

Helmut Seidel Fest, Munich, July 16-17, 2026

Non Standard Axiomatic Semantics

Patrick Cousot
Courant Institute, NYU

Axiomatic Semantics

On wikipedia (axiomatic semantics)

"Axiomatic semantics define the meaning of a command in a program by describing its effect on assertions about the program state."

"It is closely related to Hoare logic."

semantics of programming languages

"semantics is the rigorous mathematical logic study of the meaning of programming languages."

so semantics should be non-ambiguous
(up to an isomorphism). Is it ???

On the definition of the naturals

Peano's definition (1889)

$$0 \in \mathbb{N}$$

$$\frac{n \in \mathbb{N}}{n+1 \in \mathbb{N}}$$

$$n+1 = S(n)$$

$$\forall n \in \mathbb{N} \setminus \{0\}. \quad n \neq 0$$

$$\forall n, m \in \mathbb{N}. \quad n+1 = m+1 \Rightarrow n = m$$

Non standard models (Skolem, 1934)

0 1 2 ...

standard model

0 1 2 -1' 0' 1' ...

... ... -1' 0' 1' -1'' 0'' 1'' ...

...

All non standard models satisfy
Peano axioms!

Dedekind Principle of Recurrence (1888)

Principle of induction (recurrence)

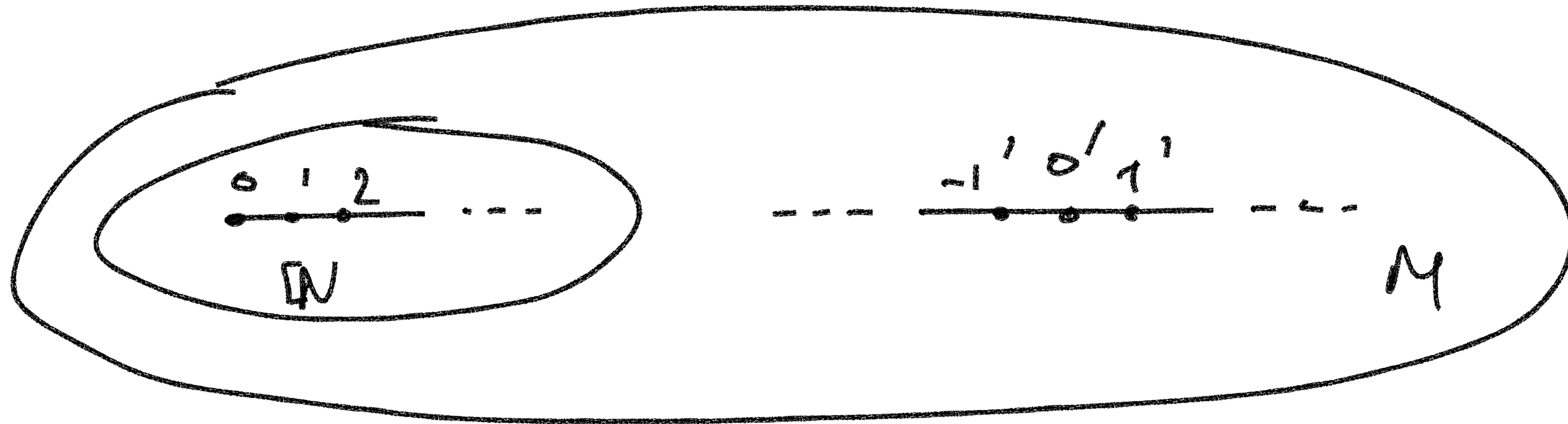
$$P(0), \quad \forall n. P(n) \Rightarrow P(n+1)$$

$$\forall n. P(n).$$

Add the requirement:

