Nonstandard Axiomatic Semantics

Patrick Cousot

Courant Institute, NYU.

Axiomatic semantics : Hoare logic

defines the semantics of programs (at some level of abstraction)

Axiomatic semantics : Hoare logic

defines the semantics of programs (at some level of abstraction)

Is it ambiguous ?

Axiomatic semantics : Hoare logic

defines the semantics of programs (at some level of abstraction)

Is it ambiguous ? YES because

it does not define the behavior of programs in a unique way.

Back to the axiomatic semantics

- The problem is with iteration `while(B)s`

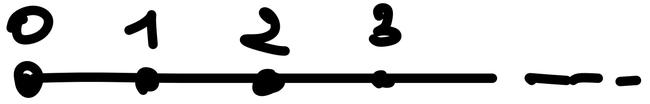
Back to the axiomatic semantics

- The problem is with iteration `while(B)s`
- Example `while (true) x=x+1;`
  - standard model (the memory state is simplified into the value of x)



Back to the axiomatic semantics

- The problem is with iteration `while(B)s`
- Example `while (true) x=x+1;`
  - standard model (the memory state is simplified into the value of x)



  - Non standard model:



A historic analog: Peano Arithmetic

Naturals by Peano:

- $0 \in \mathbb{N}$
- $\dfrac{n \in \mathbb{N}}{S(n) \in \mathbb{N}}$ where successor is $S(n) = n+1$

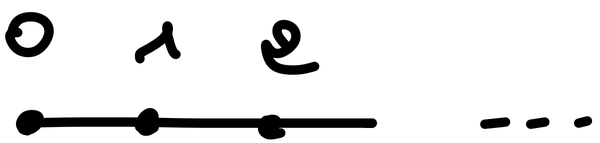
A historic analog: Peano Arithmetic

Naturals by Peano:

- $0 \in \mathbb{N}$
- $\dfrac{n \in \mathbb{N}}{S(n) \in \mathbb{N}}$ where successor is $S(n) = n+1$

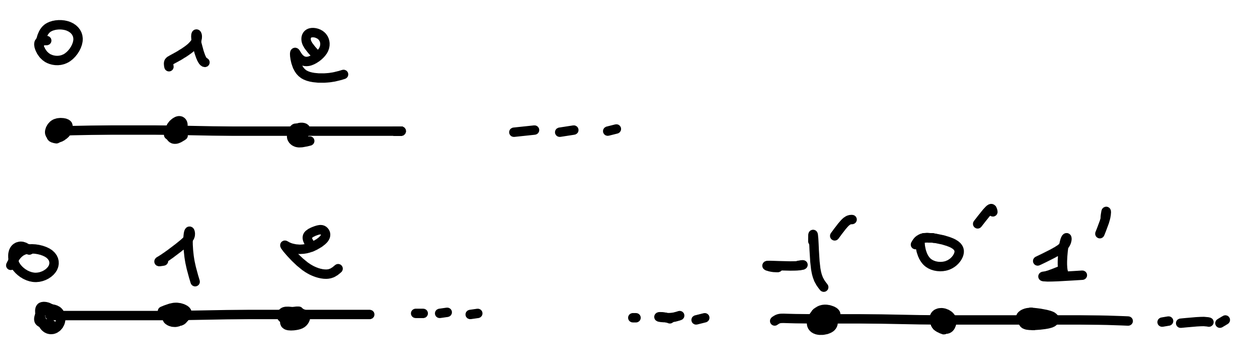
This does not defines the naturals in a unique way.

