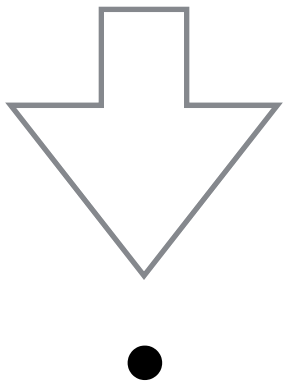
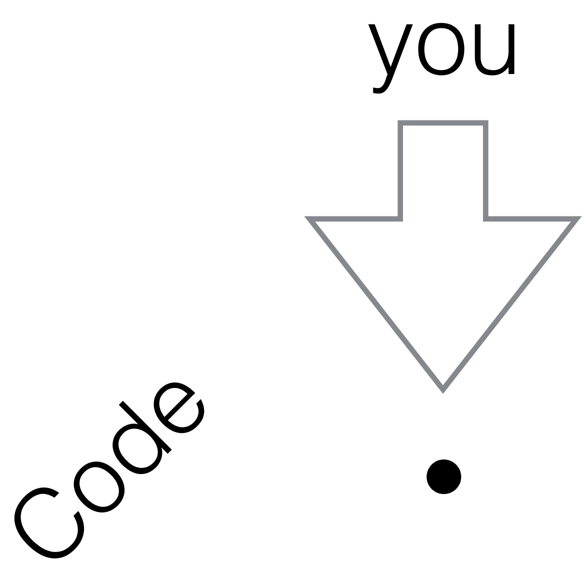
Constructive Galois Connections