The principle of induction should be sound for the natural

Soundness of recurrence eliminates $\Rightarrow$
standard models



$$0 \in M, \forall x \in M. x+1 \in M$$

but $M \neq N$ so M is not a model
of N

A modern definition of the standard model

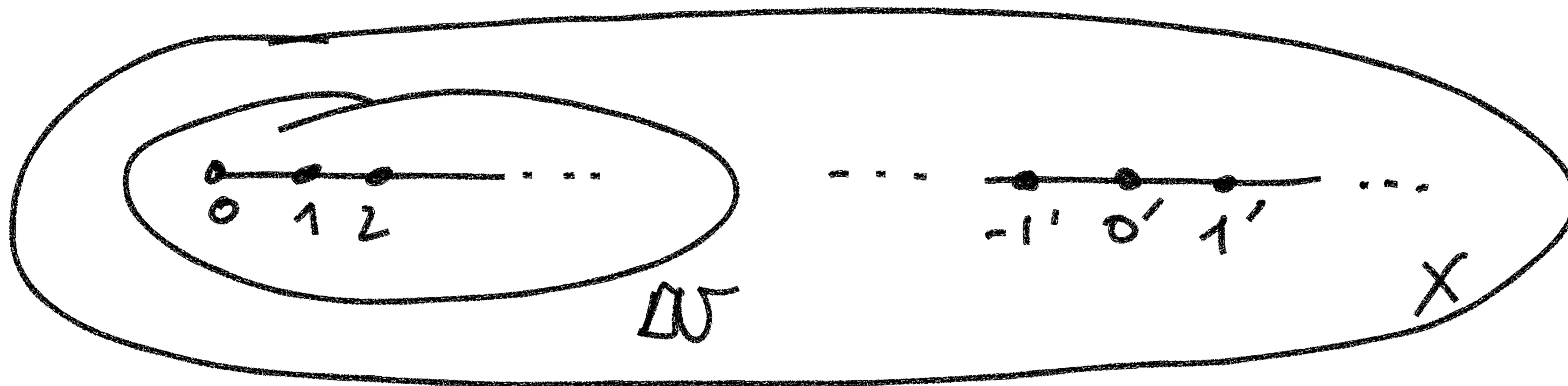
- $0 \in \mathbb{N}$
 - $n \in \mathbb{N} \Rightarrow n+1 \in \mathbb{N}$
 - $n \neq m \Rightarrow n+1 \neq m+1$
 - $\forall n \in \mathbb{N}. n+1 \neq 0$
 - the set $\mathbb{N}$ is the smallest set such that $0 \in \mathbb{N}$ and $\forall n \in \mathbb{N}. n+1 \in \mathbb{N}$
- } Peano

Alternatives: Zermelo: $0 = \{\}$, $n+1 = \{n\}$ Von Neumann
 $0 = \{\}$ & $n+1 = n \cup \{n\}$

A least fixpoint definition of the natural

$$N = \text{LFP}^{\leq} \lambda x. \{0\} \cup \{n+1 \mid n \in x\}$$

The non-standard models satisfy the equation $X = \{0\} \cup \{n+1 \mid n \in X\}$ but are not the smallest ones



Park fixpoint induction is the principle of recurrence

Park induction (f increasing on a complete lattice)

$$\text{lfp}^E f \sqsubseteq P \Leftrightarrow \exists I. f(I) \sqsubseteq I \wedge I \sqsubseteq P$$

For soundness only

$$f(P) \sqsubseteq P \Rightarrow \text{lfp} f \sqsubseteq P$$

This is recurrence

$$\{0\} \cup \{n+1 \mid n \in P\} \subseteq P$$

$$\Leftrightarrow \{0\} \subseteq P \wedge \{n+1 \mid n \in P\} \subseteq P$$

$$\Leftrightarrow 0 \in P \wedge \forall n \in P. n+1 \in P$$

so that by fix point induction

$$\Rightarrow \text{eff}_P^c \sim X. \{0\} \cup \{n+1 \mid n \in X\} \subseteq P$$

that is $\Omega \subseteq P$.

Definitions of the naturals

- Peano $\Rightarrow$ has non-standard models
- Peano + Dedekind $\Rightarrow$ requiring the recurrence principle to be sound for the naturals eliminates the non-standard models
- The modern least-fix point definition
 - eliminates the non-standard models
 - recovers the recurrence principle as an instance of Park induction

Standard (and Non-Standard) Traces

States (of a simple imperative language)

- $\mathbb{L}$ set of labels
- $\mathbb{X}$ set of variables
- $\mathbb{V}$ set of values
- $\mathbb{E} = \mathbb{X} \rightarrow \mathbb{V}$ environments
- $\Sigma = \mathbb{L} \times \mathbb{E}$ states

Standard finite traces

$$\sigma \in \Sigma^* = \bigcup_{n \geq 0} [0, n] \rightarrow \Sigma$$



starts and terminates

Notation of non standard naturals

- $\mathbb{N} + \delta$, $\delta \in [0, \omega]$ is the following set of non-standard naturals



