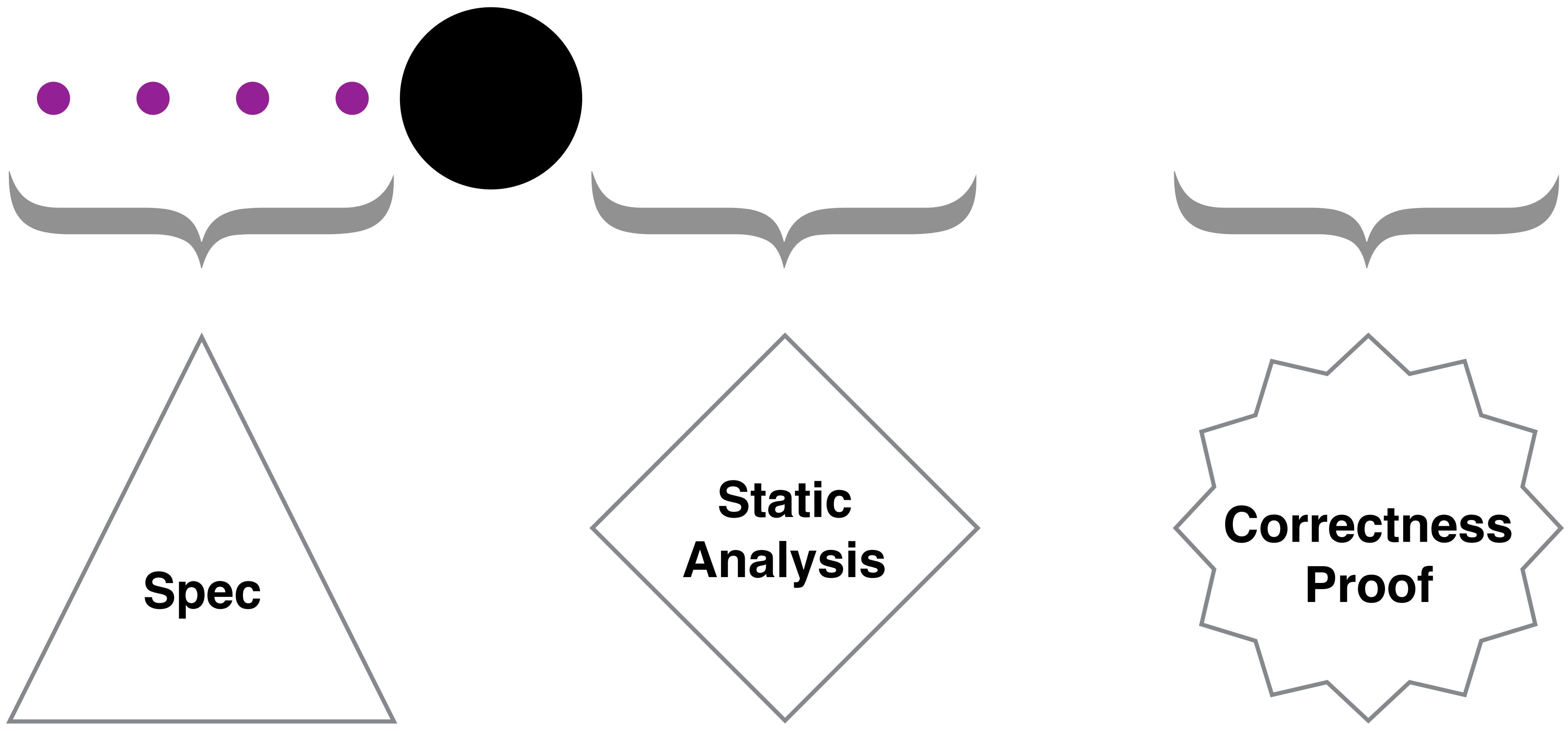
Abstract
Interpretation



Abstract Interpretation

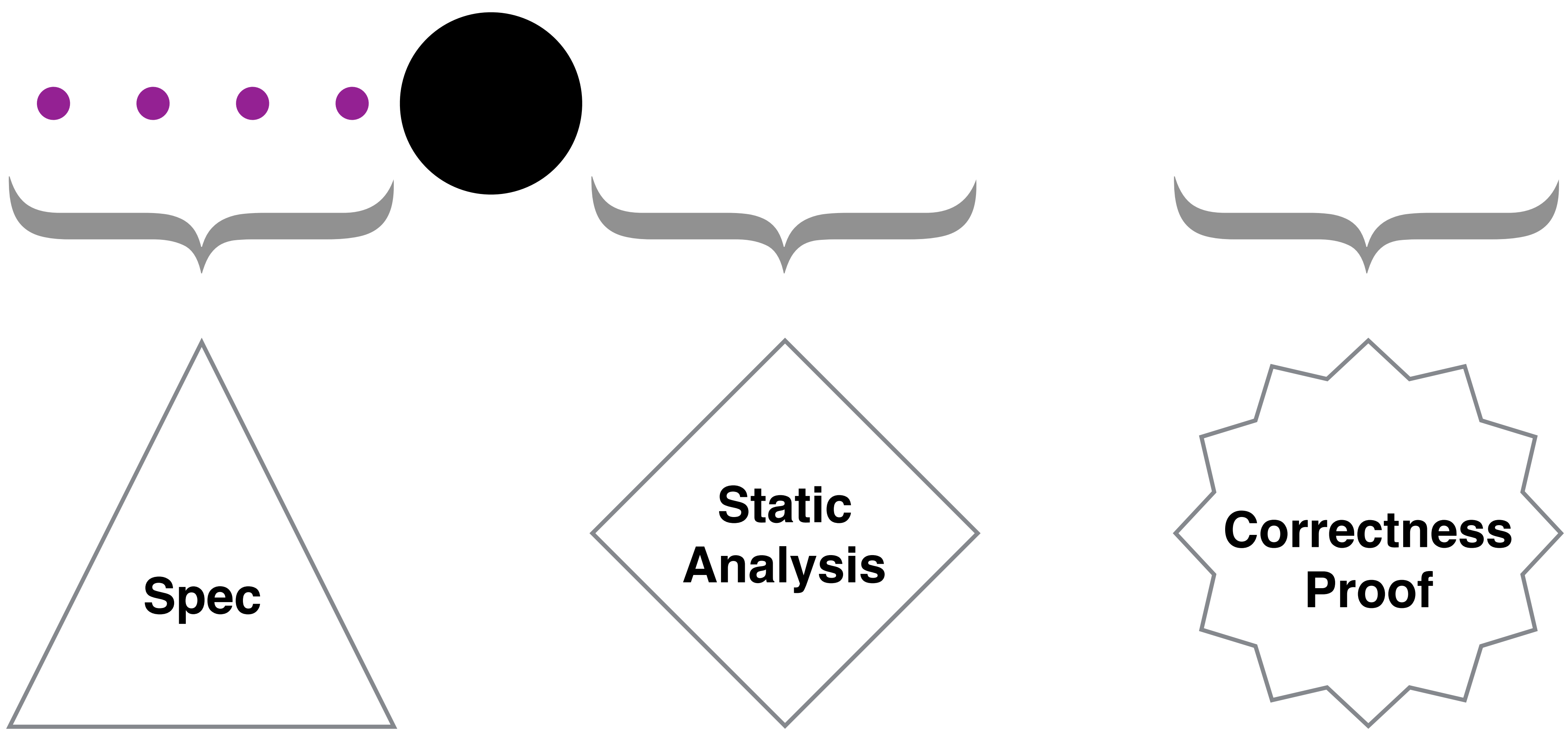


Abstract Interpretation



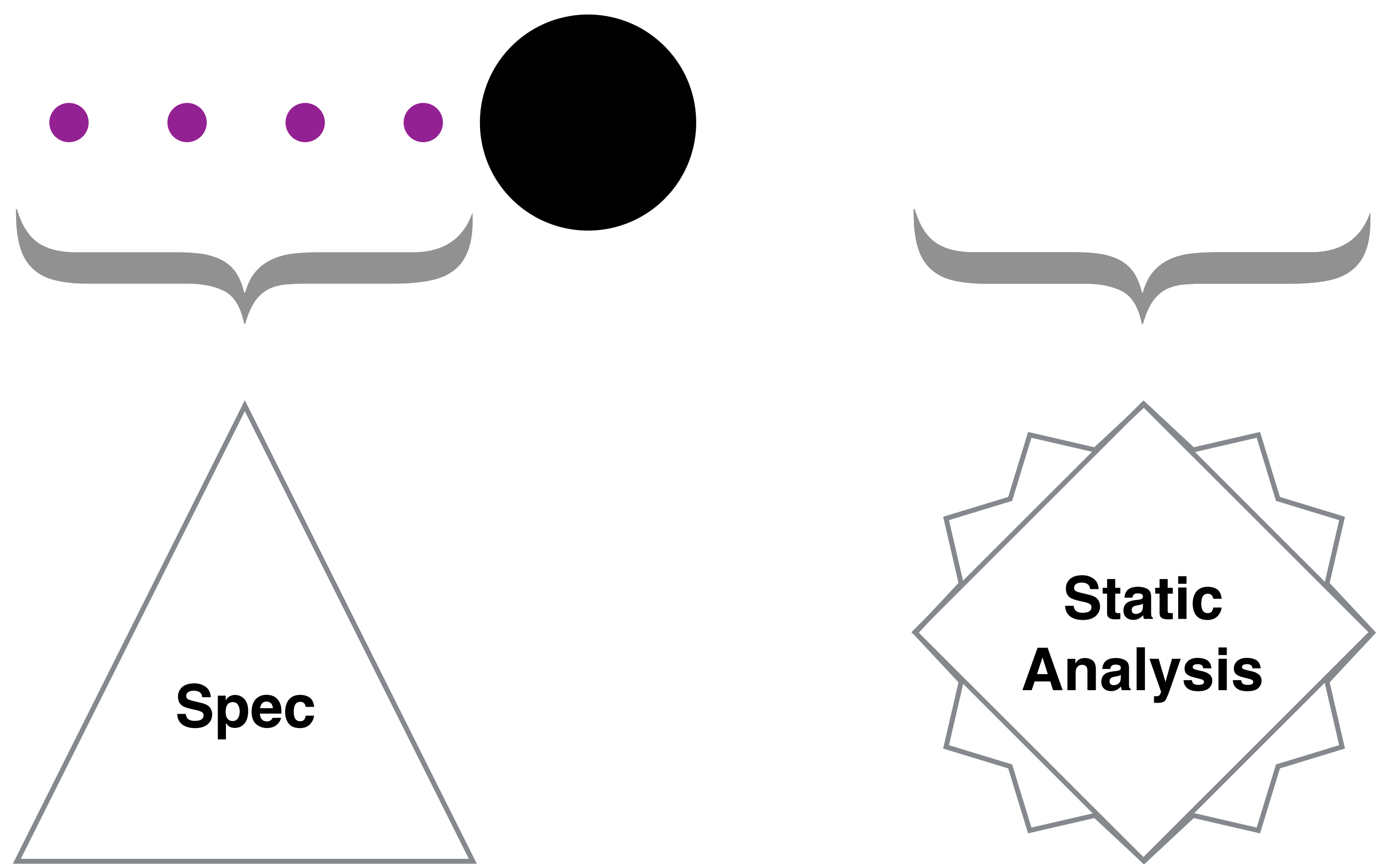
Abstract Interpretation

Calculational Design



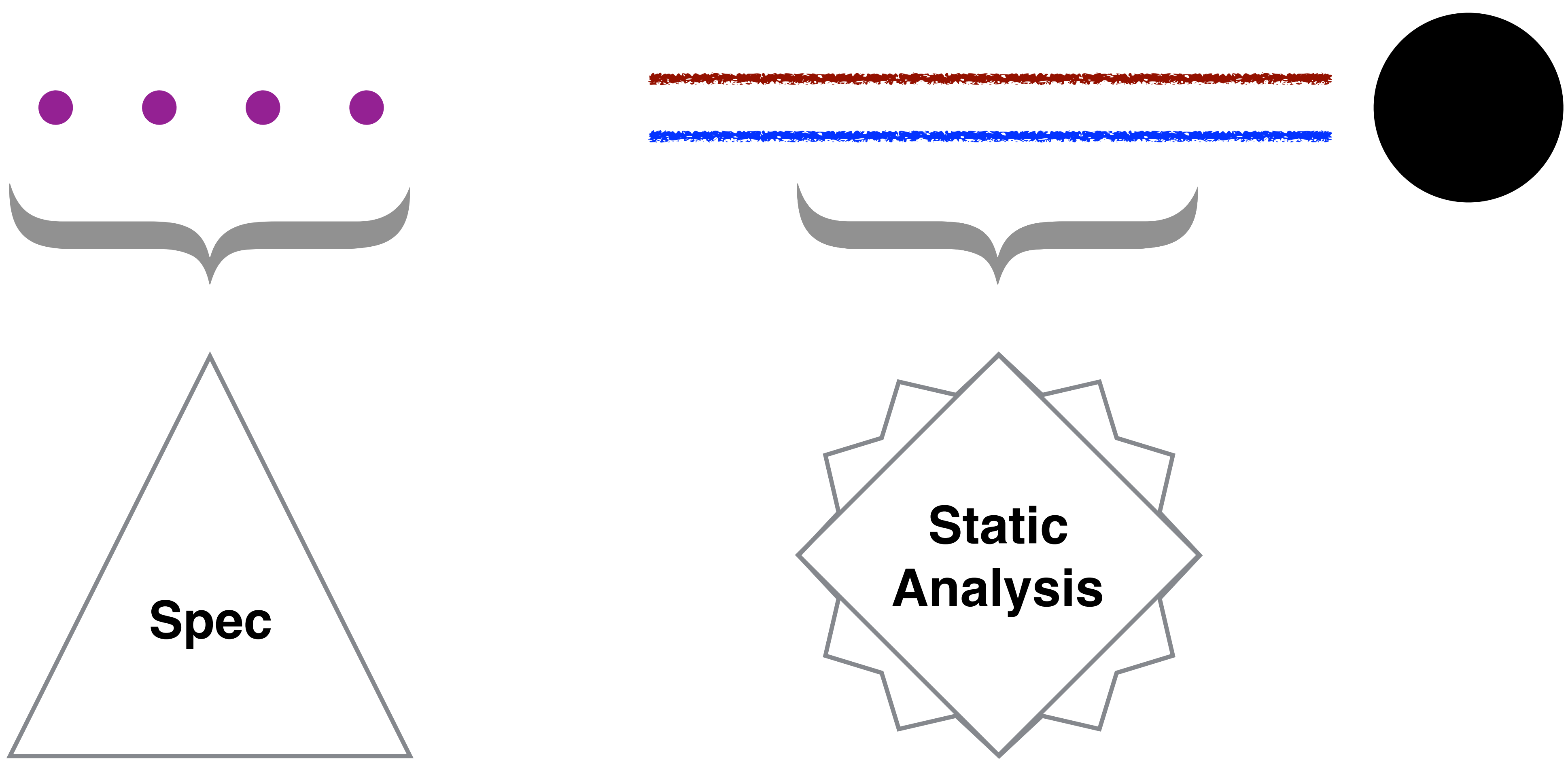
Abstract Interpretation

Calculational Design



Abstract Interpretation

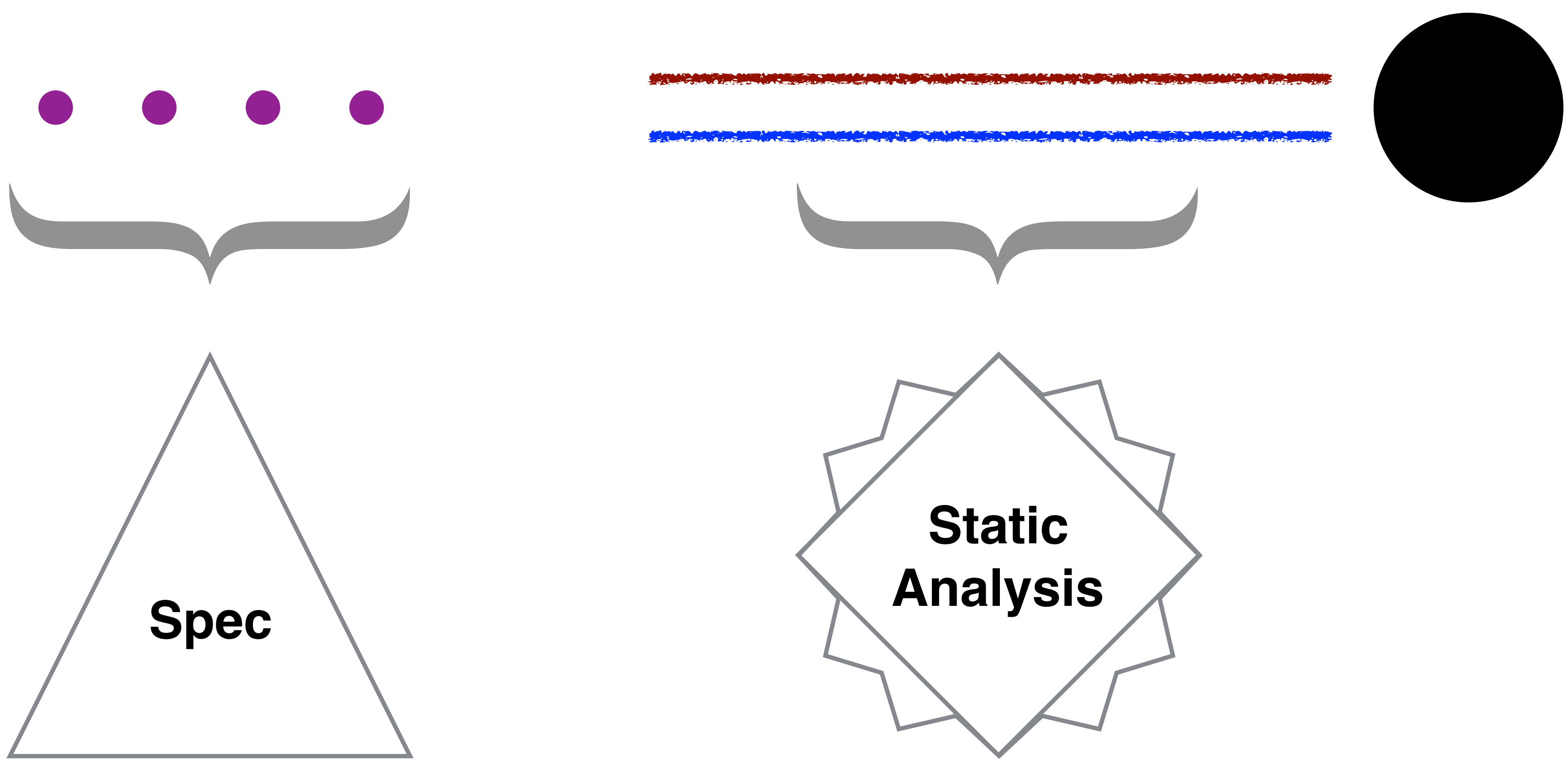
Calculational Design



Abstract Interpretation

Calculational Design

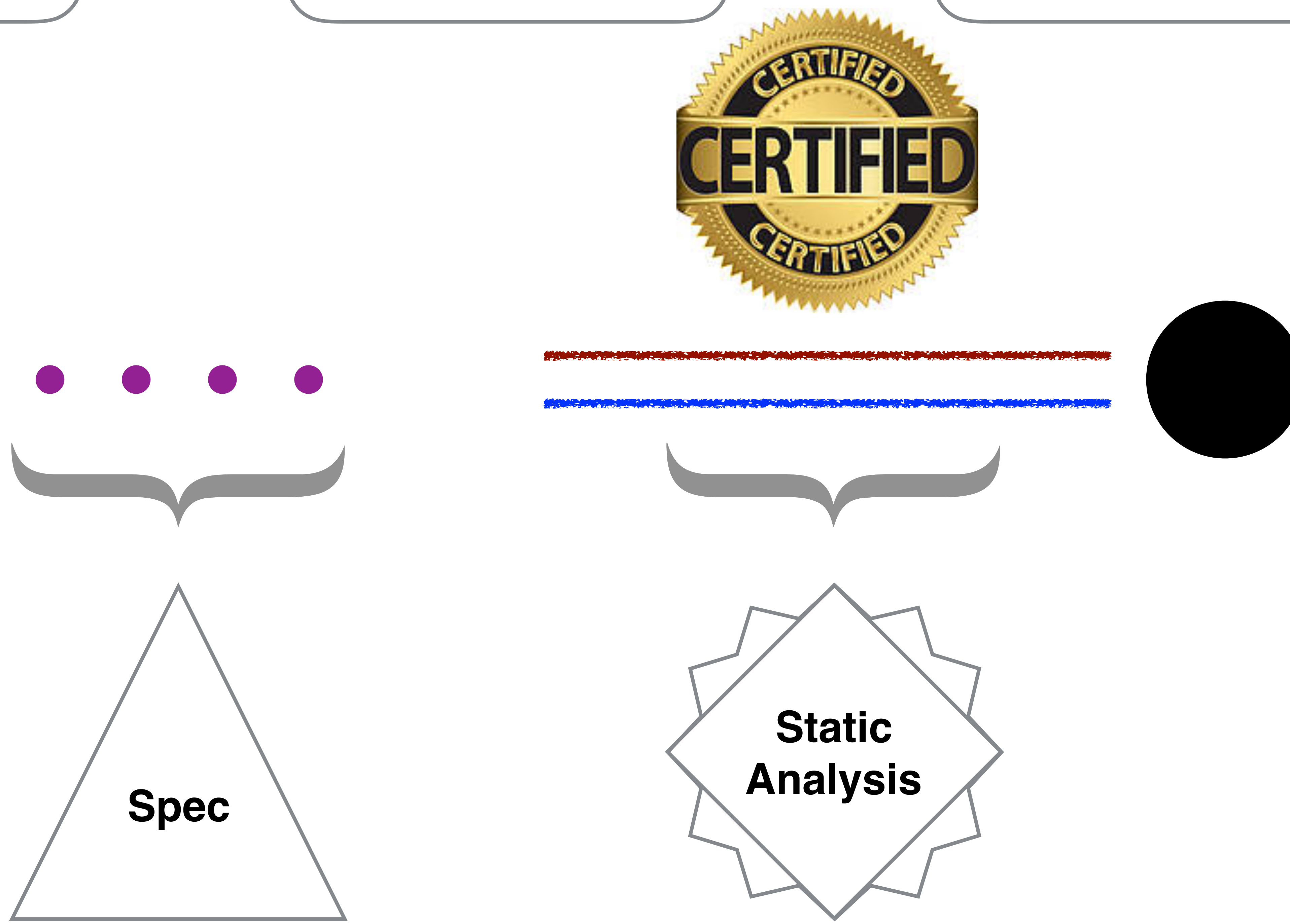
Proof Assistants



Abstract Interpretation

Calculational Design

Proof Assistants



The Dream

Abstract Interpreters

- Synthesized specification
- 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

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 Pichardie

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**]. … 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 ∈ {10,20}