standard naturals

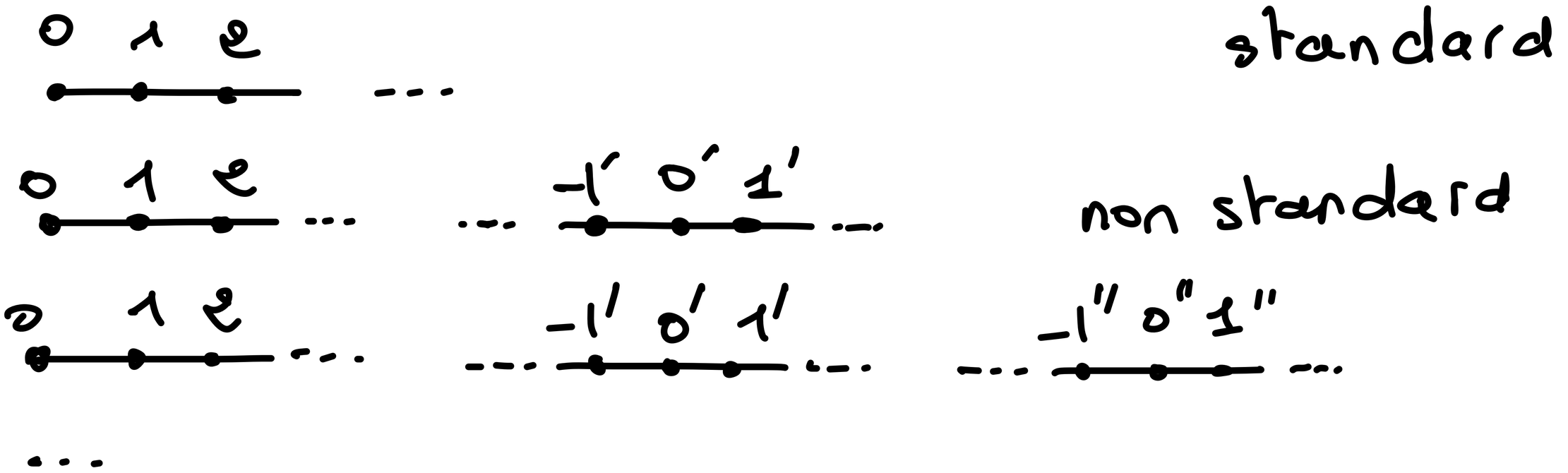


standard

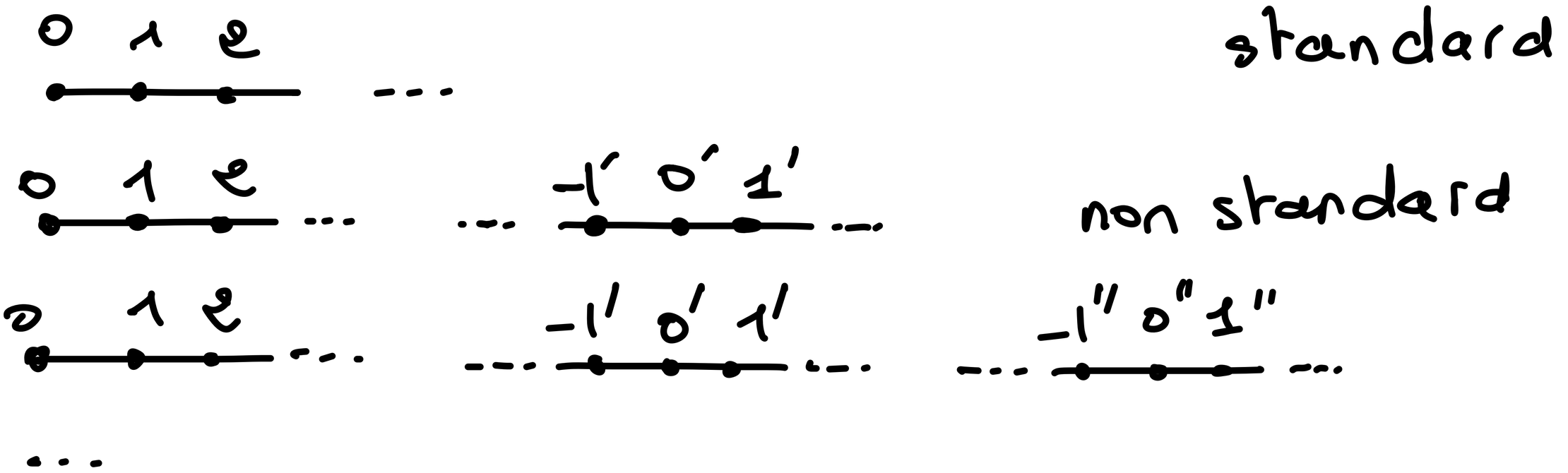
Non standard naturals (Skolem)



Non standard naturals (Skolem)



Non standard naturals (Skolem)



How did mathematicians solved the problem ?