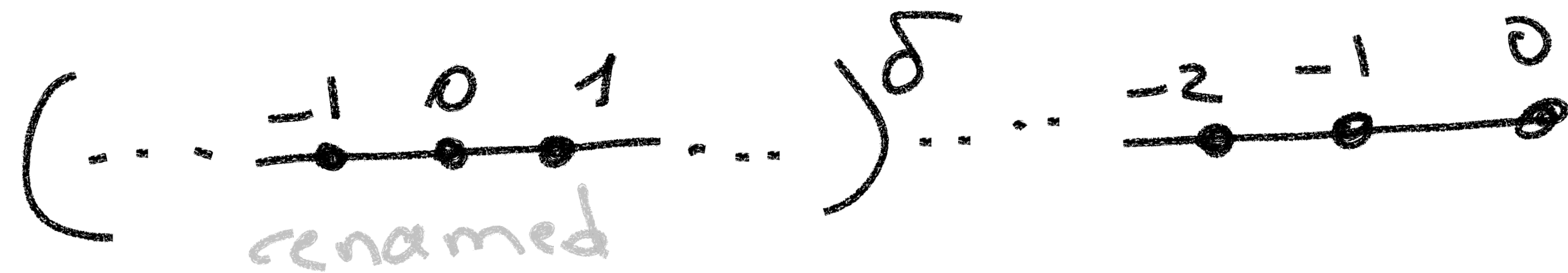
start but
never
terminates

- $\mathbb{N} = \mathbb{N} + 0$

- Example on $\mathbb{N} + \delta$:
while (1)
 $x := x + 1$;

Non standard negatives

- $\mathbb{N}^{-\delta} \triangleq \{-x \mid x \in \mathbb{N}^{+\delta}\}$

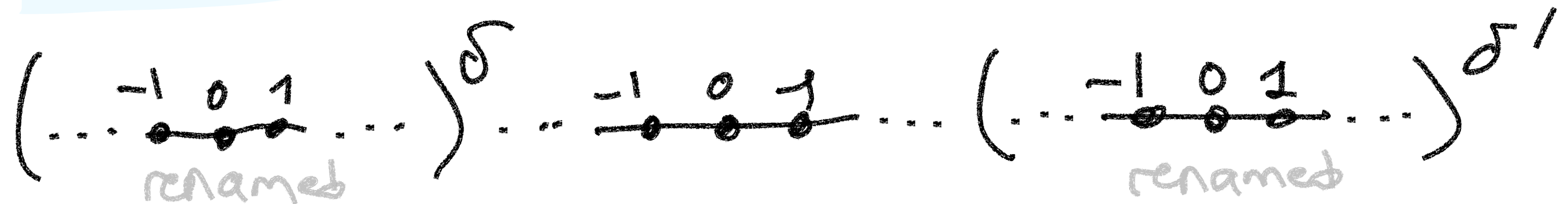


never starts
but terminates

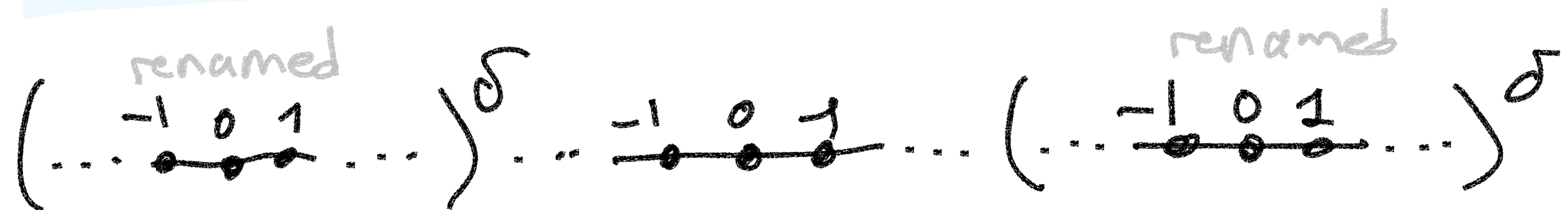
- Example on $\mathbb{N}^{-\delta}$
while ($x \neq 0$)
 $x = x + 1$;

Non Standard Integers

- $\mathbb{N} - \delta + \delta' \triangleq \mathbb{N} - \delta \cup \mathbb{N} + \delta'$