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

$x \in \{10, 20\}$ → $x \in \langle 10, 20 \rangle$

```
…
if (b) {x ≔ 10} else {x ≔ 20}
…
```

$$\begin{tikzcd} x \in \{10,20\} \arrow[r] \arrow[d, phantom, "\subseteq" description] & x \in \langle 10,20 \rangle \arrow[dl] \\ x \in \{10,\ldots,20\} & \end{tikzcd}$$

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

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

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

$\subseteq$

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

$x \in \langle 10,20 \rangle$

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

$\wp(\mathbb{Z})$

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

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

$\cap\!|$

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

$x \in \langle 10, 20 \rangle$

Undecidable

Decidable

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

Classical Reasoning $\lightning$ *Program Extraction* *calculate.cousot*

```
α(eval[n])(ρ♯)
⦃ defn of α ⦄
= αᴵ(eval[n](γᴿ(ρ♯)))
⦃ defn of eval[n] ⦄
= αᴵ({i | ρ ⊢ n ↦ i})
⦃ defn of _⊢_↦_ ⦄
= αᴵ({i})
⦃ defn of eval♯[n] ⦄
≜ eval♯[n](ρ♯)
```

calculate.cousot

```
α(eval[n])(ρ♯)
≀ defn of α ⟆
= αᴵ(eval[n](γᴿ(ρ♯)))
≀ defn of eval[n] ⟆
= αᴵ({i | ρ ⊢ n ↦ i})
≀ defn of _⊢_↦_ ⟆
= αᴵ({i})
≀ 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 * ]
   ≀ defn[eval[ Num n ]] ⟆
▸ ⟦ αᴵ * · (return · n) ⟧
▸ ≀ right-unit[*] ⟆
▸ ⟦ pure · eval♯[ Num n ] · ρ♯ ⟧
```

Four Stories

Direct Verification ✗ `calculate`

Abstract Interpretation ✗ `mechanize`

Four Stories

Direct Verification	✗ `calculate`
Abstract Interpretation	✗ `mechanize`
Kleisli GCs	✓ `calculate` ½ `mechanize`
Constructive GCs	✓ `calculate` ✓ `mechanize`