Dedekind

The recurrence principle should be sound for naturals

This eliminates non-standard naturals

Example :

$S = \{0, 1, 2, \ldots -1', 0', 1', \ldots\}$

$\mathbb{N} \subset \{0, 1, 2, \ldots\}$ the standard naturals

we have

- $0 \in \mathbb{N}$
- $\forall n \in S.\ n \in \mathbb{N} \Rightarrow n+1 \in \mathbb{N}$

but $S \notin \mathbb{N}$

so S is not a model of Peano arithmetics

A modern solution

$$\mathbb{N} = \mathrm{lfp}^{\subseteq} \overbrace{\lambda X.\ \{0\} \cup \{n+1 \mid n \in X\}}^{F}$$

A modern solution

$$\mathbb{N} = \mathrm{lfp}^{\subseteq} \overbrace{\lambda X.\ \{0\} \cup \{n+1 \mid n \in X\}}^{F}$$

- the function F is $\subseteq$-increasing in the complete lattice of sets of natural symbool sentences $(0,\ 0+1,\ 0+1+1,\ \ldots)$

A modern solution

$$\mathbb{N} = \mathrm{lfp}^{\subseteq} \overbrace{\lambda X.\ \{0\} \cup \{n+1 \mid n \in X\}}^{F}$$

- the function F is $\subseteq$-increasing in the complete lattice of sets of natural symbool sentences (0, $0+1$, $0+1+1$, ...)
- By Tarski's fixpoint theorem
  - $\mathbb{N}$ exists
  - $\mathbb{N}$ is unique

What about the recurrence principle ?

Park induction:

$$\mathrm{lfp}^{\subseteq}_{\emptyset} F \subseteq P \Leftrightarrow \exists I.\, F(I) \subseteq I \wedge I \subseteq P$$

that is

$$\bigcup \mathcal{I} \subseteq P \Leftrightarrow \exists I.\, F(I) \subseteq I \wedge I \subseteq P$$

and $F(I) \subseteq I$ is recurrence !

Recurrence

$$F(I) \subseteq I$$

$$\Leftrightarrow \quad \{0\} \cup \{n+1 \mid n \in I\} \subseteq I$$

$$\Leftrightarrow \quad \{0\} \subseteq I \;\wedge\; \{n+1 \mid n \in I\} \subseteq I$$

$$\Leftrightarrow \quad 0 \in I \;\wedge\; \forall n \in I.\, n+1 \in I$$

so soundness and completeness of recurrence is a consequence of the fixpoint definition

Non standard axiomatic semantics

- Moore logic does not specify the domain of variables (floats or reals)
- while (true) x=x+1
  - Standard interpretation:



(state = value of x)

d

Non standard axiomatic semantics

- Hoare logic does not specify the domain of variables (floats or reals)
- while (true) x=x+1

. Standard interpretation:



(state = value of x)

. Non standard interpretation:



(the domain of traces can be non-standard naturals)

- while $(x<0)$ $x = x+1$

Non standard semantics

$$\{ n \mid n \in \mathbb{N} \}$$

$$\cup \{ -n \; -n+1 \; \cdots \; -1 \; 0 \mid n \in \mathbb{N} \}$$

$$\cup \{ \cdots \; \cdots \; -n \; \cdots \; -1 \; 0 \}$$

- while (x<0) x = x+1

Non standard semantics

$\{ \vdots^{n} \mid n \in \mathbb{N} \}$

$\cup$ $\{$  $\mid n \in \mathbb{N} \}$

$\cup$ $\{$  $\}$

The trace that never start but terminates is the symmetric of non-terminating traces that start but never terminate.

Fixpoint definition of the non-standard semantics.

For the iteration

- forward traces (finite or transfinite) can be defined by fixpoints ;
- backward traces (finite or transfinite) can be defined by fixpoints ;
- standard and non-standard semantics are a combination of the two.

(see details in the paper)

Hoare logic is an abstraction of the (non) standard semantics (Cousot, POPL &24)

Example (standard semantics)

- Σ states
- Σ^+ finite traces on states Σ
- Σ^ω infinite traces
- $\mathcal{C}$ commands of a prog. lang.
- $S[\![\mathcal{C}]\!] \in \wp(\Sigma^+ \cup \Sigma^\omega)$ standard semantics

- Transformer
  - $P \in \wp(\Sigma)$ precondition
  - $\mathrm{post}[\![S]\!]P \triangleq \{s' \in \Sigma \mid \exists s \in P, \sigma : \langle s, \sigma \rangle \to^* \langle s', \sigma \rangle \in S\}$
- Hoare logic
  - $H(C) = \{\{P\}\, C\, \{Q\} \mid P, Q \in \wp(\Sigma) \wedge \mathrm{post}[\![S[\![C]\!]]\!]P \subseteq Q\}$