- $\mathbb{N} \pm \delta \triangleq \mathbb{N} - \delta + \delta$



never starts and never terminates

(Non Standard) traces

— non-standard infinite traces

$$\Sigma^{-\delta+\delta'} \triangleq W^{-\delta+\delta'} \rightarrow \Sigma$$

— Including the standard finite traces

$$\Sigma^{*-\delta+\delta'} = \Sigma^* \cup \Sigma^{-\delta+\delta'}$$

— The standard finite or infinite traces are

$$\Sigma^{*\infty} \triangleq \Sigma^{*+0}$$

$$\{ \overset{0}{\bullet} \overset{1}{\bullet} \overset{2}{\bullet} \dots \overset{n-1}{\bullet} \overset{n}{\bullet} \mid n \in \mathbb{N} \} \cup \{ \overset{0}{\bullet} \overset{1}{\bullet} \overset{2}{\bullet} \dots \overset{n}{\bullet} \overset{n+1}{\bullet} \dots \}$$

Moise & Lauer Axiomatic Semantics

Hoare logic

- Postulated by Hoare (1968)
- Proved sound and relatively complete by Cook (using weakest preconditions on sets + expressivity) (1978)
- An abstraction of a structural trace semantics (POPL 2024)

Hoare logic as language definition

- the axiomatic technique for the definition of programming language semantics appears to be like the formal syntax of the ALGOL 60 report, in that it is sufficiently simple to be understood both by the implementor and by the reasonably sophisticated user of the language. *To be discussed*
- axioms offer a simple and flexible technique for leaving certain aspects of a language *undefined*, for example, range of integers, accuracy of floating point, and choice of overflow technique. *and also non-naturals and traces which are not excluded.*

Relative completeness and expressiveness

- The assertion language may not be able to express loop invariant

e.g. first order logic cannot express fix points

- **expressiveness** : assume the logic can express set-theoretic loop invariant

Eliminating the expressiveness problem

- Take the "assertion language" to be sets

⇒ Loop invariants are expressible as sets

(which is nothing but what Cook is doing in his completeness proof.)

Trace Semantic Domains

— Standard Semantic Domain :

$$\mathbb{D}^{+\infty} = \mathcal{F}(\Sigma^{+\infty}) = \mathcal{F}(\Sigma^* + 0)$$

— Non-standard Semantic Domains:

$$\mathbb{D}^{*- \delta + \delta'} = \mathcal{F}(\Sigma^{*- \delta + \delta'})$$

— A semantic domain is a set of finite and (non-standard) infinite traces

(other non-standard trace semantics)

$\text{Ord} \rightarrow \Sigma$

(Ord is not a non-standard model of Peano naturals since any $n \neq 0$ must have a predecessor)

- suggested in footnote 17 page 53 of

Patrick Cousot:

Constructive design of a hierarchy of semantics of a transition system by abstract interpretation. Theor. Comput. Sci. 277(1-2): 47-103 (2002)

- fully developed in

Roberto Giacobazzi, Isabella Mastroeni: **Non-Standard Semantics for Program Slicing.** High. Order Symb. Comput. 16(4): 297-339 (2003)

Trace semantics of assignment

• $T^* [x := E;] \triangleq \{ \langle e, p \rangle \langle e', p[x \leftarrow \underbrace{\mathcal{E}(E)}_{\text{value of expression } E}] \rangle \mid p \in E \}$

Annotations for the trace $\langle e, p \rangle \langle e', p[x \leftarrow \mathcal{E}(E)] \rangle$:

- $\langle e, p \rangle$: at $[x := E]$
- p : initial value of p variables
- $p[x \leftarrow \mathcal{E}(E)]$: final value of variables after $[x := E]$
- $\mathcal{E}(E)$: value of expression E

• $T^{-\delta + \delta'} [x := E;] \triangleq \emptyset$

no infinite traces, assignment always terminates

Standard trace semantics of iteration

$$S ::= \text{while}_e^e (B)_{e'} S_b^{e''} \quad \begin{array}{l} \text{at } [S] = \text{after } [S_b] \\ \text{at } [S_b] \end{array} \quad \text{after } [S]$$

Finite traces :

$$T^*[S] = \text{efp} \subseteq F^*[S]$$

$$F^*[S] \times = \{ \langle e, p \rangle \langle e'', p \rangle \mid \neg B[B] p \} \cup \\ \{ \langle e, p \rangle \langle e', p \rangle \sigma \langle e, p' \rangle \sigma' \mid B[B] p \wedge \\ \langle e', p \rangle \sigma \langle e, p' \rangle \in T[S_b] \wedge \\ \langle e, p' \rangle \sigma' \in X \}$$