Direct Verification

Direct Verification

```
succ  : ℕ → ℕ
```

Direct Verification

`succ : ℕ → ℕ` $\qquad\qquad$ $\mathbb{P} \coloneqq \{E, O\}$

Direct Verification

```
succc  : ℕ → ℕ            ℙ ≔ {E,O}

flip : ℙ → ℙ
flip(E) ≔ O
flip(O) ≔ E
```

Direct Verification

```
succ  : ℕ → ℕ                ℙ ≔ {E,O}

flip : ℙ → ℙ                 ⟦_⟧ : ℙ → ℘(ℕ)
flip(E) ≔ O                  ⟦E⟧ ≔ { n | even(n) }
flip(O) ≔ E                  ⟦O⟧ ≔ { n |  odd(n) }
```

Direct Verification

$$\mathtt{succ} : \mathbb{N} \to \mathbb{N}$$

$$\mathbb{P} \coloneqq \{\mathtt{E},\mathtt{O}\}$$

$$\mathtt{flip} : \mathbb{P} \to \mathbb{P}$$
$$\mathtt{flip}(\mathtt{E}) \coloneqq \mathtt{O}$$
$$\mathtt{flip}(\mathtt{O}) \coloneqq \mathtt{E}$$

$$[\![\_]\!] : \mathbb{P} \to \wp(\mathbb{N})$$
$$[\![\mathtt{E}]\!] \coloneqq \{\, n \mid \mathtt{even}(n) \,\}$$
$$[\![\mathtt{O}]\!] \coloneqq \{\, n \mid \mathtt{odd}(n) \,\}$$

$$\boxed{\mathtt{sound} : n \in [\![p]\!] \Longrightarrow \mathtt{succ}(n) \in [\![\mathtt{flip}(p)]\!]}$$

Direct Verification

✓ `flip` can be extracted and executed

✓ ⟦_⟧ can be mechanized effectively

✗ Is `flip` *optimal?*

✗ How to *derive* `flip` from `succ`?

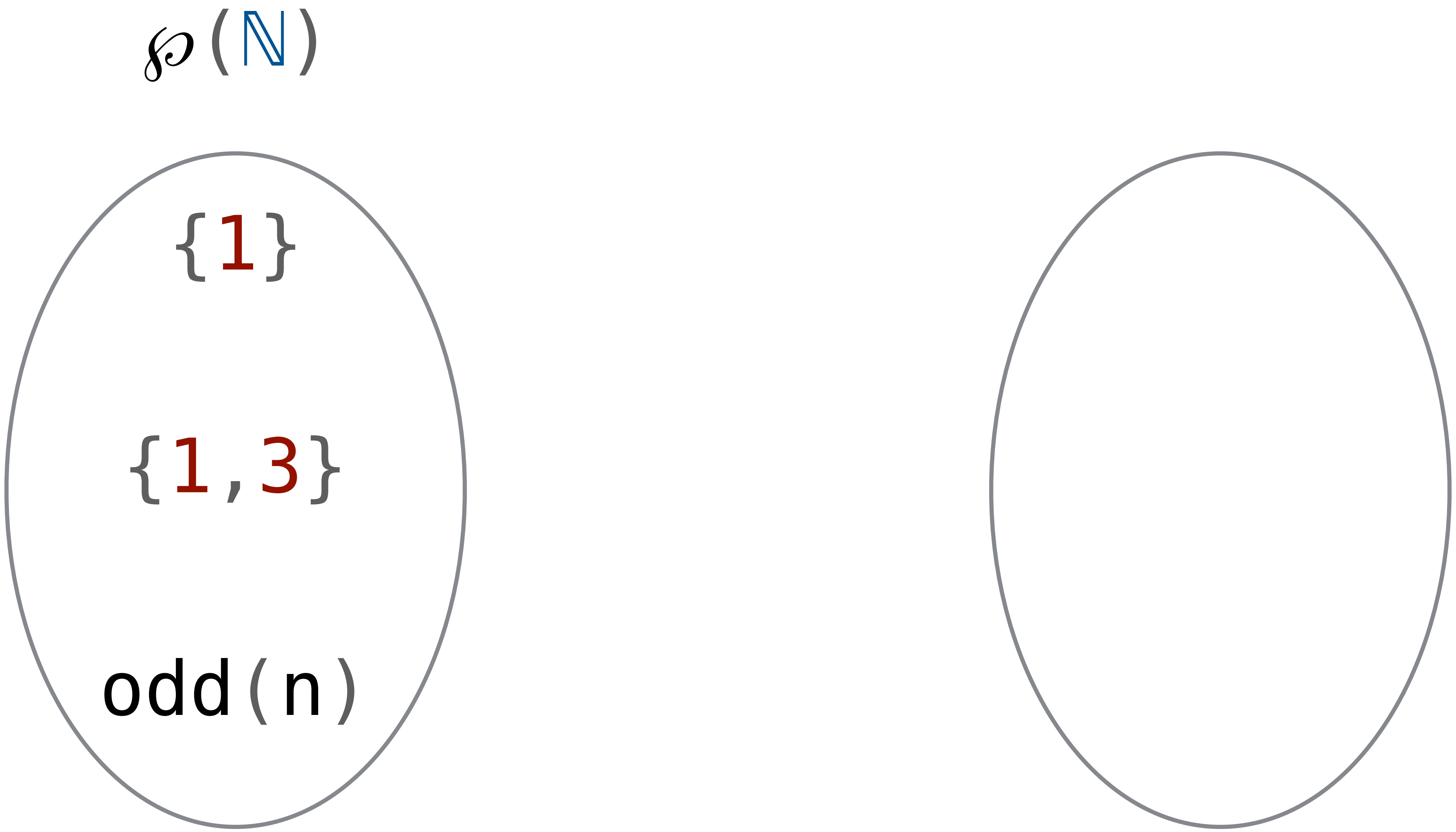
Four Stories

Direct Verification	✗ `calculate`
Abstract Interpretation	✗ `mechanize`
Kleisli GCs	✓ `calculate` ½ `mechanize`
Constructive GCs	✓ `calculate` ✓ `mechanize`

Abstract Interpretation

Abstract Interpretation

Abstract Interpretation



Abstract Interpretation

$\wp(\mathbb{N})$

{1}

{1,3}

odd(n)