$= \alpha(S[\![C]\!])$

where the abstraction α maps (non-) standard semantics to Hoare triples

Ambiguity of Hoare logic

- the abstraction α gives the same Hoare logic when applied to any standard or non-standard traces semantics

Ambiguity of Hoare logic

- the abstraction α gives the same Hoare logic when applied to any standard or non-standard traces semantics

- A frequent phenomenon in abstraction since some characteristics of the semantics are abstracted away.

Let us follow Dedekind idea :

If an axiomatization is ambiguous, add what is missing

- Moore logic is not good at handling infinite behaviors
- But it can be generalized to handle termination (Manna & Pnueli)
- We are not interested in termination but in non-termination at ∞ !

Temporary Conclusion

Axiomatic Semantics =

Hoare logic + standard trace interpretation

↑

Implicit in Hoare and Lamer work

Temporary Conclusion

Axiomatic Semantics =

Hoare logic + standard trace interpretation

↑

Implicit in Hoare and Lamer wor

Can we do better ?

YES (otherwise I would not have asked the question)

Idea : Knuth Termination Proof Method

YES (otherwise I would not have asked the question)

Idea : Knuth Termination Proof Method

- Add an integer counter (auxiliary variable) to the loop
- Initialize the counter to zero
- Increment in the loop body
- Prove (by Hoare Logic) that the counter is bounded.

- Knuth method is sound but incomplete
  (does not work for unbounded nondeterminism)

- Knuth method is sound but incomplete (does not work for unbounded nondeterminism)

- We don't care since we want to eliminate transfinite traces, not infinite ones

Preventing Non Standard Infinite Traces while (B) Sb

- The counter maps the indexes of non-standard traces to ordinals
- Requirement in axiomatic semantics:

$$\exists K \in \mathbb{N}^{+\delta} \to \mathbb{O} \text{ increasing } . \forall n \in \mathbb{N}^{+\delta} . P \wedge \mathtt{B} \Rightarrow K(n) < \omega \wedge$$
$$\forall \alpha \in \mathbb{O} . \{P \wedge \mathtt{B} \wedge K(n) = \alpha\} \, \mathtt{Sb} \, \{P \wedge K(n+1) = \alpha \oplus 1\}$$

(kf)

non-standard time (anything satisfying Peano axioms)

non-standard successor

ordinal addition

Preventing Nonstandard Infinite Backward or Forward Traces

while (B) Sb

↓ backward time, anything with 0 and predecessor

$$\exists K \in \mathbb{N}^{-\delta} \to \mathbb{O} \text{ decreasing (antitone) } . \forall n \in \mathbb{N}^{-\delta} . \forall \alpha \in \mathbb{O}$$

$$\{P \wedge \mathtt{B} \wedge K(n) = \alpha \oplus 1\}\, \mathtt{Sb}\, \{P \wedge K(n+1) = \alpha\} \wedge$$

$$(P \wedge K(n) = 0) \Rightarrow \neg \mathtt{B} \wedge \bigcup_{n \in \mathbb{N}^{-0}} K(n) < \omega \qquad (K_b)$$

- Decrease at each step
- Exit on 0
- Bounded by ω

Axiomatic semantics =

Hoare Logic

+ Forward and Backward Execution w- boundedness (K_f) & (K_b)

Practical consequences ?

Do we have to redo all of our proofs in Hoare Logic ?

Practical consequences ?

Do we have to redo all of our proofs in Hoare Logic ?

No because the non-standard requirement (K) always holds for standard trace semantics

Conclusion

- Tony Hoare always "postulated", and so did Edger Dijkstra

Conclusion

- Tony Hoare always "postulated", and so did Edger Dijkstra
- Postulating is great but sometimes ambiguous

  Exemple : Euclidian / Hyperbolic / Elliptic geometries

Conclusion

- Tony Hoare always "postulated", and so did Edger Dijkstra
- Postulating is great but sometimes ambiguous
  Exemple : Euclidian / Hyperbolic / Elliptic geometries
- The problem can be solved for axiomatic semantics (with no practical consequences :)

THE END

THANK YOU