Standard trace semantics of iteration

Infinite future traces:

$$S ::= \text{while}^e(B)^{e'} S_b^{e''} \leftarrow \text{after}[S]$$

$\uparrow$ $\uparrow$ $\uparrow$
 $\text{at}[S] =$ $\text{at}[S_b]$ $\text{at}[S_b]$

$$T^+ [S] = \text{gfp}^\subseteq F^+ [S]$$

$$F^+ [S] X = \{ \langle e, p \rangle \langle e', p \rangle \sigma \langle e, p' \rangle \sigma' \mid \begin{aligned} & \langle e', p \rangle \sigma \langle e, p' \rangle \in T^* [S_b] \wedge \\ & (\langle e, p' \rangle \sigma' \in X \vee \\ & \langle e, p' \rangle \sigma' \in T^+ [S_b]) \end{aligned} \}$$

Non-standard past infinite traces

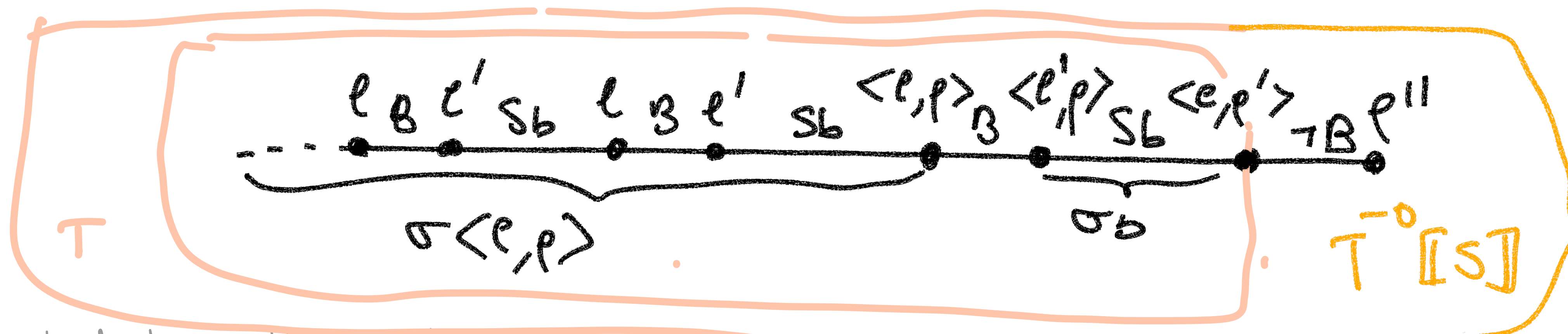
$$S ::= \text{while}^e(B)^{e'} S_b \ e''$$

$$T^{-0}[S] \triangleq \text{let } T = \text{gfp}^S F^{-0}[S] \text{ in}$$

$$\{ \sigma \langle e, p \rangle \langle e'', p \rangle \mid \sigma \langle e, p \rangle \in T \wedge \neg \mathbb{B}[B] p \}$$

$$F^{-0}[S] X \triangleq \{ \sigma \langle e, p \rangle \langle e', p \rangle \sigma_b \langle e, p' \rangle \mid \sigma \langle e, p \rangle \in X$$

$$\mathbb{B}[B] p \wedge \langle e', p \rangle \sigma_b \langle e, p' \rangle \in T[S_b] \}$$



Non Standard Past and Future Infinite Traces

$$S ::= \text{while}^e(B) c' \leq_b c''$$

$$T^{-0+0}[S] = \{ \sigma \langle e, p \rangle \sigma' \mid \sigma \langle e, p \rangle \in T^{+0}[S] \wedge \langle e, p \rangle \sigma' \in T^{-0}[S] \}$$

(possible generalization to $\sigma > 0$)

Non standard semantics

$$T[S] = \underbrace{T^*[S] \cup T^{+0}[S]}_{\text{Standard}} \cup \underbrace{T^{-0}[S] \cup T^{-0+0}[S]}_{\text{Non Standard}}$$

Standard

↑
finite

↑
starts but
no termination

Non Standard

↑
never
start but
terminate

↑
never start
and never
terminate

Hoare logic is an
abstraction of a trace
semantics

Hoare Triple

$\{P\}S\{Q\}$

- standard interpretation :