David Darais
University of Maryland

David Van Horn
University of Maryland

you

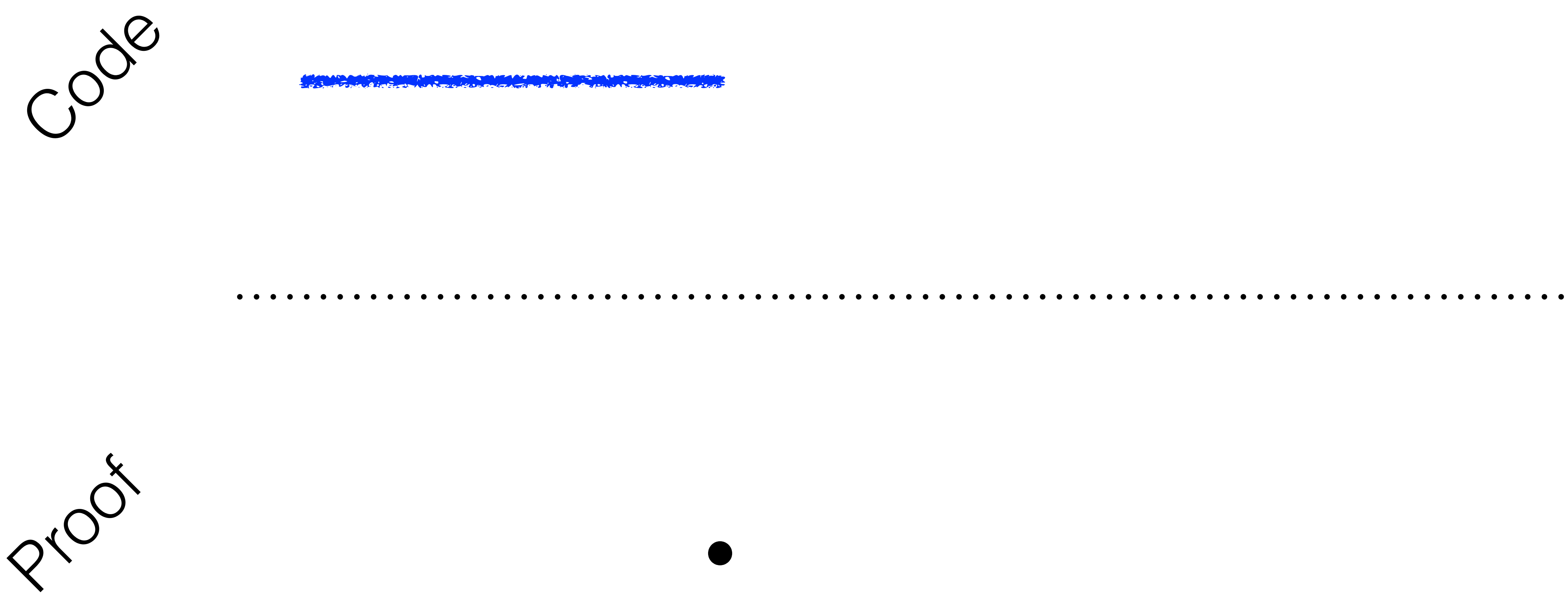


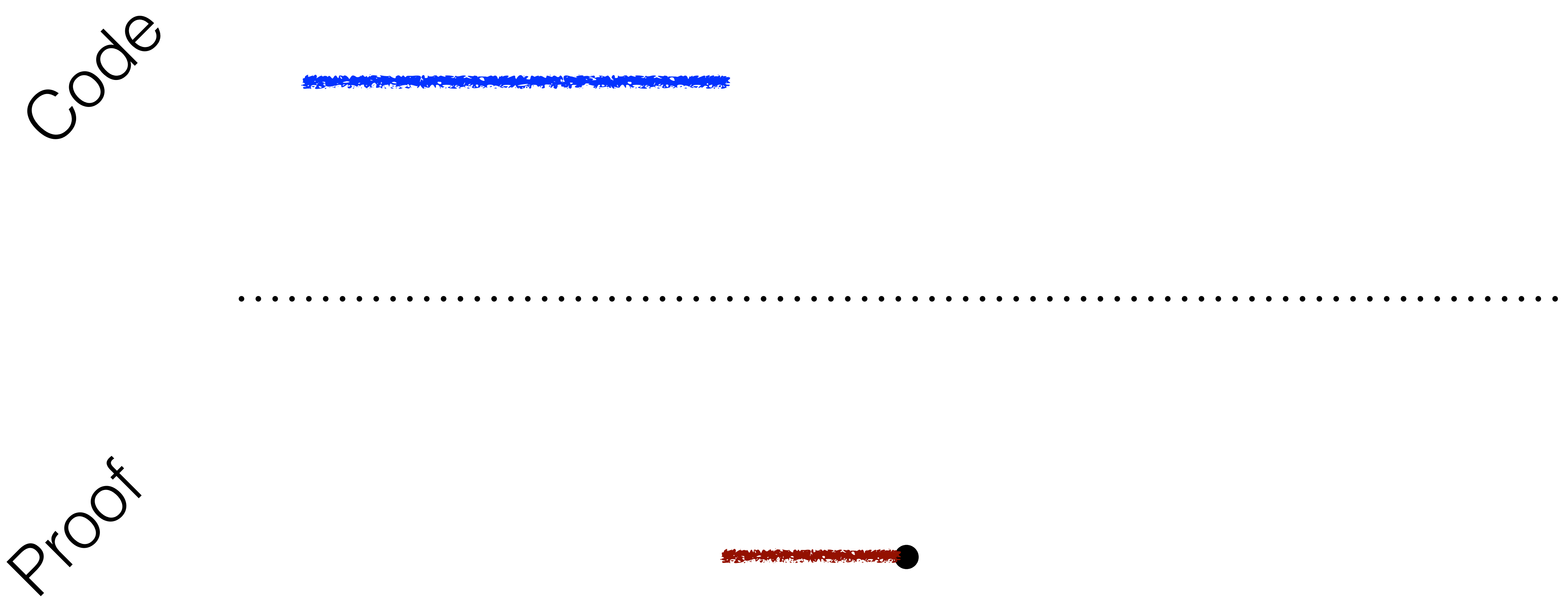

you
Code

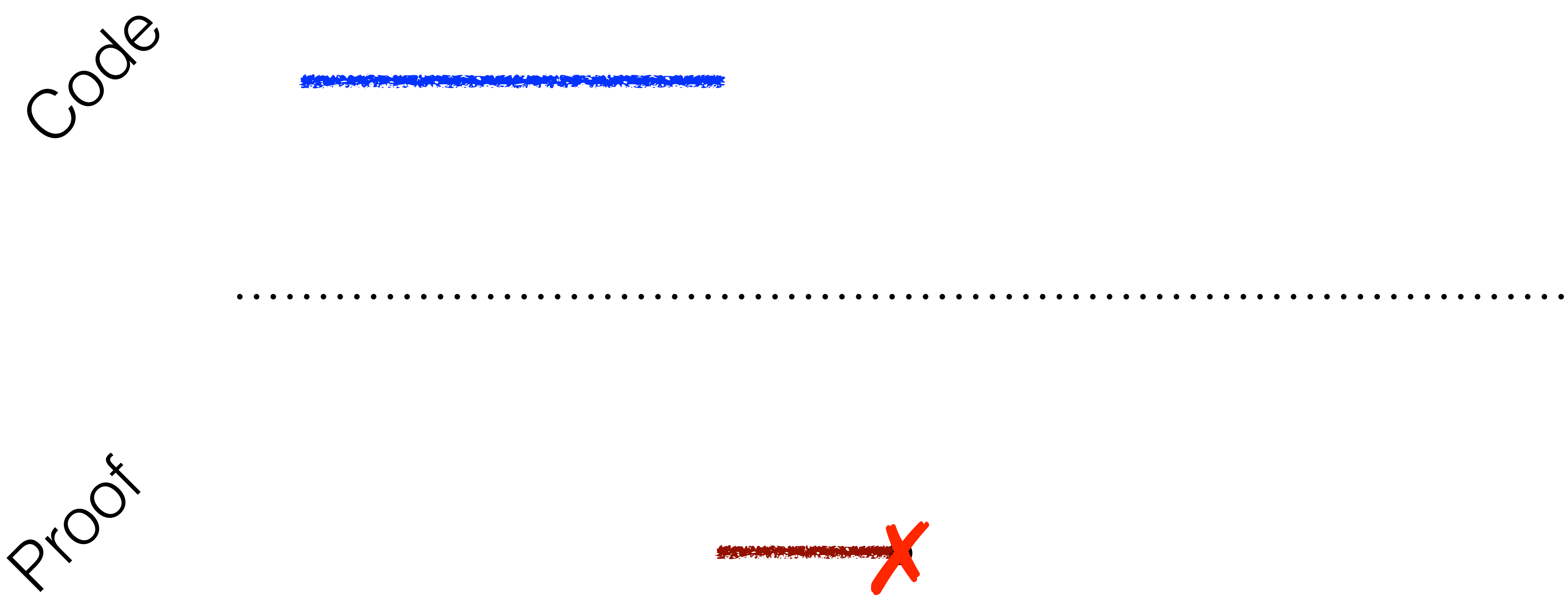

Code

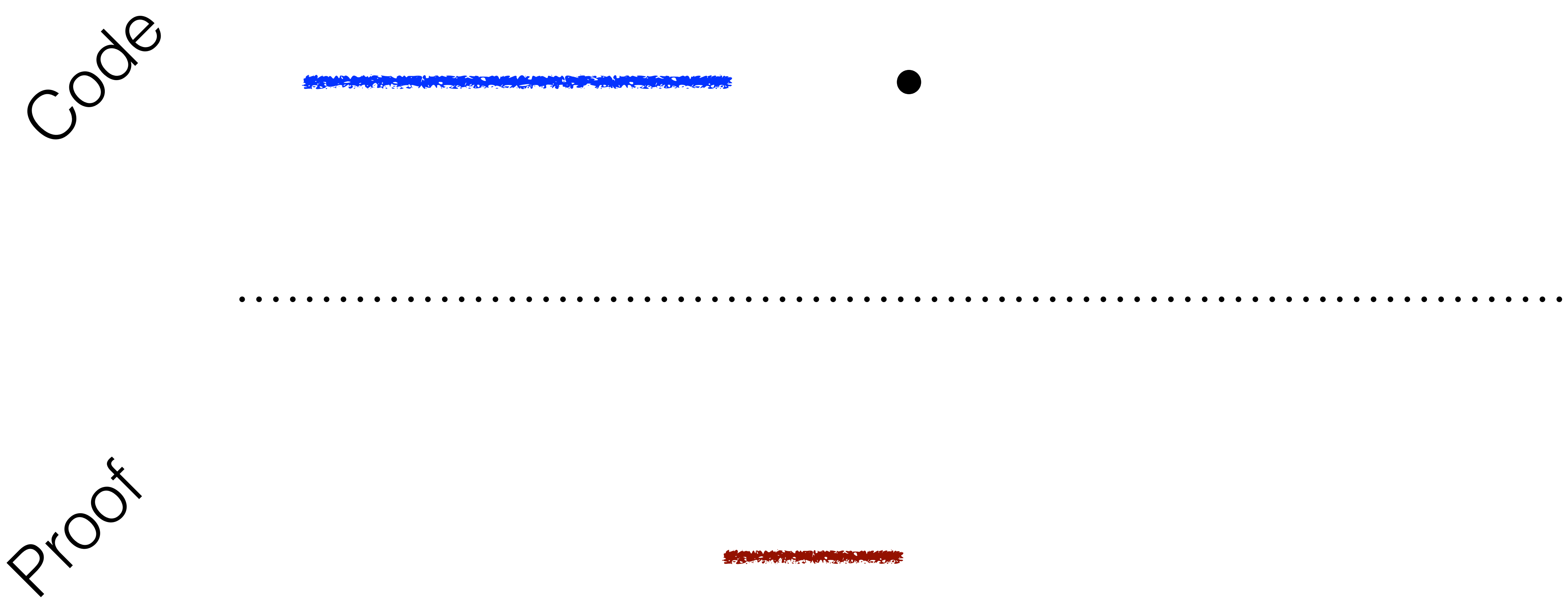
Code

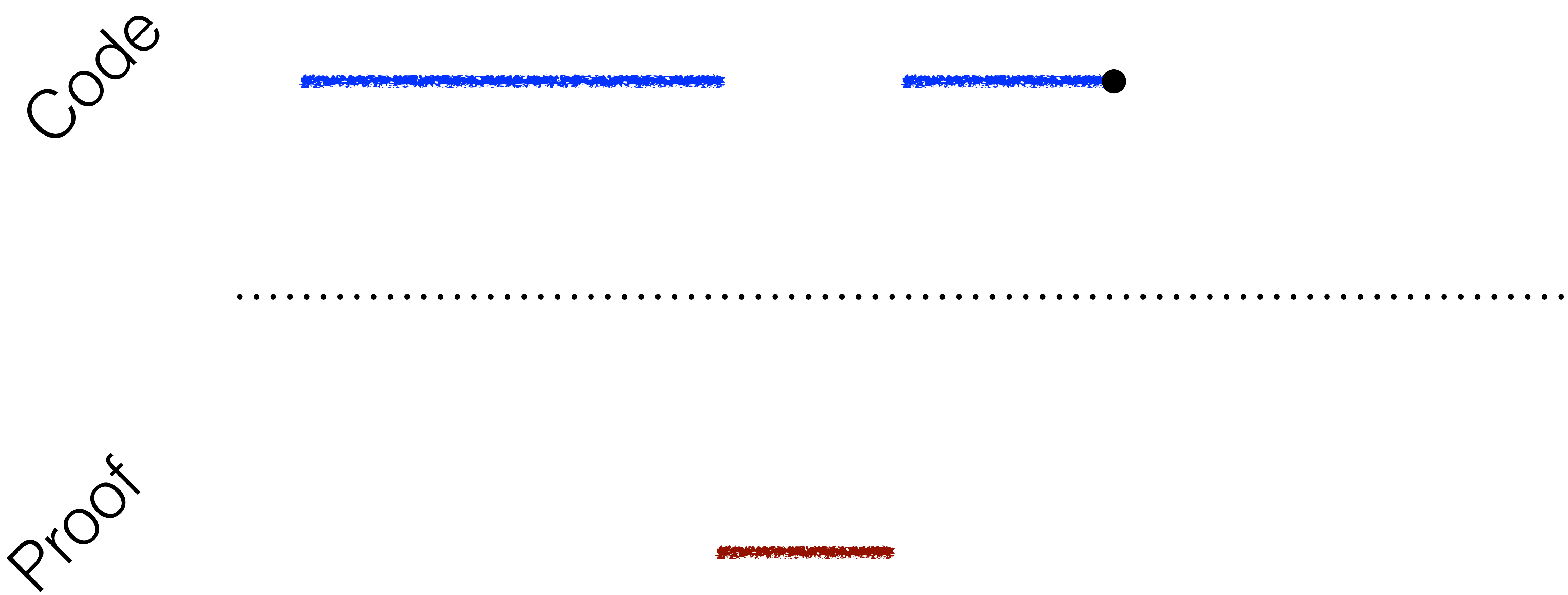
Proof

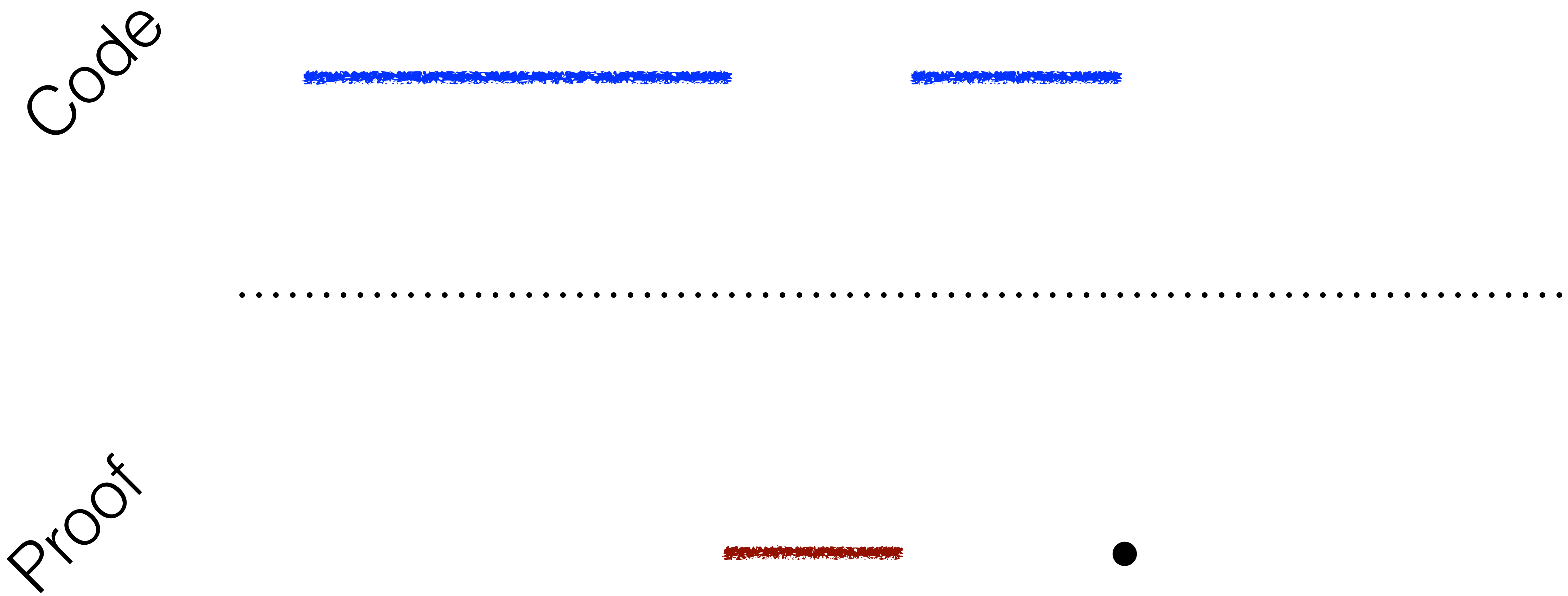

Code
Proof

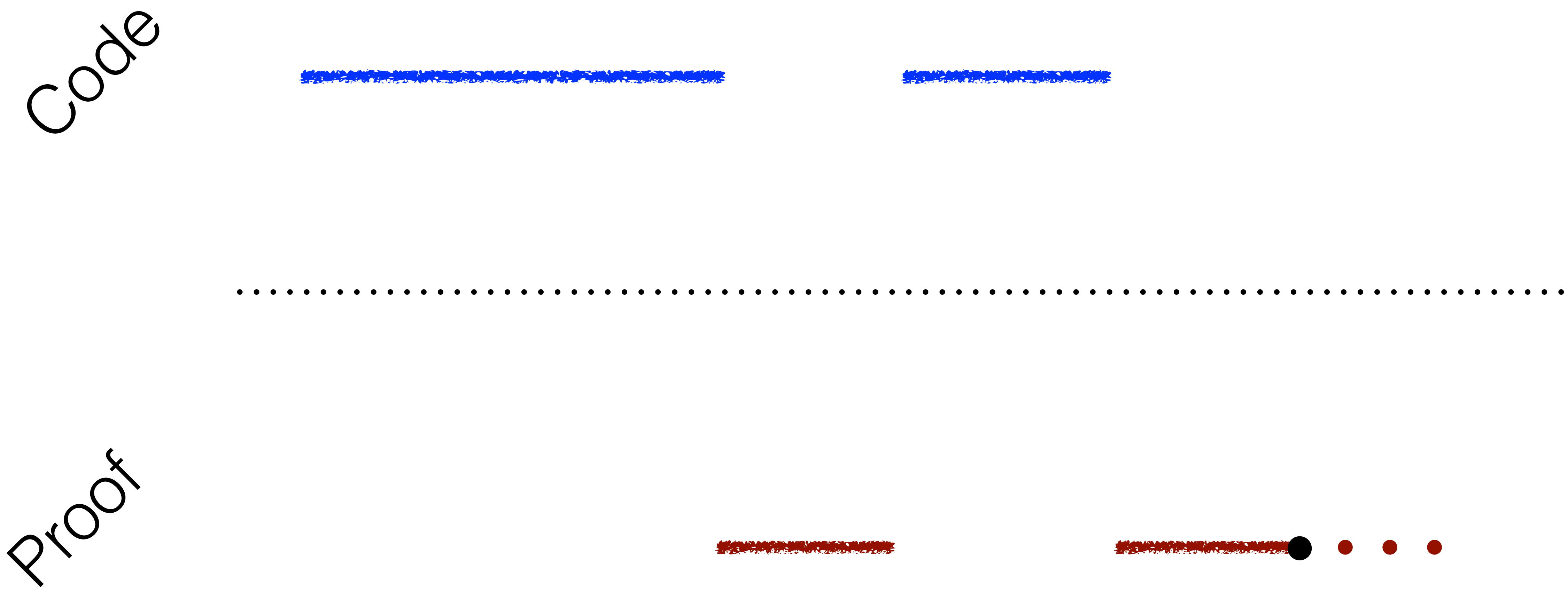

Code
Proof


Code
Proof


Code
Proof


Code
Proof


Code
Proof

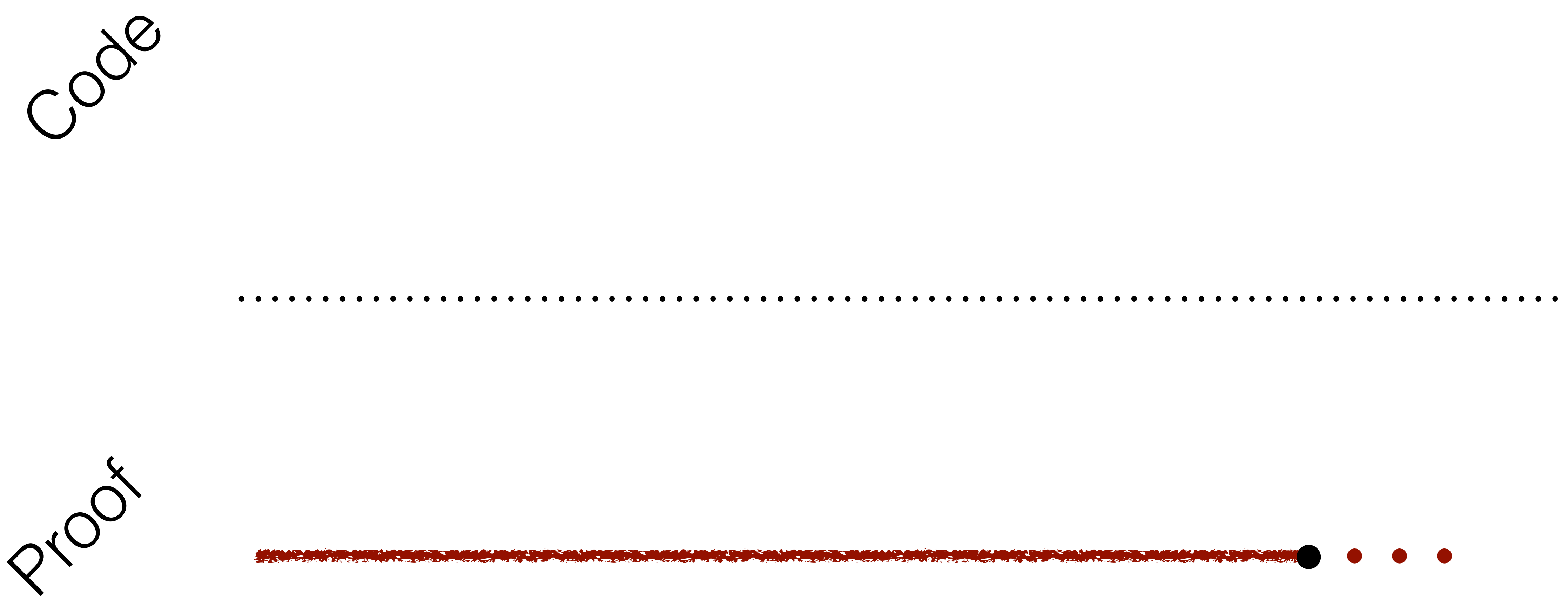

Code
Proof

Just write the proof

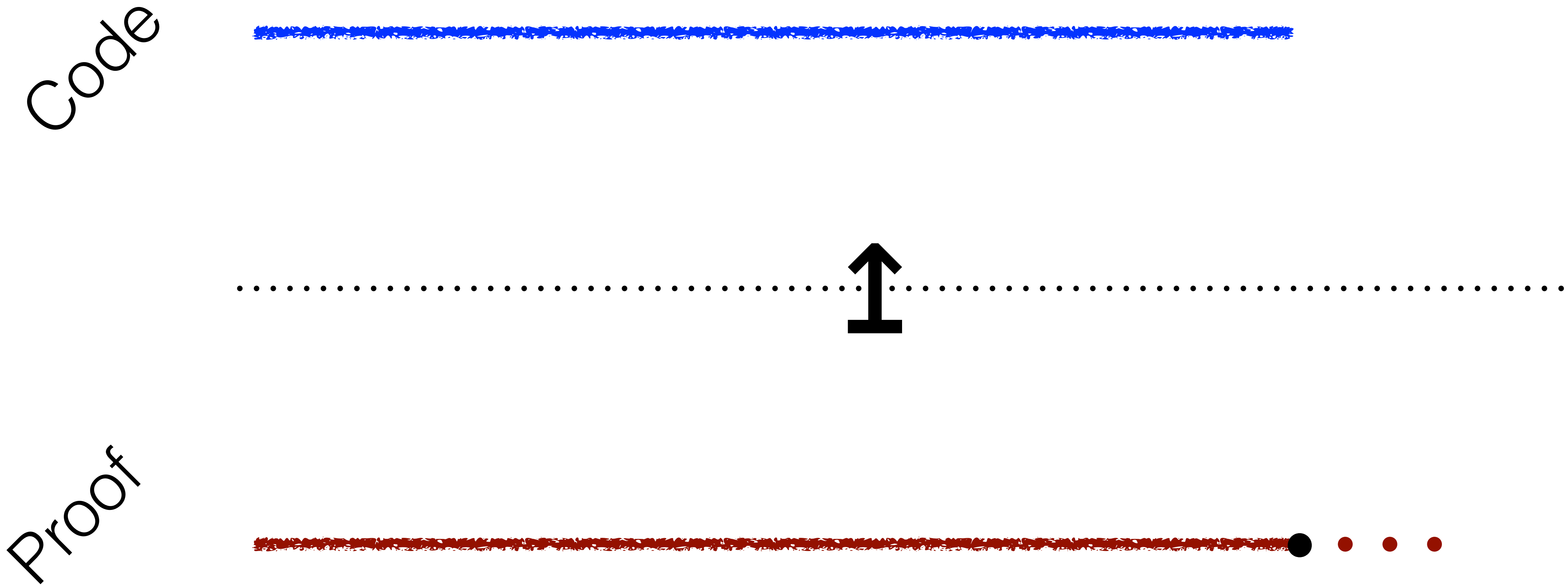
Code

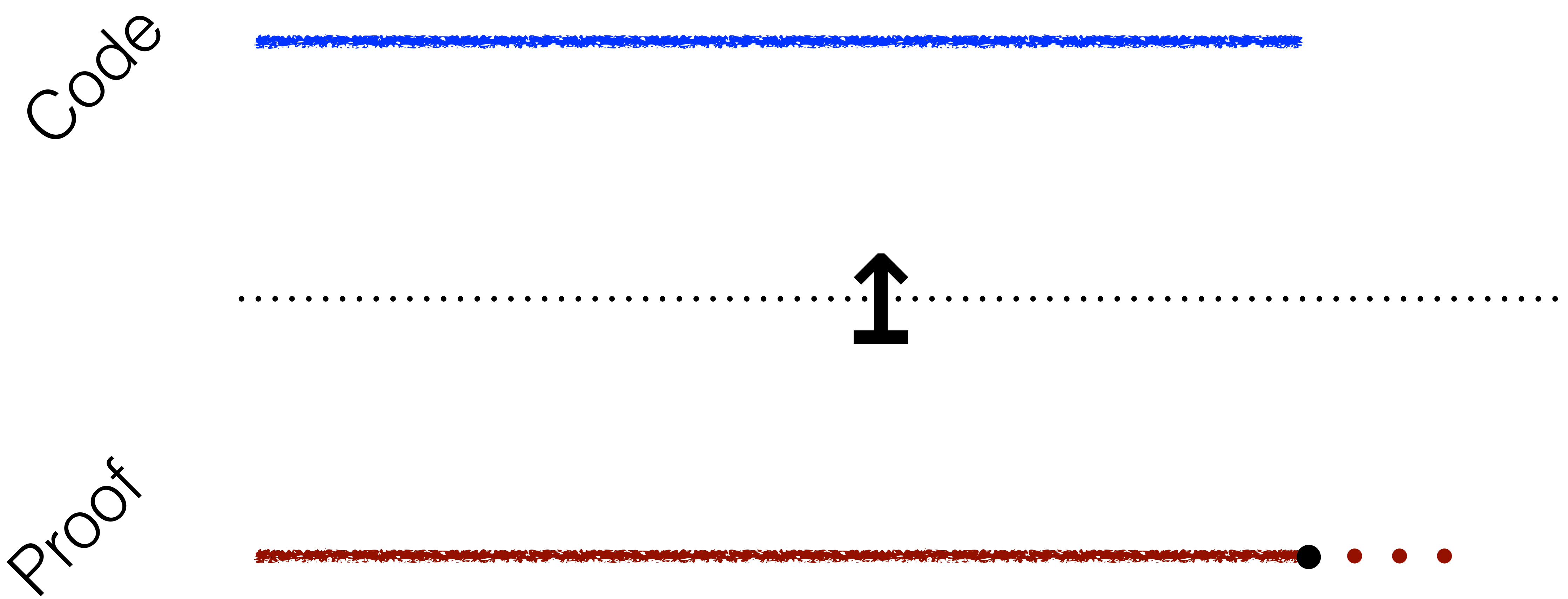
Proof

-

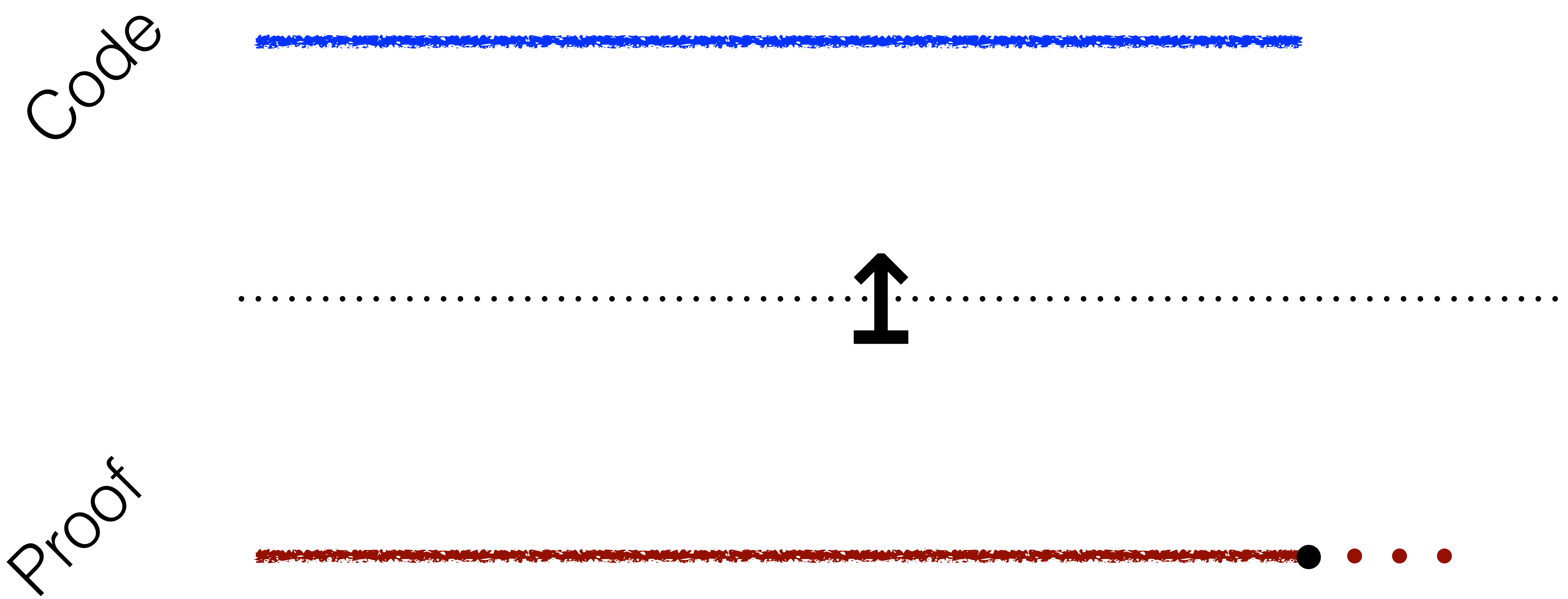


Code
Proof


Code
Proof



- Calculational Abstract Interpretation (spec $\mapsto$ alg)



- Calculational Abstract Interpretation (spec ↦ alg)
- Constructive Logic (proof ↦ code)

Abstract Interpretation and Constructive Logic don’t mix

(until now)

Three Stories

Three Stories

Direct Verification

✗ `framework`
✓ `mechanize`

Three Stories

Direct Verification	✗ `framework` ✓ `mechanize`
Abstract Interpretation	✓ `framework` ✗ `mechanize`

Three Stories

Direct Verification	✗ `framework` ✓ `mechanize`
Abstract Interpretation	✓ `framework` ✗ `mechanize`
Constructive GCs	✓ `framework` ✓ `mechanize`

Direct Verification

Direct Verification

```
succ  : ℕ → ℕ
```

Direct Verification

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

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

Direct Verification

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

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

$\mathtt{succ}^\sharp : \mathbb{P} \to \mathbb{P}$
$\mathtt{succ}^\sharp(\mathtt{E}) \coloneqq \mathtt{O}$
$\mathtt{succ}^\sharp(\mathtt{O}) \coloneqq \mathtt{E}$

Direct Verification

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

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

$$\begin{aligned} \mathtt{succ}^\sharp &: \mathbb{P} \to \mathbb{P} \\ \mathtt{succ}^\sharp(E) &\coloneqq O \\ \mathtt{succ}^\sharp(O) &\coloneqq E \end{aligned}$$

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

Direct Verification

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

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

$$\begin{aligned}