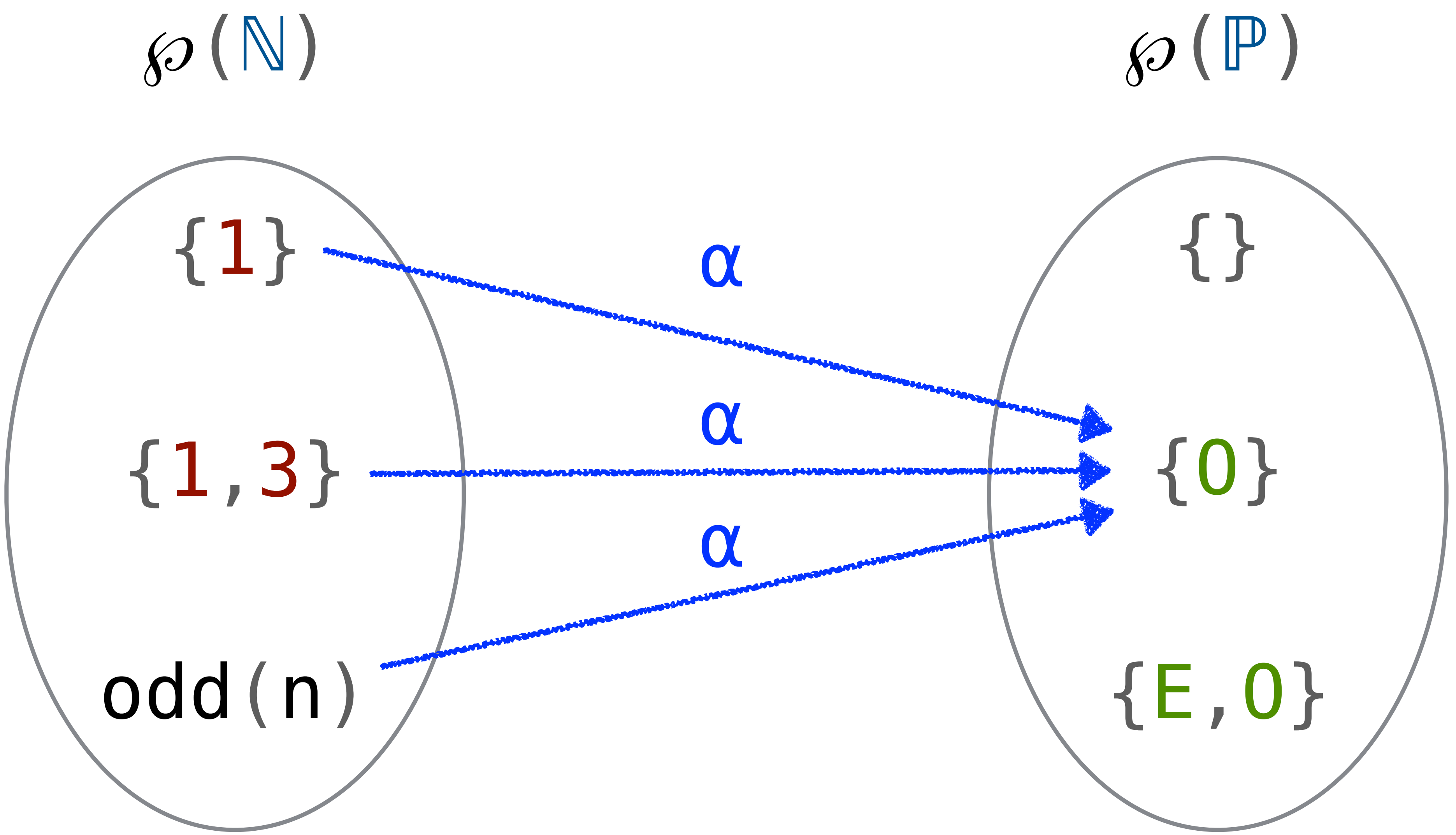
$\wp(\mathbb{P})$

{}

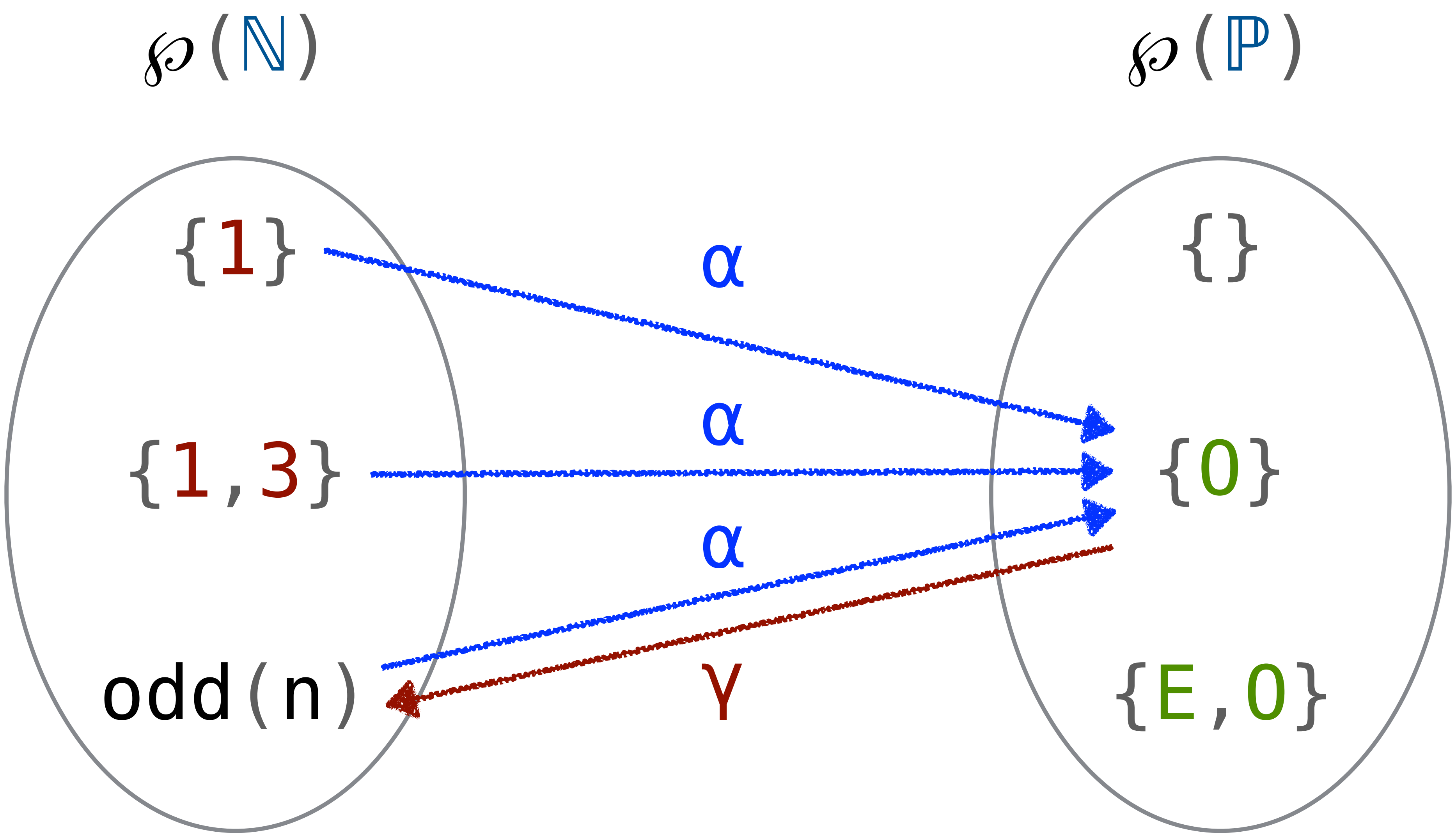
{O}

{E,O}

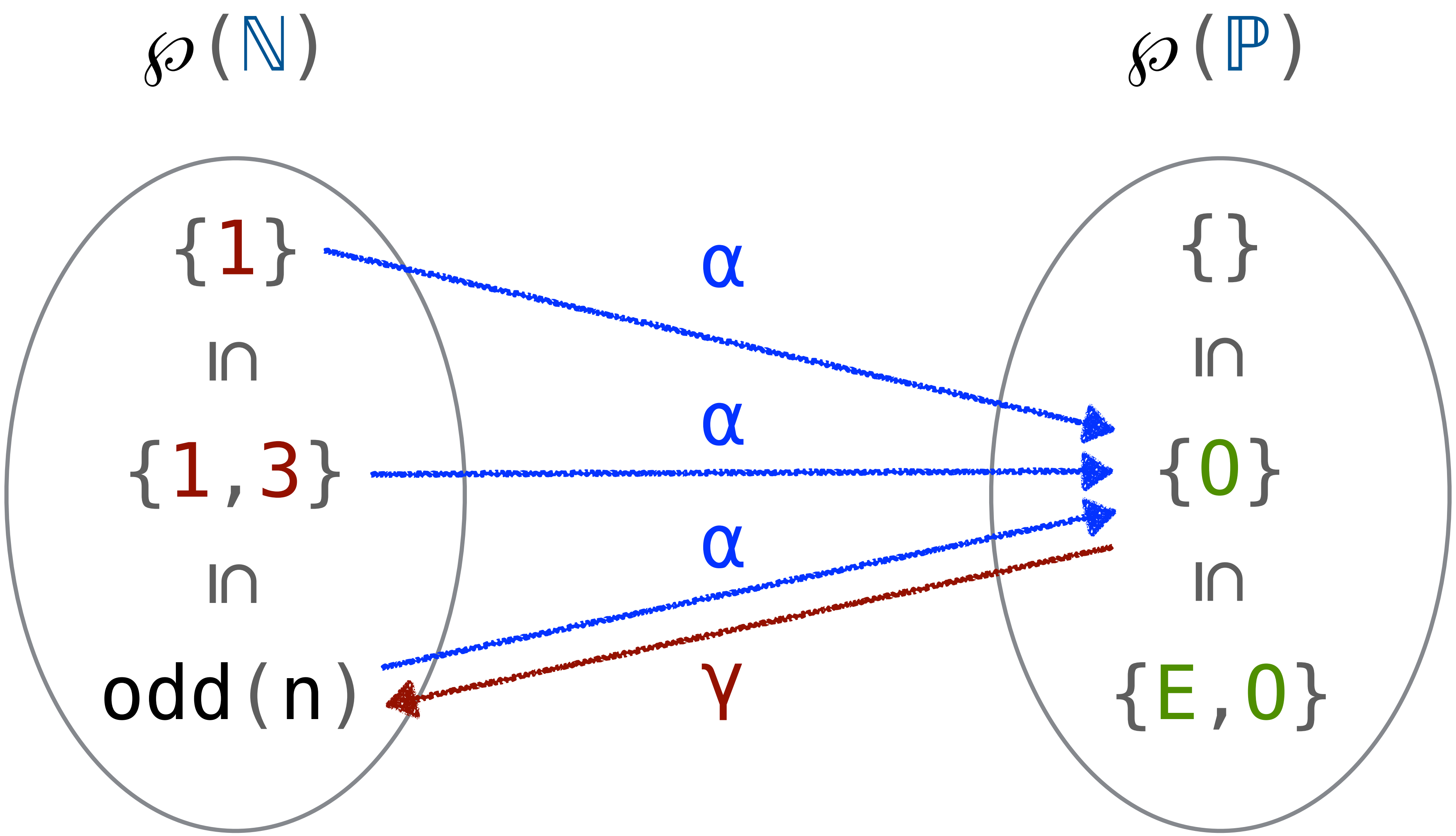
Abstract Interpretation



Abstract Interpretation

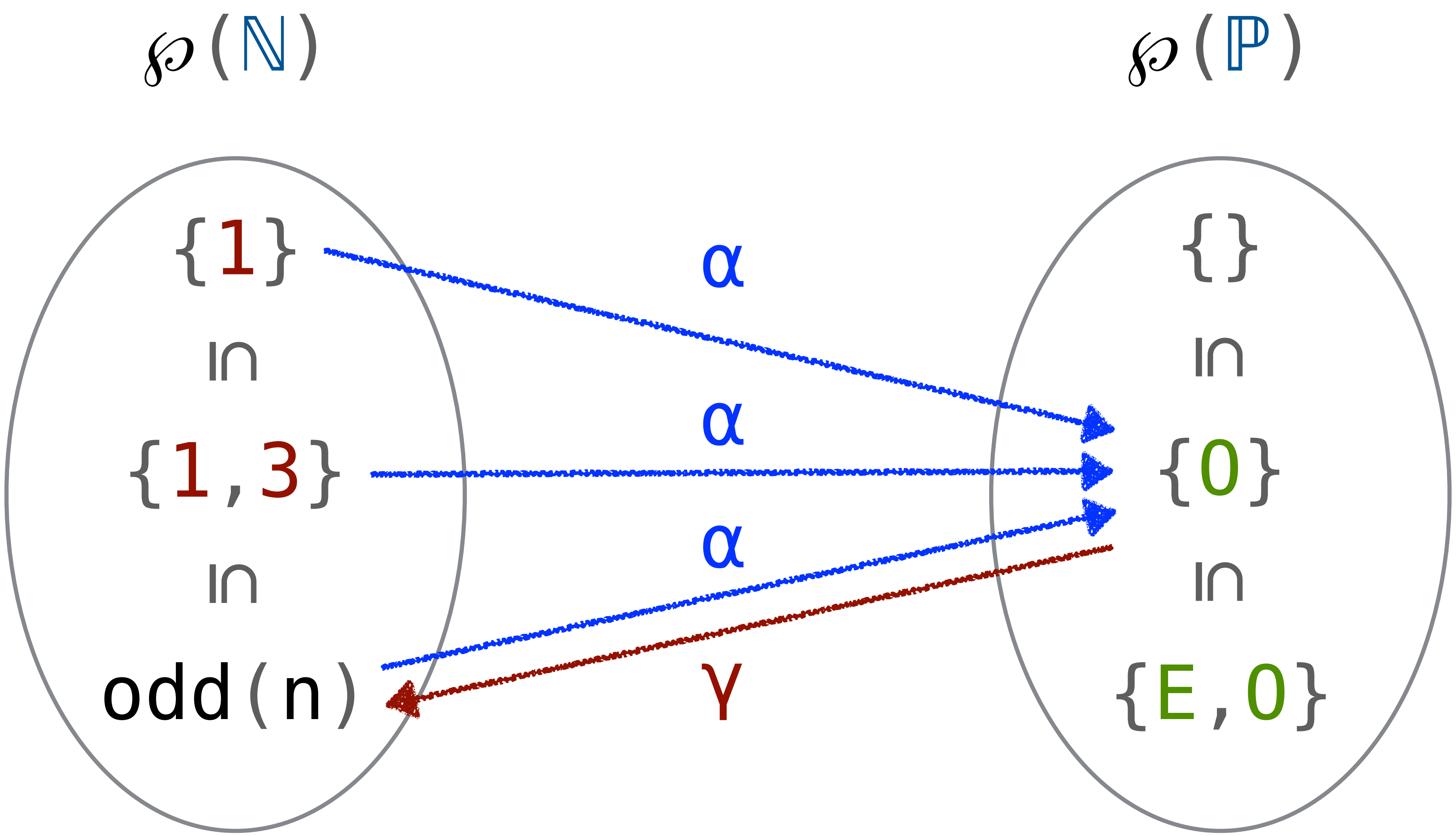


Abstract Interpretation



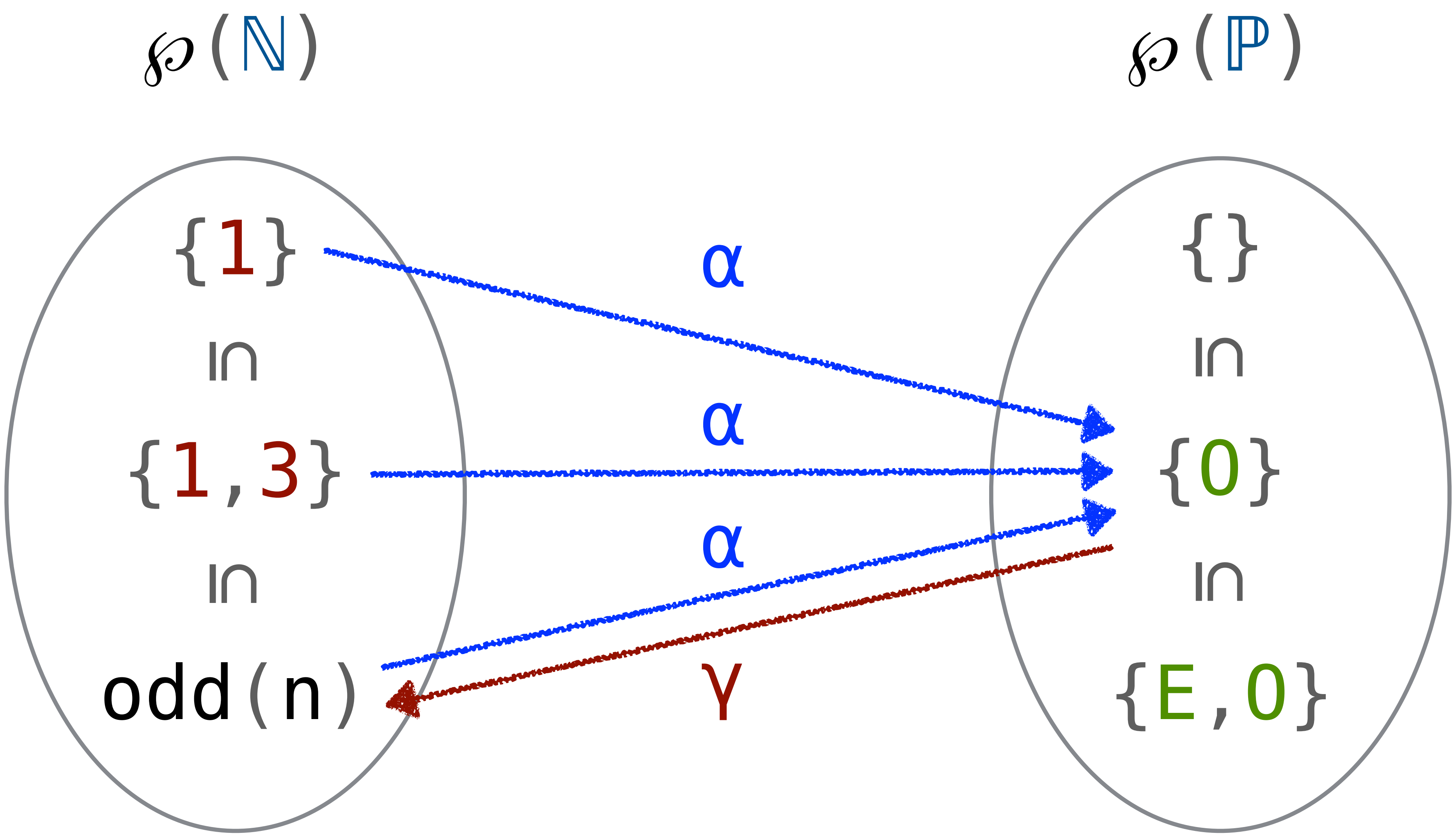
$N \subseteq \gamma(\alpha(N))$

Abstract Interpretation



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

Abstract Interpretation



$$\frac{N \subseteq \gamma(\alpha(N)) \quad \wedge \quad \alpha(\gamma(P)) \subseteq P}{N \subseteq \gamma(P) \iff \alpha(N) \subseteq P}$$