For any finite execution of S starting in environment $p \in P$ and terminating in final environment p' has $p' \in Q$

- Non standard interpretation

--- and any infinite past execution with invariant P terminating in final environment p' has $p' \in Q$

Trace semantics to Hoare triples abstraction

$$\alpha_H[S]_T = \{ \{P\} S \{Q\} \}$$

$$\begin{aligned} & \forall \langle \text{at}[S], p \rangle \sigma \langle \text{after}[S], p' \rangle \in T. p \in P \Rightarrow p' \in Q \\ & \wedge \forall \sigma \langle \text{at}[S], p \rangle \sigma' \langle \text{after}[S], p' \rangle \in T. p \in P \Rightarrow p' \in Q \end{aligned}$$

standard
↑
non standard

Partial correctness:

- Terminating execution in T^* and $T^{-\delta}$ are taken into account ($\delta \geq 0$)
- Non terminating executions in $T^{+\delta}$ and $T^{-\delta+\delta}$ are ignored

Trace semantics to Hoare triple abstraction

$$\langle \mathcal{G}(\Sigma^* - \delta + \delta'), \subseteq \rangle \xrightleftharpoons[\alpha_M[S]]{\delta_H[S]} \langle \mathcal{G}(\mathcal{F}(E) \times \mathcal{F}(E)), \subseteq \rangle$$

Trace
semantic S

Set of valid Hoare
triples for S

The more traces
the more valid
Hoare triples

Like POPL 2024 but with
non-standard semantics!

Hoare logic triples for statement S

$$\underbrace{\wp[S]}_{\text{Set of Hoare triples for } S} = \underbrace{\alpha_H[S]}_{\text{Trace to Hoare triples abstraction}} \left(\underbrace{\tau[S]}_{\text{Trace semantics}} \right)$$

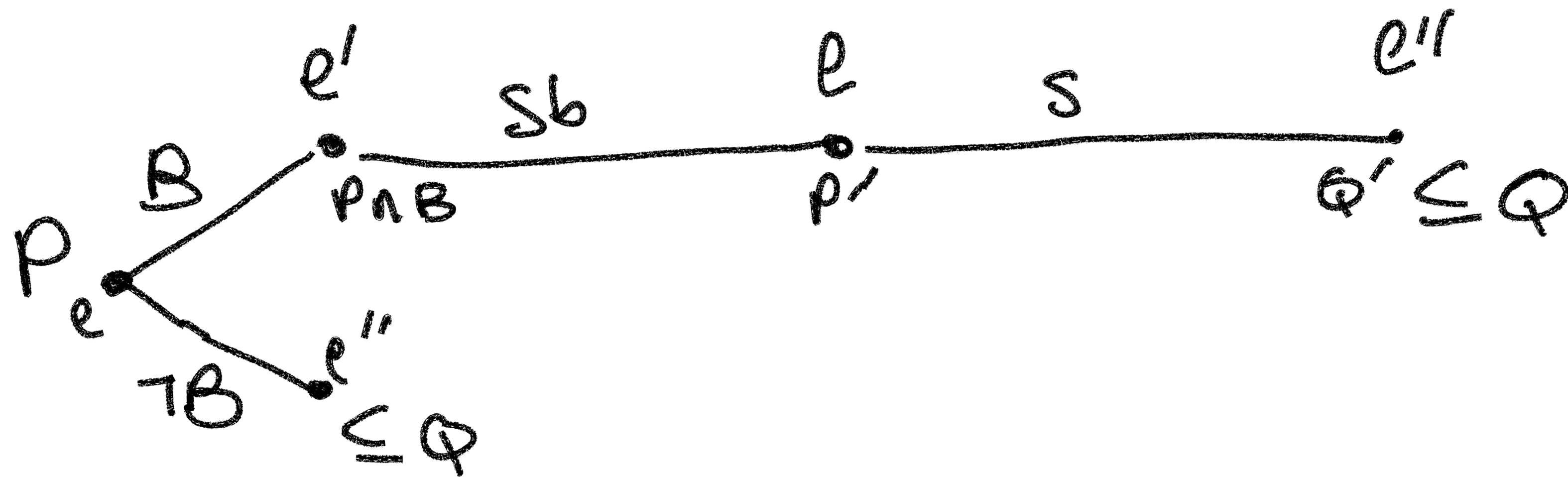
Knowing $\tau[S]$ we derive $\wp[S]$
by calculational design

Hoare triples for iteration $S ::= \text{while}^e(B)^{e'} S_b^{e''}$

$$\text{fp}[S] = \text{gfp}^{\leq} F^H[S]$$

induction

$$F^H[S]X = \{ \langle P \rangle S \langle Q \rangle \mid P \cap \neg B \subseteq Q \wedge \exists \langle P' \rangle S \langle Q' \rangle \in X. \\ \{ P \cap B \rangle S_b \langle P' \rangle \wedge Q' \subseteq Q \}$$



Floyd's induction on traces length in disguise!