&\mathtt{succ}\sharp : \mathbb{P} \to \mathbb{P} \\
&\mathtt{succ}\sharp(\mathtt{E}) \coloneqq \mathtt{O} \\
&\mathtt{succ}\sharp(\mathtt{O}) \coloneqq \mathtt{E}
\end{aligned}$$

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

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

Direct Verification

```
succ♯ : ℙ → ℙ
succ♯(E) ≔ O
succ♯(O) ≔ E
```

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

Direct Verification

$$\wp(\mathbb{N}) \coloneqq \mathbb{N} \to \texttt{prop}$$

$$\begin{aligned}
&\texttt{succ}\sharp : \mathbb{P} \to \mathbb{P} \\
&\texttt{succ}\sharp(\texttt{E}) \coloneqq \texttt{O} \\
&\texttt{succ}\sharp(\texttt{O}) \coloneqq \texttt{E}
\end{aligned}$$

$$\begin{aligned}
&[\![_]\!] : \mathbb{P} \to \wp(\mathbb{N}) \\
&[\![\texttt{E}]\!] \coloneqq \{\ n \mid \texttt{even}(n)\ \} \\
&[\![\texttt{O}]\!] \coloneqq \{\ n \mid \texttt{odd}(n)\ \}
\end{aligned}$$

Direct Verification

$\wp(\mathbb{N}) \coloneqq \mathbb{N} \rightarrow \texttt{prop}$

$\texttt{succ}\sharp : \mathbb{P} \rightarrow \mathbb{P}$
$\texttt{succ}\sharp(\texttt{E}) \coloneqq \texttt{O}$
$\texttt{succ}\sharp(\texttt{O}) \coloneqq \texttt{E}$

$[\![\_]\!] : \mathbb{P} \rightarrow (\mathbb{N} \rightarrow \texttt{prop})$
$[\![\texttt{E}]\!] \coloneqq \{\ n \mid \texttt{even}(n)\ \}$
$[\![\texttt{O}]\!] \coloneqq \{\ n \mid \texttt{odd}(n)\ \}$

Direct Verification

$$\wp(\mathbb{N}) \coloneqq \mathbb{N} \to \mathtt{prop}$$

$$\begin{aligned} \mathtt{succ}^\sharp &: \mathbb{P} \to \mathbb{P} \\ \mathtt{succ}^\sharp(\mathtt{E}) &\coloneqq \mathtt{O} \\ \mathtt{succ}^\sharp(\mathtt{O}) &\coloneqq \mathtt{E} \end{aligned}$$

$$\begin{aligned} [\![\_]\!] &: \mathbb{P} \to (\mathbb{N} \to \mathtt{prop}) \\ [\![\mathtt{E}]\!] &\coloneqq \mathtt{even} \\ [\![\mathtt{O}]\!] &\coloneqq \mathtt{odd} \end{aligned}$$

Direct Verification

$\wp(\mathbb{N}) \coloneqq \mathbb{N} \to \mathtt{prop}$

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

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

succ$\sharp$ can be extracted and executed

Direct Verification

$\wp(\mathbb{N}) \coloneqq \mathbb{N} \to \texttt{prop}$

$\texttt{succ}^\sharp : \mathbb{P} \to \mathbb{P}$
$\texttt{succ}^\sharp(\texttt{E}) \coloneqq \texttt{O}$
$\texttt{succ}^\sharp(\texttt{O}) \coloneqq \texttt{E}$