Abstract Interpretation

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

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

"**P** is sound for **N**"

$$\alpha(\mathbf{N}) \subseteq \mathbf{P}$$

Abstract Interpretation

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

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

"f^{P} is sound for f^{N}"

$$\alpha \circ f^{N} \circ \gamma \sqsubseteq f^{P}$$

Abstract Interpretation

```
α : ℘(ℕ) → ℘(ℙ)
α(N) ≔ {parity(n) | n ∈ N}
```

Abstract Interpretation

$$\alpha : \wp(\mathbb{N}) \to \wp(\mathbb{P})$$
$$\alpha(N) \coloneqq \{\mathrm{parity}(n) \mid n \in N\}$$

$$\gamma : \wp(\mathbb{P}) \to \wp(\mathbb{N})$$
$$\gamma(P) \coloneqq \{n \mid p \in P \land n \in [\![p]\!]\}$$

Abstract Interpretation

$\alpha : \wp(\mathbb{N}) \rightarrow \wp(\mathbb{P})$
$\alpha(N) \coloneqq \{parity(n) \mid n \in N\}$

$\alpha \approx map(parity)$

$\gamma : \wp(\mathbb{P}) \rightarrow \wp(\mathbb{N})$
$\gamma(P) \coloneqq \{n \mid p \in P \wedge n \in [\![p]\!]\}$

$\gamma \approx extend([\![\_]\!])$

Abstract Interpretation

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

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

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

$\texttt{flip} : \mathbb{P} \rightarrow \mathbb{P}$

Abstract Interpretation

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

$$\mathtt{succ} : \mathbb{N} \to \mathbb{N}$$
$$\mathtt{flip} : \mathbb{P} \to \mathbb{P}$$

$$\uparrow\mathtt{succ} : \wp(\mathbb{N}) \to \wp(\mathbb{N})$$
$$\uparrow\mathtt{succ}(\mathtt{N}) \coloneqq \{\mathtt{succ}(\mathtt{n}) \mid \mathtt{n} \in \mathtt{N}\}$$

$$\uparrow\mathtt{flip} : \wp(\mathbb{P}) \to \wp(\mathbb{P})$$
$$\uparrow\mathtt{flip}(\mathtt{P}) \coloneqq \{\mathtt{flip}(\mathtt{p}) \mid \mathtt{p} \in \mathtt{P}\}$$

Abstract Interpretation

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

$\mathtt{succ} : \mathbb{N} \to \mathbb{N}$
$\mathtt{flip} : \mathbb{P} \to \mathbb{P}$

$\uparrow\mathtt{succ} : \wp(\mathbb{N}) \to \wp(\mathbb{N})$
$\uparrow\mathtt{succ}(N) \coloneqq \{\mathtt{succ}(n) \mid n \in N\}$

$\uparrow\mathtt{flip} : \wp(\mathbb{P}) \to \wp(\mathbb{P})$
$\uparrow\mathtt{flip}(P) \coloneqq \{\mathtt{flip}(p) \mid p \in P\}$

$\boxed{\mathtt{sound} : \alpha(\uparrow\mathtt{succ}(\gamma(P))) \subseteq \uparrow\mathtt{flip}(P)}$

Abstract Interpretation

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

$\mathtt{succ} : \mathbb{N} \to \mathbb{N}$
$\mathtt{flip} : \mathbb{P} \to \mathbb{P}$

$\uparrow\mathtt{succ} : \wp(\mathbb{N}) \to \wp(\mathbb{N})$
$\uparrow\mathtt{succ}(N) \coloneqq \{\mathtt{succ}(n) \mid n \in N\}$

$\uparrow\mathtt{flip} : \wp(\mathbb{P}) \to \wp(\mathbb{P})$
$\uparrow\mathtt{flip}(P) \coloneqq \{\mathtt{flip}(p) \mid p \in P\}$

sound	$: \alpha(\uparrow\mathtt{succ}(\gamma(P))) \subseteq \uparrow\mathtt{flip}(P)$
optimal	$: \alpha(\uparrow\mathtt{succ}(\gamma(P))) = \uparrow\mathtt{flip}(P)$

Abstract Interpretation

```
optimal : α(↑succ(γ(P))) = ↑flip(P)
```

Abstract Interpretation

```
calc : α(↑succ(γ(P))) = … ≜ ↑flip(P)
```

Abstract Interpretation

$\boxed{\texttt{calc : } \alpha(\uparrow\texttt{succ}(\gamma(\texttt{P}))) = \ldots \triangleq \uparrow\texttt{flip}(\texttt{P})}$

$\alpha(\uparrow\texttt{succ}(\gamma(\{\texttt{E}\})))$

Abstract Interpretation

```
calc : α(↑succ(γ(P))) = … ≜ ↑flip(P)
```

```
α(↑succ(γ({E})))
= α(↑succ({n | even(n)}))
```

Abstract Interpretation

$\boxed{\texttt{calc : } \alpha(\uparrow\texttt{succ}(\gamma(\texttt{P}))) = \ldots \triangleq \uparrow\texttt{flip}(\texttt{P})}$

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

Abstract Interpretation

$\boxed{\texttt{calc : } \alpha(\uparrow\texttt{succ}(\gamma(\texttt{P}))) = \dots \triangleq \uparrow\texttt{flip}(\texttt{P})}$

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

Abstract Interpretation

```
calc : α(↑succ(γ(P))) = … ≜ ↑flip(P)
```

```
α(↑succ(γ({E})))
= α(↑succ({n | even(n)}))
= α({succ(n) | even(n)})
= α({n | odd(n)})
= {O}
```

Abstract Interpretation

$\boxed{\texttt{calc} : \alpha(\uparrow\mathrm{succ}(\gamma(P))) = \ldots \triangleq \uparrow\mathrm{flip}(P)}$

$$
\begin{aligned}
& \alpha(\uparrow\mathrm{succ}(\gamma(\{E\}))) \\
= \;& \alpha(\uparrow\mathrm{succ}(\{n \mid \mathrm{even}(n)\})) \\
= \;& \alpha(\{\mathrm{succ}(n) \mid \mathrm{even}(n)\}) \\
= \;& \alpha(\{n \mid \mathrm{odd}(n)\}) \\
= \;& \{O\} \\
\triangleq \;& \uparrow\mathrm{flip}(\{E\})
\end{aligned}
$$

Abstract Interpretation

$$\wp(\mathbb{P}) \quad \mapsto \quad \ldots \quad \mapsto \quad \wp(\mathbb{P})$$

```
calc : α(↑succ(γ(P))) = … ≜ ↑flip(P)
```

Abstract Interpretation

$$\wp(\mathbb{P}) \quad \mapsto \quad \ldots \quad \mapsto \quad \wp(\mathbb{P})$$

$$\boxed{\texttt{calc : } \alpha(\uparrow\texttt{succ}(\gamma(\texttt{P}))) = \ldots \triangleq \uparrow\texttt{flip}(\texttt{P})}$$

$$\wp(\mathbb{P}) \coloneqq (\mathbb{P} \to \texttt{prop}) \approx \text{“}\texttt{specification}\text{”}$$
$$\wp(\mathbb{P}) \coloneqq \{\mathbb{P}\} \approx \text{“}\texttt{constructed}\text{”}$$

Abstract Interpretation

✓ Optimal specifications

✓ Calculational framework

✗ Requires axioms

✗ Definitions don't compute

Four Stories

Direct Verification	✗ calculate
Abstract Interpretation	✗ mechanize
Kleisli GCs	✓ calculate ½ mechanize
Constructive GCs	✓ calculate ✓ mechanize

Kleisli GCs

$$\alpha : \wp(\mathbb{N}) \to \wp(\mathbb{P}) \qquad \uparrow\mathtt{succ} : \wp(\mathbb{N}) \to \wp(\mathbb{N})$$

$$\gamma : \wp(\mathbb{P}) \to \wp(\mathbb{N}) \qquad \uparrow\mathtt{flip} : \wp(\mathbb{P}) \to \wp(\mathbb{P})$$

