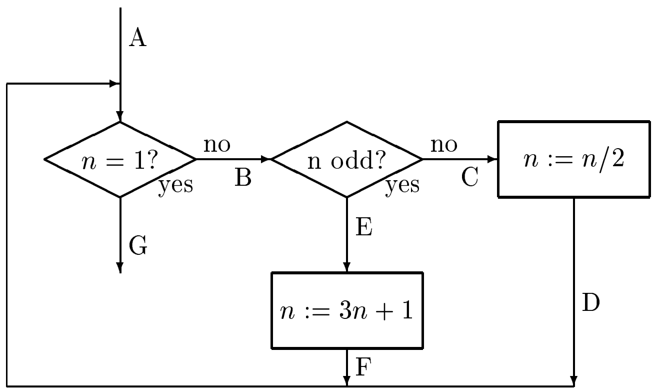
approximation-abstraction
non-standard execution on abstraction values using abstract operators
$a \sqsubseteq a'$ a is more precise, a is not as abstract as a'
safe, sound, conservative, correct
semantics-based
homomorphic, semi-homomorphic

$$\begin{tikzcd} 2^{Store} \arrow[r] \arrow[d] & 2^{Store} \arrow[d] \\ \text{Abs} \arrow[r] & \sqsupseteq \end{tikzcd}$$

Example:



n=5	A	B	C	D	E	F	G
	$\{5\}$	$\{5$ 16 8 4 $2\}$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\{1\}$
	odd	T	...	...	...	...	odd

naïve analysis: terminating? "enough" input values
$\Rightarrow$ instead compute on domain {even, odd}
need: semantics of non-standard execution and compare it with the original semantics
idea: standard execution as a special case of non-standard
Cousot '77: Collecting semantics (Accumulating semantics)
program point $\longmapsto$ set of all possible stores reachable.
(given: initial program point, initial set of stores S_0)

store: $Var \longrightarrow Val$, Store: Val^{Var} is the set of all stores
$< 2^{Store}, \subseteq >$ complete lattice
pair of abstraction-meaning function (monotone):
$\alpha : < 2^{Store}, \subseteq > \longrightarrow < Abs, \sqsubseteq >$ monotone, abstraction
$\gamma : < Abs, \sqsubseteq > \longrightarrow < 2^{Store}, \subseteq >$ monotone, meaning
$acc(p) = \{s : Var \to Val \mid < p, s > = next^i(< p_0, s_0 >), s_0 \in S_0, i \in \mathbb{N}\}$
$< acc(A), \ldots, acc(G) >$ least solution of fixpoint equation

$acc(A) = S_0$
$acc(B) = acc(A) \cap \{s | s(n) \neq 1\}$
$acc(C) = acc(B) \cap \{s | s(n) even\}$
$acc(D) = f_{n/2}(acc(C))$
$\vdots$
$acc(G) = (acc(A) \cup acc(D) \cup acc(F)) \cap \{s | s(n) = 1\}$ $< \{< s_1, \ldots, s_7 > | s_1, \ldots, s_7 \in 2^{Store}\}, \subseteq' >$ is also a complete lattice. When the lattice is complete, there is always a least solution for a fixpoint equation.

$\mu X.F(X) = X$
$\bot \cup F(\bot) \cup F^2(\bot) \cup \ldots$
iterative computation of lfp (least fixpoint) does not terminate
idea: apply abstraction α to sets involved in equation to obtain new equation over abstract lattice $< Abs, \sqsubseteq >$.
$acc^{\#}(A) = \alpha(S_0) \qquad (= odd \text{ if } S_0 = \{5\})$
$acc^{\#}(B) = acc^{\#}(A) \sqcap \top$
$acc^{\#}(C) = \ldots$
$acc^{\#}(D) = f^{\#}_{n/2}(acc^{\#}(C))$
$\vdots$

α :
$S \mapsto odd \qquad \text{if } s \subseteq \{odd \text{ value}\}$
$S \mapsto even \qquad \text{if } s \subseteq \{even \text{ value}\}$
$S \mapsto \bot \qquad \text{if } s = \emptyset$
$S \mapsto \top \qquad \text{otherwise } (S \cap even \neq \emptyset; S \cap odd \neq \emptyset)$

γ :
$odd \mapsto \{odd \text{ numbers}\}$
$even \mapsto \{even \text{ numbers}\}$
$\bot \mapsto \emptyset$
$\top \mapsto \mathbb{N}$

γ is not the inverse function of α, cause α is not injective.

$f^{\#}_{n/2}$:
$odd \mapsto \top$
$even \mapsto \top$
$\bot \mapsto \bot$
$\top \mapsto \top$

if α was homomorphic, then $acc^{\#}(pp) = \alpha(acc(pp))$ but α is <u>not</u> homomorphic:
$$\underbrace{\underbrace{\alpha(S_1)}_{\{2\}} \sqcap \underbrace{\alpha(S_2)}_{\{4\}}}_{even} \neq \underbrace{\alpha(S_1 \cap S_2)}_{\bot} \Rightarrow \alpha(S_1) \sqcap \alpha(S_2) \sqsupseteq \alpha(S_1 \cap S_2)$$
We will have $acc^{\#}(pp) \sqsupseteq \alpha(acc(pp))$