$[\![\_]\!] : \mathbb{P} \to (\mathbb{N} \to \texttt{prop})$
$[\![\texttt{E}]\!] \coloneqq \texttt{even}$
$[\![\texttt{O}]\!] \coloneqq \texttt{odd}$

$\texttt{succ}^\sharp$ can be extracted and executed

$[\![\_]\!]$ can be defined constructively without axioms

Direct Verification

$\wp(\mathbb{N}) \coloneqq \mathbb{N} \rightarrow \texttt{prop}$

$\texttt{succ}\sharp : \mathbb{P} \rightarrow \mathbb{P}$
$\texttt{succ}\sharp(\texttt{E}) \coloneqq \texttt{O}$
$\texttt{succ}\sharp(\texttt{O}) \coloneqq \texttt{E}$

$[\![\_]\!] : \mathbb{P} \rightarrow (\mathbb{N} \rightarrow \texttt{prop})$
$[\![\texttt{E}]\!] \coloneqq \texttt{even}$
$[\![\texttt{O}]\!] \coloneqq \texttt{odd}$

$\textbf{succ}\sharp$ can be extracted and executed

$[\![\_]\!]$ can be defined constructively without axioms

Is $\textbf{succ}\sharp$ optimal? (why not $\texttt{succ}\sharp(\texttt{E}) \coloneqq \{\texttt{E},\texttt{O}\}$)

Direct Verification

$\wp(\mathbb{N}) \coloneqq \mathbb{N} \rightarrow \texttt{prop}$

$\texttt{succ}\sharp : \mathbb{P} \rightarrow \mathbb{P}$
$\texttt{succ}\sharp(\texttt{E}) \coloneqq \texttt{O}$
$\texttt{succ}\sharp(\texttt{O}) \coloneqq \texttt{E}$

$[\![\_]\!] : \mathbb{P} \rightarrow (\mathbb{N} \rightarrow \texttt{prop})$
$[\![\texttt{E}]\!] \coloneqq \texttt{even}$
$[\![\texttt{O}]\!] \coloneqq \texttt{odd}$

succ♯ can be extracted and executed

$[\![\_]\!]$ can be defined constructively without axioms

Is **succ**♯ optimal? (why not $\texttt{succ}\sharp(\texttt{E}) \coloneqq \{\texttt{E},\texttt{O}\}$)

Can one derive **succ**♯ from **succ** directly?

Direct Verification

$\wp(\mathbb{N}) \coloneqq \mathbb{N} \rightarrow \texttt{prop}$

$\texttt{succ}^\sharp : \mathbb{P} \rightarrow \mathbb{P}$
$\texttt{succ}^\sharp(\texttt{E}) \coloneqq \texttt{O}$
$\texttt{succ}^\sharp(\texttt{O}) \coloneqq \texttt{E}$

$[\![\_]\!] : \mathbb{P} \rightarrow (\mathbb{N} \rightarrow \texttt{prop})$
$[\![\texttt{E}]\!] \coloneqq \texttt{even}$
$[\![\texttt{O}]\!] \coloneqq \texttt{odd}$

$\mathbf{succ}^\sharp$ can be extracted and executed

$[\![\_]\!]$ can be defined constructively without axioms

✓ mechanize

Is $\mathbf{succ}^\sharp$ optimal? (why not $\texttt{succ}^\sharp(\texttt{E}) \coloneqq \{\texttt{E},\texttt{O}\}$)

Can one derive $\mathbf{succ}^\sharp$ from **succ** directly?