Kleisli GCs

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

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

$\uparrow\mathtt{succ} : \mathbb{N} \to \wp(\mathbb{N})$

$\uparrow\mathtt{flip} : \mathbb{P} \to \wp(\mathbb{P})$

Kleisli GCs

$$\alpha : \mathbb{N} \to \mathbb{P} \to \mathtt{prop} \qquad {\uparrow}\mathtt{succ} : \mathbb{N} \to \mathbb{N} \to \mathtt{prop}$$
$$\gamma : \mathbb{P} \to \mathbb{N} \to \mathtt{prop} \qquad {\uparrow}\mathtt{flip} : \mathbb{P} \to \mathbb{P} \to \mathtt{prop}$$

$$\wp(X) \coloneqq X \to \mathtt{prop}$$

Kleisli GCs

$$\alpha : \mathbb{N} \to \wp(\mathbb{P}) \qquad\qquad \uparrow\mathtt{succ} : \mathbb{N} \to \wp(\mathbb{N})$$

$$\gamma : \mathbb{P} \to \wp(\mathbb{N}) \qquad\qquad \uparrow\mathtt{flip} : \mathbb{P} \to \wp(\mathbb{P})$$

Kleisli GCs

$$\alpha : \mathbb{N} \rightarrow \wp(\mathbb{P}) \qquad\qquad \uparrow\mathtt{succ} : \mathbb{N} \rightarrow \wp(\mathbb{N})$$

$$\gamma : \mathbb{P} \rightarrow \wp(\mathbb{N}) \qquad\qquad \uparrow\mathtt{flip} : \mathbb{P} \rightarrow \wp(\mathbb{P})$$

$$\boxed{\dfrac{N \subseteq \gamma(\alpha(N)) \quad \wedge \quad \alpha(\gamma(P)) \subseteq P}{N \subseteq \gamma(P) \Leftrightarrow \alpha(N) \subseteq P}}$$

Kleisli GCs

$$\alpha : \mathbb{N} \to \wp(\mathbb{P}) \qquad \uparrow\mathrm{succ} : \mathbb{N} \to \wp(\mathbb{N})$$

$$\gamma : \mathbb{P} \to \wp(\mathbb{N}) \qquad \uparrow\mathrm{flip} : \mathbb{P} \to \wp(\mathbb{P})$$

$$\boxed{\dfrac{\mathrm{id} \sqsubseteq \gamma \circ \alpha \quad \wedge \quad \alpha \circ \gamma \sqsubseteq \mathrm{id}}{\mathrm{id}(N) \subseteq \gamma(P) \iff \alpha(N) \subseteq \mathrm{id}(P)}}$$

Kleisli GCs

$$\alpha : \mathbb{N} \to \wp(\mathbb{P}) \qquad \uparrow\mathtt{succ} : \mathbb{N} \to \wp(\mathbb{N})$$

$$\gamma : \mathbb{P} \to \wp(\mathbb{N}) \qquad \uparrow\mathtt{flip} : \mathbb{P} \to \wp(\mathbb{P})$$

$$\boxed{\dfrac{\mathtt{ret} \sqsubseteq \gamma \circledast \alpha \quad \wedge \quad \alpha \circledast \gamma \sqsubseteq \mathtt{ret}}{\mathtt{ret}(n) \subseteq \gamma(p) \iff \alpha(n) \subseteq \mathtt{ret}(p)}}$$

Kleisli GCs

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

$$\uparrow\texttt{succ} : \mathbb{N} \rightarrow \wp(\mathbb{N})$$
$$\uparrow\texttt{flip} : \mathbb{P} \rightarrow \wp(\mathbb{P})$$

$$\boxed{\dfrac{\texttt{ret} \sqsubseteq \gamma \circledast \alpha \quad \wedge \quad \alpha \circledast \gamma \sqsubseteq \texttt{ret}}{\texttt{ret}(n) \subseteq \gamma(p) \Leftrightarrow \alpha(n) \subseteq \texttt{ret}(p)}}$$

$$\boxed{\texttt{sound} : \alpha \circ \uparrow\texttt{succ} \circ \gamma \sqsubseteq \uparrow\texttt{flip}}$$

Kleisli GCs

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

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

$\uparrow\mathtt{succ} : \mathbb{N} \to \wp(\mathbb{N})$

$\uparrow\mathtt{flip} : \mathbb{P} \to \wp(\mathbb{P})$

$$\frac{\mathtt{ret} \sqsubseteq \gamma \circledast \alpha \quad \wedge \quad \alpha \circledast \gamma \sqsubseteq \mathtt{ret}}{\mathtt{ret}(n) \subseteq \gamma(p) \iff \alpha(n) \subseteq \mathtt{ret}(p)}$$

$\mathtt{sound} : \alpha \circledast \uparrow\mathtt{succ} \circledast \gamma \sqsubseteq \uparrow\mathtt{flip}$

Kleisli GCs

✓ Optimal specifications

✓ Calculational framework

✓ No axioms

✗ Definitions don't compute

Four Stories

Direct Verification	✗ `calculate`
Abstract Interpretation	✗ `mechanize`
Kleisli GCs	✓ `calculate` ½ `mechanize`
Constructive GCs	✓ `calculate` ✓ `mechanize`

Constructive GCs

$$\alpha : \mathbb{N} \rightarrow \wp(\mathbb{P}) \qquad\qquad \texttt{ret} \sqsubseteq \gamma \circledast \alpha$$
$$\wedge$$
$$\gamma : \mathbb{P} \rightarrow \wp(\mathbb{N}) \qquad\qquad \alpha \circledast \gamma \sqsubseteq \texttt{ret}$$

Constructive GCs

$$\alpha : \mathbb{N} \to \wp(\mathbb{P}) \qquad \qquad \text{ret} \sqsubseteq \gamma \circledast \alpha$$
$$\gamma : \mathbb{P} \to \wp(\mathbb{N}) \quad \wedge \quad \alpha \circledast \gamma \sqsubseteq \text{ret}$$

\- -

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

Constructive GCs

$$\alpha : \mathbb{N} \to \wp(\mathbb{P}) \qquad\qquad \mathrm{ret} \sqsubseteq \gamma \circledast \alpha$$
$$\gamma : \mathbb{P} \to \wp(\mathbb{N}) \quad \wedge \quad \alpha \circledast \gamma \sqsubseteq \mathrm{ret}$$

\- -

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

constructive

Constructive GCs

$$\alpha \;:\; \mathbb{N} \to \wp(\mathbb{P})$$
$$\gamma \;:\; \mathbb{P} \to \wp(\mathbb{N})$$

Constructive GCs

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

Constructive GCs

$$\texttt{parity} : \mathbb{N} \to \mathbb{P}$$
$$[\![\_]\!] : \mathbb{P} \to \wp(\mathbb{N})$$

Constructive GCs

$$\mathtt{parity} : \mathbb{N} \to \mathbb{P}$$
$$[\![\_]\!] : \mathbb{P} \to \wp(\mathbb{N})$$

$$n \in [\![\mathtt{parity}(n)]\!]$$

Constructive GCs

$$\text{parity} : \mathbb{N} \to \mathbb{P}$$
$$[\![\_]\!] : \mathbb{P} \to \wp(\mathbb{N})$$

$$n \in [\![\text{parity}(n)]\!] \quad \wedge \quad n \in [\![p]\!] \Rightarrow \text{parity}(n) \sqsubseteq p$$

Constructive GCs

$$\text{parity} : \mathbb{N} \to \mathbb{P}$$
$$[\![\_]\!] : \mathbb{P} \to \wp(\mathbb{N})$$

$$\frac{n \in [\![\text{parity}(n)]\!] \quad \wedge \quad n \in [\![p]\!] \Rightarrow \text{parity}(n) \sqsubseteq p}{n \in [\![p]\!] \iff \text{parity}(n) \sqsubseteq p}$$

Constructive GCs

$$\text{parity} : \mathbb{N} \to \mathbb{P}$$
$$[\![\_]\!] : \mathbb{P} \to \wp(\mathbb{N})$$

$$\frac{n \in [\![\text{parity}(n)]\!] \quad \wedge \quad n \in [\![p]\!] \Rightarrow \text{parity}(n) \sqsubseteq p}{n \in [\![p]\!] \Leftrightarrow \text{parity}(n) \sqsubseteq p}$$

$$\text{sound} : n \in [\![p]\!] \Longrightarrow \text{parity}(\text{succ}(n)) \sqsubseteq \text{flip}(p)$$

Constructive GCs

- ✓ Optimal specifications
- ✓ Calculational framework
- ✓ No Axioms
- ✓ Definitions that compute

And More

And More

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

And More

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

And More

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

And More

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

And More

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

And More

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

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

$$\boxed{n \in \gamma(p) \iff \alpha(n) \sqsubseteq p}$$

✓ calculate
✓ mechanize