The while rule is included: $S ::= \text{while}^e(B)^{e'} S_b^{e''}$

$$\{ \vdash P \vdash S \vdash Q \mid \exists I. P \subseteq I \wedge [I \cap B] S_b [I] \wedge I \cap \neg B \subseteq Q \}$$

$$\subseteq \mathcal{H}[S]$$

This can be proved as follows (similar to POPL 24)

Moore triples for $S ::= \text{while } (B) S_b$

$$F[P] = \lambda I. P \cup \bigcup \{I' \mid \underbrace{\{I \wedge B\} S_b \{I'\}}\}$$

well defined by structural induction

$$\alpha_H(S) = \{ \{P\} S \{Q\} \mid \\ \underbrace{(\text{lfp} \subseteq F[P]) \cap \neg B \subseteq Q} \}$$

strongest invariant

Moare logic

Since Hoare logic does not use the strongest invariant we use Park fix point induction.

$$\underbrace{(\text{fp} \subseteq F[P]) \cap \neg B \subseteq Q}$$

$$\Leftrightarrow \exists I. F[P]I \subseteq I \wedge I \cap \neg B \subseteq Q$$

which yields Hoare rule for iteration

Non Standard Hoare Logic

Problem

- Hoare logic abstracts a standard trace model
- This was probably the intuition of Hoare
- Hoare logic has no way to express that
- And so Hoare logic is also the abstraction of non standard models

— More logic is unable to distinguish between these non-standard semantics

$\cong$ Peano arithmetic with non-standard models

what to add to Moore logic to
prevent non standard models

- must be similar to
Peano $\mathbb{N}$ $\rightarrow$ Peano $\mathbb{N}$ + ^{Dedekind} proof by recurrence
is valid


standard $\mathbb{N}$

A first (failed) attempt

Require existence of a variant function

→ forces termination, eliminate future infinite traces

→ does not eliminate past infinite traces

Assume strongest invariant (lfp) as in weakest transformers

→ the semantics is described exactly

→ does not prevent non-standard traces that belong to the semantics

Knuth termination proof method

- add a counter to each loop
 - initialize it to zero
 - increment it at each iteration
 - prove that it is bounded in Ω
- ensure counter is bounded in Ω
- ⇒ enforces termination
- ⇒ does not work with unbounded non-determinism

(automatized in 1977 with polyhedra)

BUT

Forward w-bounded Knuth method

- The counter is now in $\Omega^{\ast\delta}$, i.e. a non-standard natural
- Require that it is bounded by w (first infinite ordinal)
 - $\rightsquigarrow$ allows non-termination
 - $\rightsquigarrow$ restrict infinite forward traces in $\Omega \rightarrow \Sigma$
 - $\rightsquigarrow$ does not prevent non-standard backward traces

Backward Knuth method

- add a counter in N to each loop
- the counter is decremented at each iteration
- the final value of the counter is 0 (if the loop terminates)
- prove the counter is initially bounded in N

$\rightsquigarrow$ eliminates all traces in $\Sigma^{-\delta}$ (that never start but terminate)

Standard Moore Logic

— The classic Moore rules

+ forward w-bounded Knuth method

+ backward ~~W~~-bounded Knuth method

⇒ traces must be backward finite
and forward finite or infinite

⇒ standard trace model

But do we have something more to prove when using Hoare logic?

- No because :
 - trivially true for standard traces
 - we all assume standard traces
- the same way that when we say "the naturals" we exclude implicitly non-standard models

Conclusion on Axiomatic Semantics

Turing → proof method ...
Floyd → Assigning meaning to programs
Hoare → Axiomatic basis ...

Lauer (thesis) → Axiomatic semantics
Hoare & Lauer

an historical misunderstanding
Standard Trace Semantics guarantees uniqueness
and all other semantics are abstractions!

The End, Thank You

The End, Thank You
Happy retirement Helmut!