✗ framework

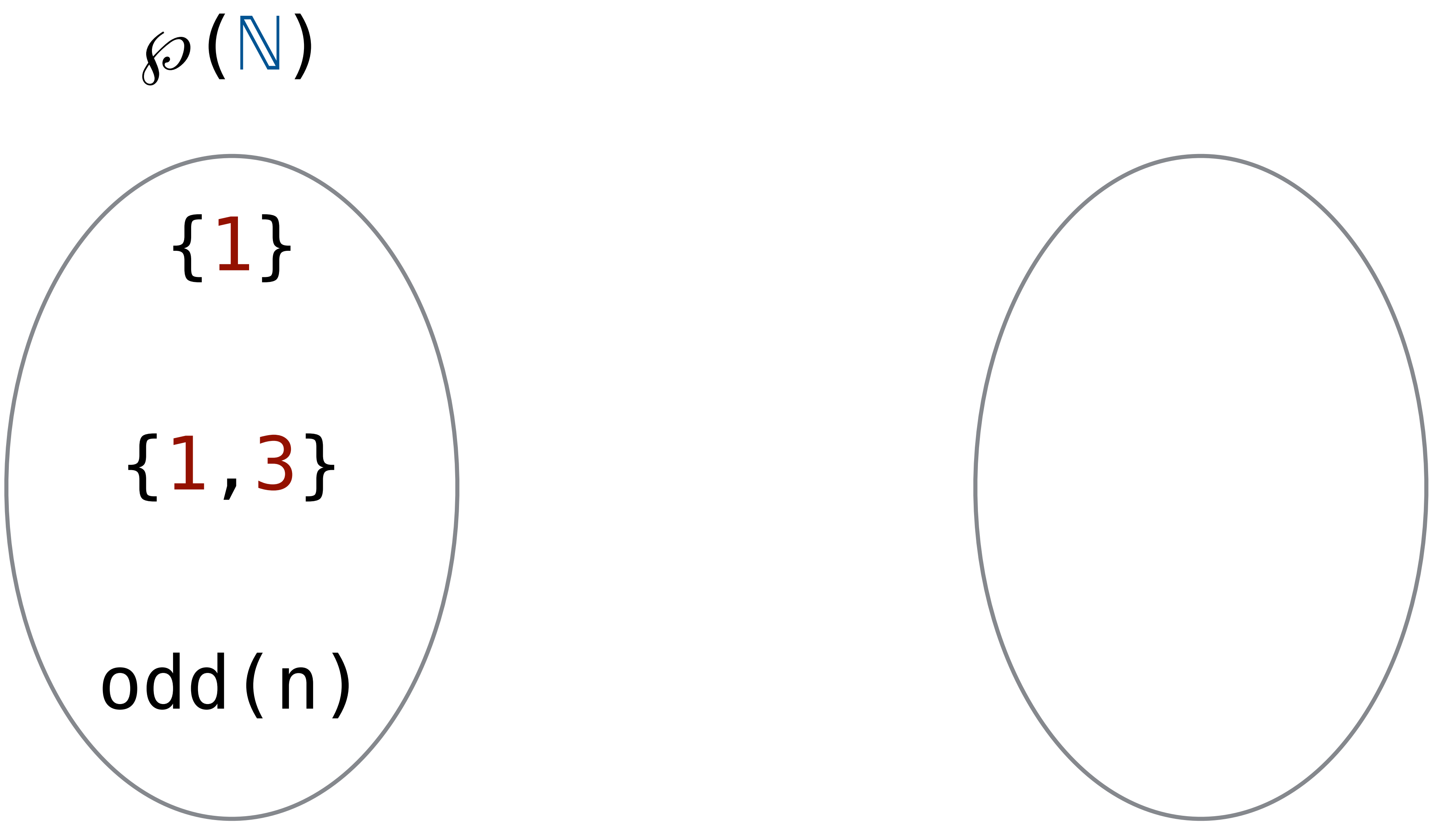
Three Stories

Direct Verification	✗ `framework` ✓ `mechanize`
Abstract Interpretation	✓ `framework` ✗ `mechanize`
Constructive GCs	✓ `framework` ✓ `mechanize`

Abstract Interpretation

Abstract Interpretation

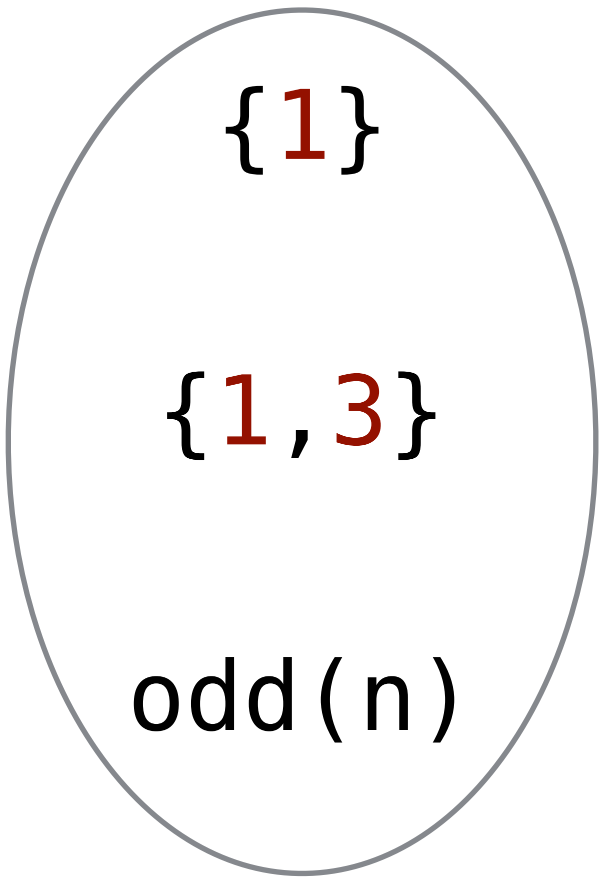
Abstract Interpretation

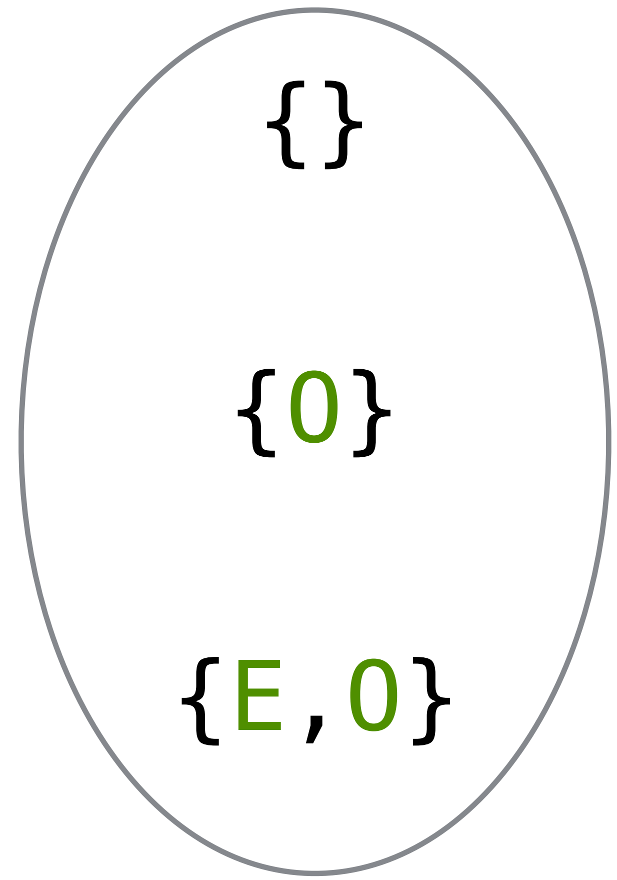


Abstract Interpretation

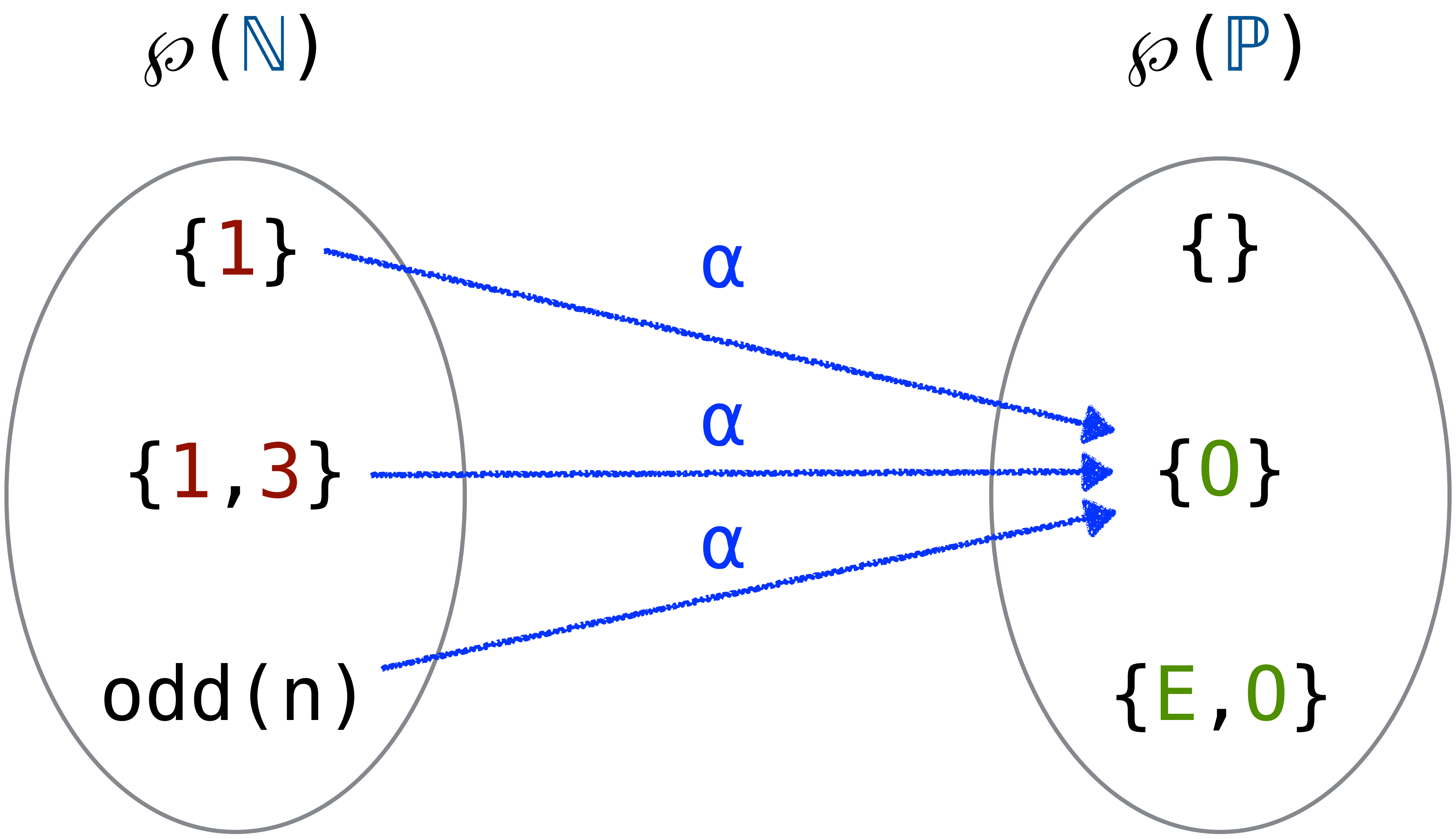
$\wp(\mathbb{N})$

$\wp(\mathbb{P})$

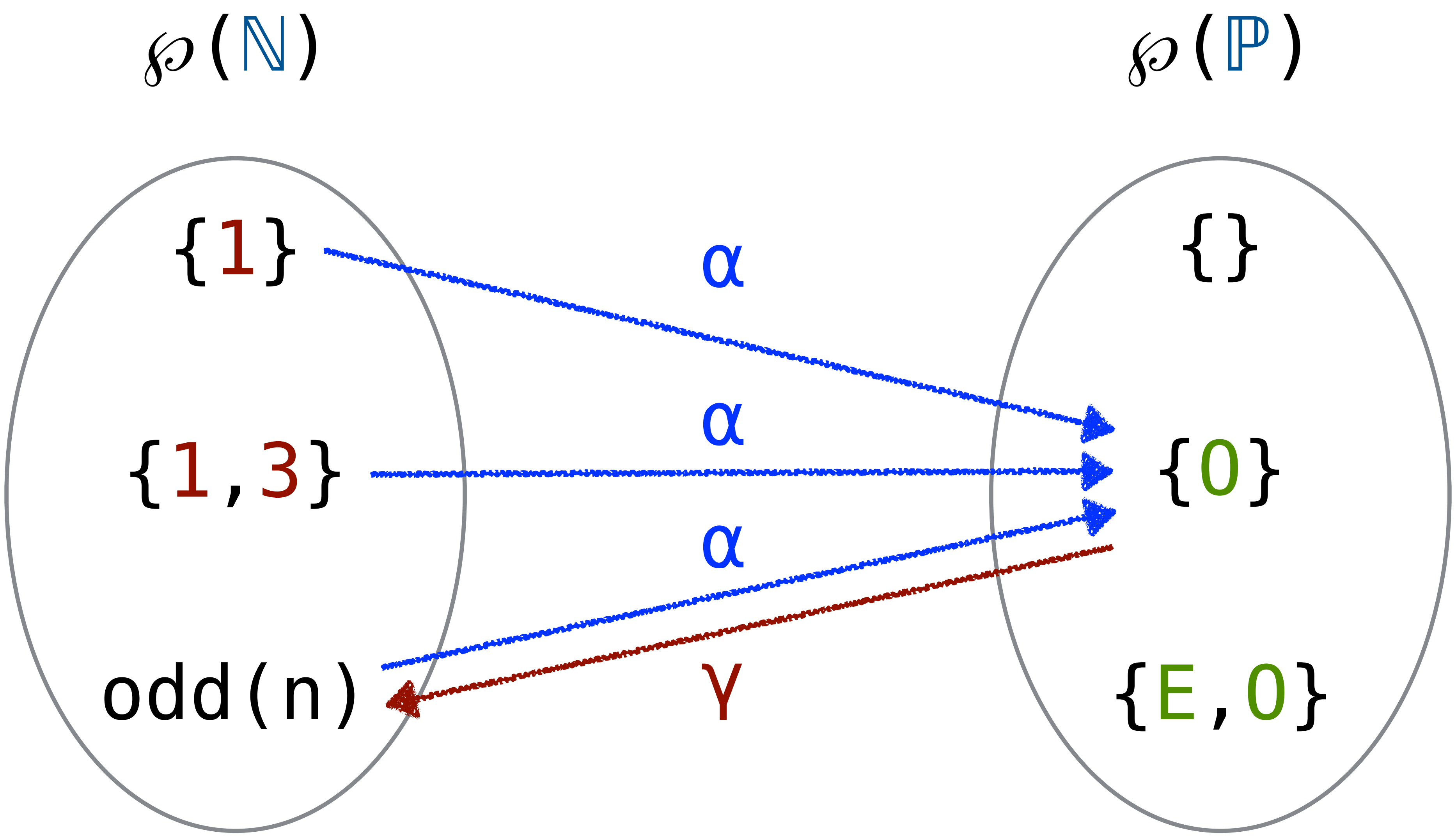




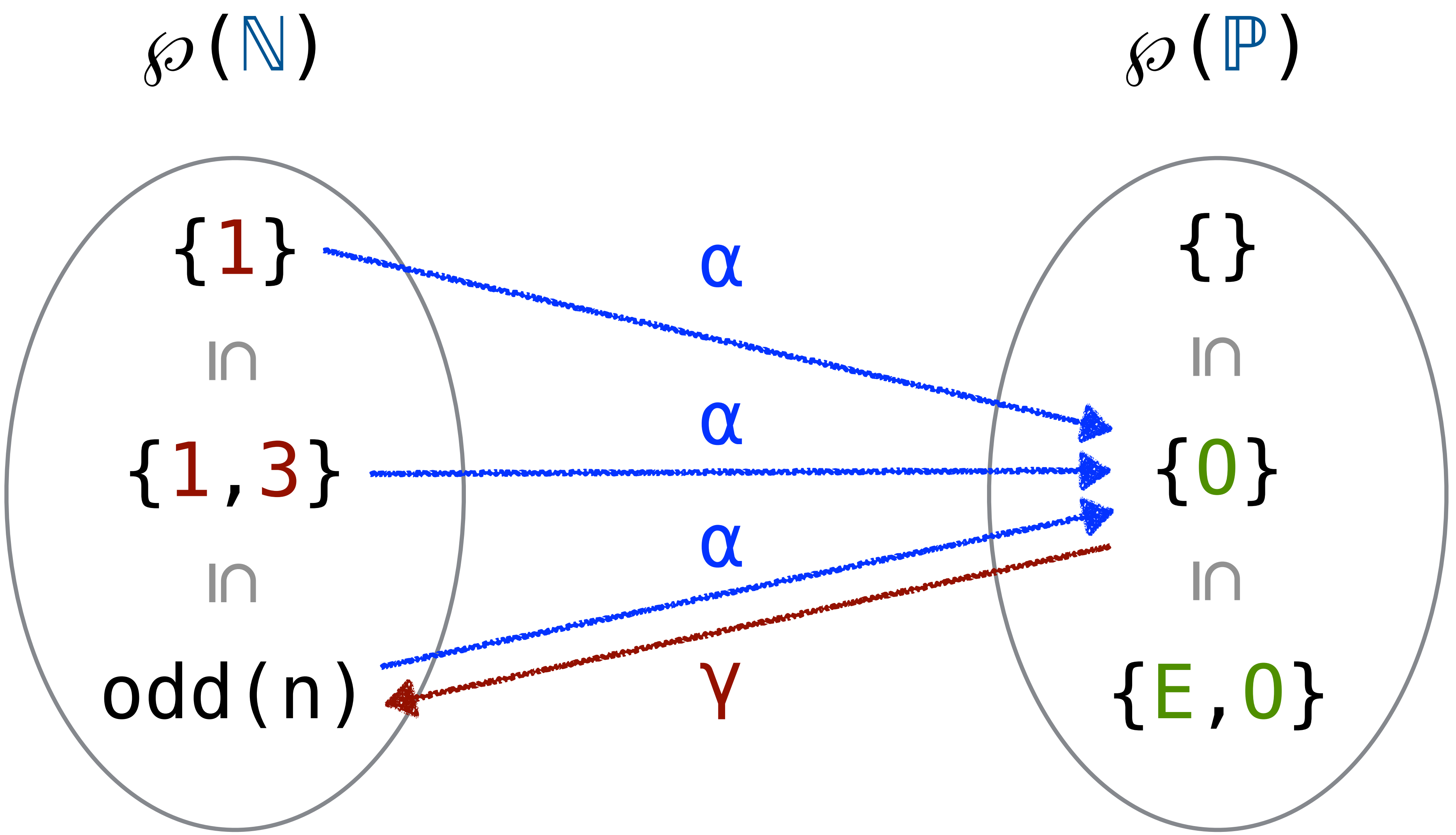
Abstract Interpretation



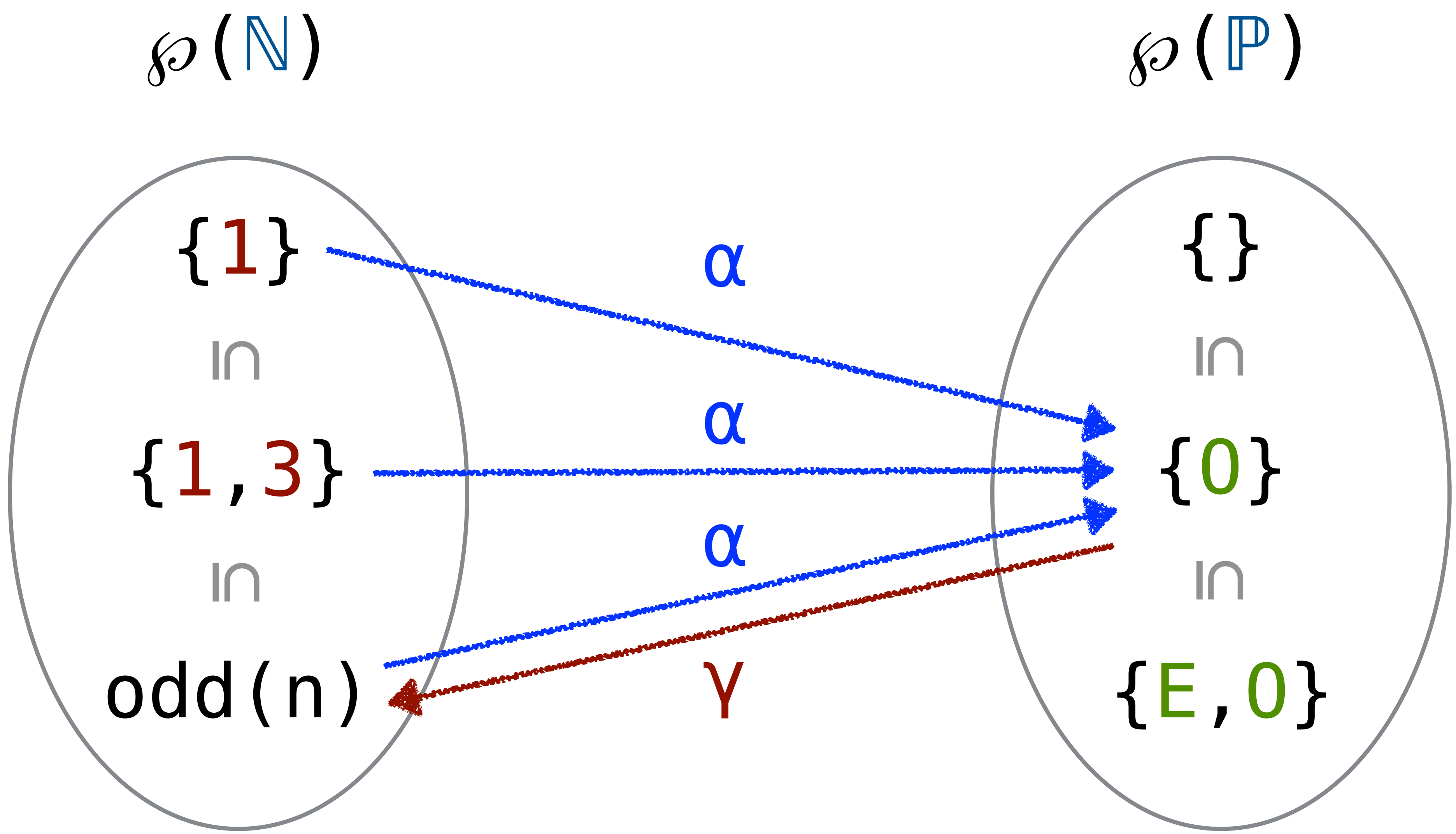
Abstract Interpretation



Abstract Interpretation

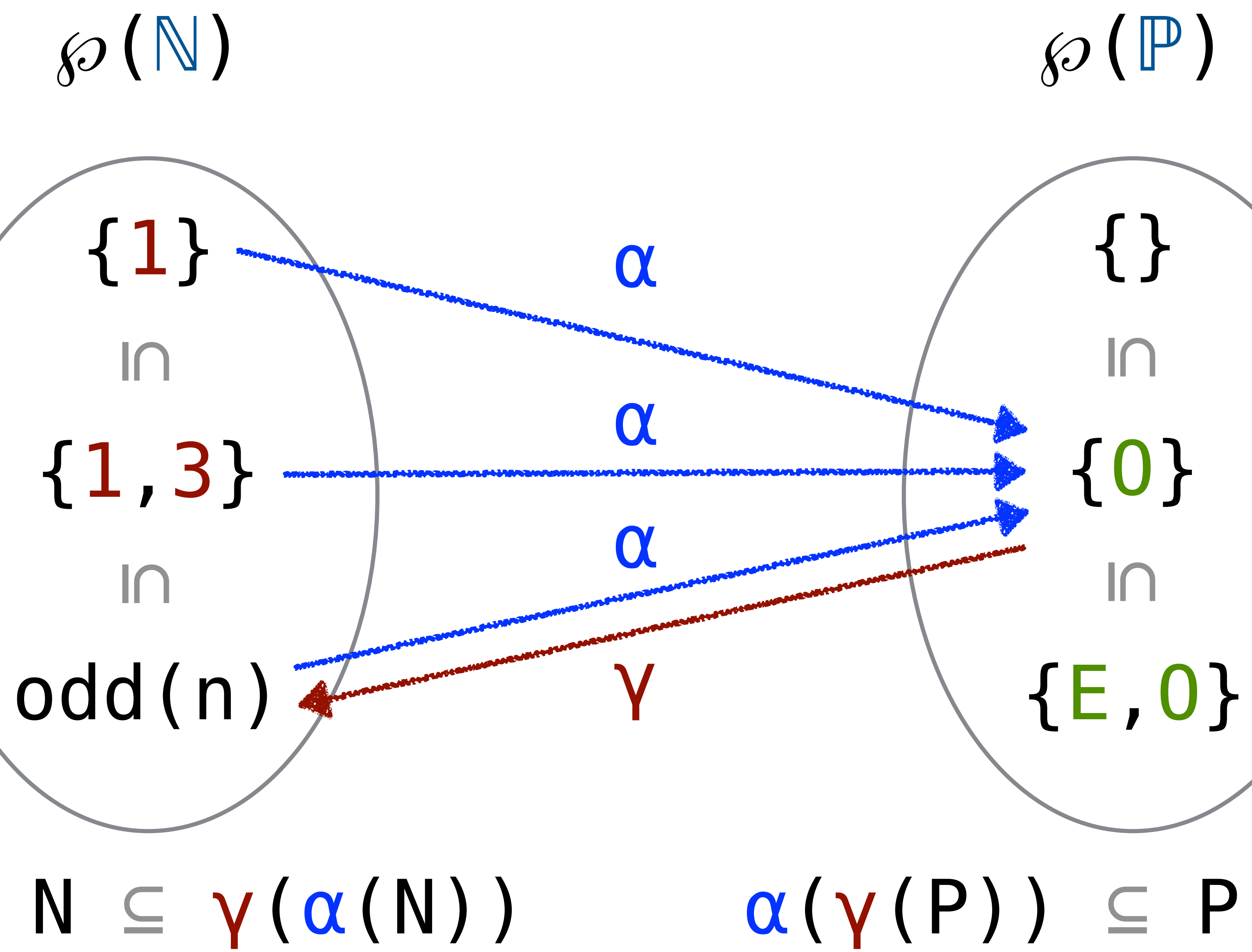


Abstract Interpretation

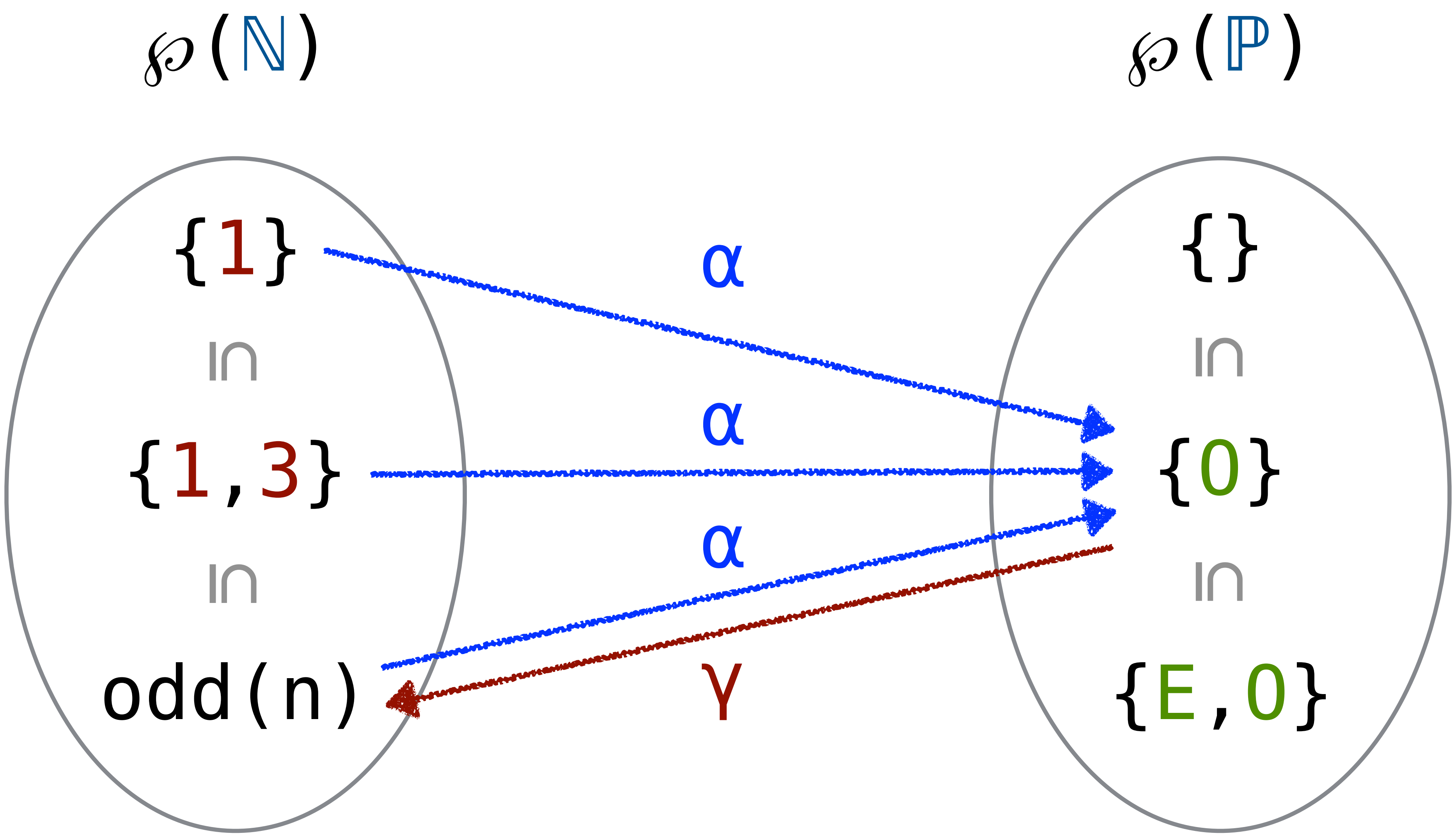


$$N \subseteq \gamma(\alpha(N))$$

Abstract Interpretation



Abstract Interpretation



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

Abstract Interpretation

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

"$\texttt{P}$ is sound for $\texttt{N}$"

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

Abstract Interpretation

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

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

"$\mathtt{P}$ is sound for $\mathtt{N}$"

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

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

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

"$\mathtt{f}^{\mathtt{p}}$ is sound for $\mathtt{f}^{\mathtt{N}}$"

Abstract Interpretation

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

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

"$\mathtt{P}$ is sound for $\mathtt{N}$"

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

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

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

"$\mathtt{f}^{\mathtt{p}}$ is sound for $\mathtt{f}^{\mathtt{N}}$"

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

Abstract Interpretation

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

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

"$\mathtt{P}$ is sound for $\mathtt{N}$"

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

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

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

"$\mathtt{f}^{\mathtt{p}}$ is sound for $\mathtt{f}^{\mathtt{N}}$"

$\alpha \circ \mathtt{f}^{\mathtt{N}} \circ \gamma \subseteq \mathtt{f}^{\mathtt{P}}$

Abstract Interpretation

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

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

Abstract Interpretation

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

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

Abstract Interpretation

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

$\alpha(N) \coloneqq \{parity(n) \mid n \in N\}$

e.g. $\alpha(\{1,3\}) = \{0\}$

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

Abstract Interpretation

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

e.g. $\alpha(\{1,3\}) = \{0\}$

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

Abstract Interpretation

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

e.g. $\alpha(\{1,3\}) = \{0\}$

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

e.g. $\gamma(\{0\}) = \{n \mid \mathrm{odd}(n)\}$

Abstract Interpretation

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

Abstract Interpretation

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

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

$$\uparrow\mathtt{succ}^\sharp : \wp(\mathbb{P}) \to \wp(\mathbb{P})$$
$$\uparrow\mathtt{succ}^\sharp(P) = \{\mathtt{succ}^\sharp(p) \mid p \in P\}$$

Abstract Interpretation

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

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

$$\uparrow\text{succ}\sharp : \wp(\mathbb{P}) \to \wp(\mathbb{P})$$
$$\uparrow\text{succ}\sharp(P) = \{\text{succ}\sharp(p) \mid p \in P\}$$

$$\boxed{\text{sound} : \alpha(\uparrow\text{succ}(\gamma(P))) \subseteq \uparrow\text{succ}\sharp(P)}$$

Abstract Interpretation

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

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

$$\uparrow\texttt{succ}^\sharp : \wp(\mathbb{P}) \to \wp(\mathbb{P})$$
$$\uparrow\texttt{succ}^\sharp(P) = \{\texttt{succ}^\sharp(p) \mid p \in P\}$$

sound	$\alpha(\uparrow\texttt{succ}(\gamma(P))) \subseteq \uparrow\texttt{succ}^\sharp(P)$
optimal	$\alpha(\uparrow\texttt{succ}(\gamma(P))) = \uparrow\texttt{succ}^\sharp(P)$

Abstract Interpretation

$$\boxed{\texttt{optimal : } \alpha(\uparrow\texttt{succ}(\gamma(\texttt{P}))) = \uparrow\texttt{succ}^\sharp(\texttt{P})}$$

Abstract Interpretation

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

Abstract Interpretation

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

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

Abstract Interpretation

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

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

Abstract Interpretation

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

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

Abstract Interpretation

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

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

Abstract Interpretation

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

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

Abstract Interpretation

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

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

Abstract Interpretation

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

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

[CDGAI: Cousot 1999]

Abstract Interpretation

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

$$\uparrow\texttt{succ}^\sharp(\{\texttt{E}\}) \triangleq \{\texttt{O}\}$$

Abstract Interpretation

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

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

$$\uparrow\texttt{succ}^\sharp(\{\texttt{E}\}) \triangleq \{\texttt{0}\}$$

Abstract Interpretation

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

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

$$\uparrow\texttt{succ}^\sharp(\{\texttt{E}\}) \triangleq \{\texttt{0}\}$$

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

Abstract Interpretation

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

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

$$\uparrow\texttt{succ}^\sharp(\{\texttt{E}\}) \triangleq \{\texttt{0}\}$$

$\wp(\mathbb{P})$ ≔ $(\mathbb{P} \rightarrow$ prop) = “specification”
$\wp(\mathbb{P})$ ≔ $[\mathbb{P}]$ = “constructed”

Abstract Interpretation

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

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

$$\uparrow\texttt{succ}^\sharp(\{\texttt{E}\}) \triangleq \{\texttt{O}\}$$

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

Abstract Interpretation

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

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

$$\uparrow\texttt{succ}^\sharp(\{E\}) \triangleq \{0\}$$

$$\wp(\mathbb{P}) \coloneqq (\mathbb{P} \to \texttt{prop}) = \text{"specification"}$$

$$\wp(\mathbb{P}) \coloneqq [\mathbb{P}] = \text{"constructed"}$$

no extraction

Abstract Interpretation

$$\wp(\mathbb{P}) \;\mapsto\; \dots \;\mapsto\; \wp(\mathbb{P})$$

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

$$\uparrow\texttt{succ}^\sharp(\{\texttt{E}\}) \triangleq \{\texttt{0}\}$$

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

$$\wp(\mathbb{P}) \coloneqq [\mathbb{P}] = \text{“constructed”}$$

Abstract Interpretation

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

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

$$\uparrow\!\texttt{succ}^\sharp(\{E\}) \triangleq \{0\}$$

$\wp(\mathbb{P}) \coloneqq (\mathbb{P} \to \texttt{prop}) =$ "specification"

$\wp(\mathbb{P}) \coloneqq [\mathbb{P}] =$ "constructed"

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

Abstract Interpretation

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

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

$\uparrow\mathrm{succ}^\sharp(\{E\}) \triangleq \{0\}$

$\wp(\mathbb{P}) \coloneqq (\mathbb{P} \to \texttt{prop})$ = "specification"

$\wp(\mathbb{P}) \coloneqq [\mathbb{P}]$ = "constructed"

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

no extraction

Abstract Interpretation

General framework (calculation)

✓ framework

Mechanization Issues (no extraction)

✗ mechanize

Abstract Interpretation

γ-only (no calculation)

½ framework

Verification with extraction
Verasco [Jourdan et al POPL 2015]

✓ mechanize

Three Stories

Direct Verification	✗ `framework` ✓ `mechanize`
Abstract Interpretation	✓ `framework` ✗ `mechanize`
Constructive GCs	✓ `framework` ✓ `mechanize`

Constructive GCs

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

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

$$\uparrow\texttt{succ}^\sharp(\{E\}) \triangleq \{0\}$$

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

$\wp(\mathbb{P}) \coloneqq [\mathbb{P}]$ = “constructed”

Constructive GCs

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

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

$$\uparrow\texttt{succ}^\sharp(\{\texttt{E}\}) \triangleq \{\texttt{0}\}$$

$\wp(\mathbb{P})$ ≔ ($\mathbb{P}$ → prop) = “specification”
$\wp(\mathbb{P})$ ≔ [$\mathbb{P}$] = “constructed”

Constructive GCs

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

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

$$\uparrow\texttt{succ}^\sharp(\{E\}) \triangleq \{0\}$$

$$\wp(\mathbb{P}) \coloneqq (\mathbb{P} \to \texttt{prop}) \wedge \text{“has effects”}$$
$$\wp(\mathbb{P}) \coloneqq (\mathbb{P} \to \texttt{prop}) \wedge \text{“no effects”}$$

Constructive GCs

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

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

$$\uparrow\mathrm{succ}^\sharp(\{E\}) \triangleq \{0\}$$

$\wp(\mathbb{P}) \coloneqq (\mathbb{P} \to \texttt{prop}) \land$ "has effects"

$\wp(\mathbb{P}) \coloneqq (\mathbb{P} \to \texttt{prop}) \land$ "no effects"

$\wp(\mathbb{P}) \rightleftarrows \mathbb{P}$ (singleton in list monad)

Constructive GCs

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

vs

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

Constructive GCs

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

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

(+ monadic GC laws)

vs

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

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

(+ GC laws)

Constructive GCs

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

(+ monadic GC laws)

vs

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

(+ GC laws)

α^{M} “has no effects”

Constructive GCs

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

$$\gamma^{M} : \mathbb{P} \to \wp(\mathbb{N}) \qquad \text{vs} \qquad \gamma : \wp(\mathbb{P}) \to \wp(\mathbb{N})$$

(+ monadic GC laws) (+ GC laws)

α^{M} “has no effects”

Constructive GCs

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

(+ monadic GC laws)

vs

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

(+ GC laws)

α^{M} "has no effects"

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

Constructive GCs

$$\boxed{\begin{array}{lcl} \eta & : & \mathbb{N} \to \mathbb{P} \\ \mu & : & \mathbb{P} \to \wp(\mathbb{N}) \end{array}}$$

Constructive GCs

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

$$\eta(n) \coloneqq \mathrm{parity}(n)$$
$$\mu(p) \coloneqq [\![p]\!]$$

Constructive GCs

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

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

$\eta(n) \coloneqq \mathrm{parity}(n)$
$\mu(p) \coloneqq [\![p]\!]$

Constructive GCs

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

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

$\eta(n) \coloneqq \mathrm{parity}(n)$

$\mu(p) \coloneqq [\![p]\!]$

$\alpha(N) \coloneqq \{\eta(n) \mid n \in N\}$

$\gamma(P) \coloneqq \{n \mid p \in P \wedge n \in \mu(p)\}$

Constructive GCs

$\boxed{\texttt{calc : } (\alpha \circ {\uparrow}\mathrm{succ} \circ \gamma)(P) = {\uparrow}\mathrm{succ}^\sharp(P)}$

$\boxed{\texttt{calc : } (\lfloor\eta\rfloor \circledast \lfloor\mathrm{succ}\rfloor \circledast \mu)(p) = \lfloor\mathrm{succ}^\sharp\rfloor(p)}$

Constructive GCs

```
calc : (α∘↑succ∘γ)(P) = ↑succ♯(P)
```

```
calc : (⌊η⌋⊛⌊succ⌋⊛μ)(p) = ⌊succ♯⌋(p)
```

Constructive GCs

```
calc : (α∘↑succ∘γ)(P) = ↑succ♯(P)
```

```
calc : (⌊η⌋⊛⌊succ⌋⊛μ)(p) = ⌊succ♯⌋(p)
```

“powerset lifting = boilerplate”

Results

Results

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

Results

- Metatheory complete w.r.t. subset of classical GC
- Same adjunction as GCs but Kleisli adjoint functors

Results

- Metatheory complete w.r.t. subset of classical GC
- Same adjunction as GCs but Kleisli adjoint functors
- Case Study: Calculational AI [Cousot 1999]

Results

- Metatheory complete w.r.t. subset of classical GC
- Same adjunction as GCs but Kleisli adjoint functors
- Case Study: Calculational AI [Cousot 1999]
- Case Study: AGT [Garcia, Clark and Tanter 2016]

Results

- Metatheory complete w.r.t. subset of classical GC
- Same adjunction as GCs but Kleisli adjoint functors
- 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
- Same adjunction as GCs but Kleisli adjoint functors
- 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

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

(+ monadic GC laws)

✓ `framework`
✓ `mechanize`

Draft: Constructive Galois Connections
http://arxiv.org/abs/1511.06965