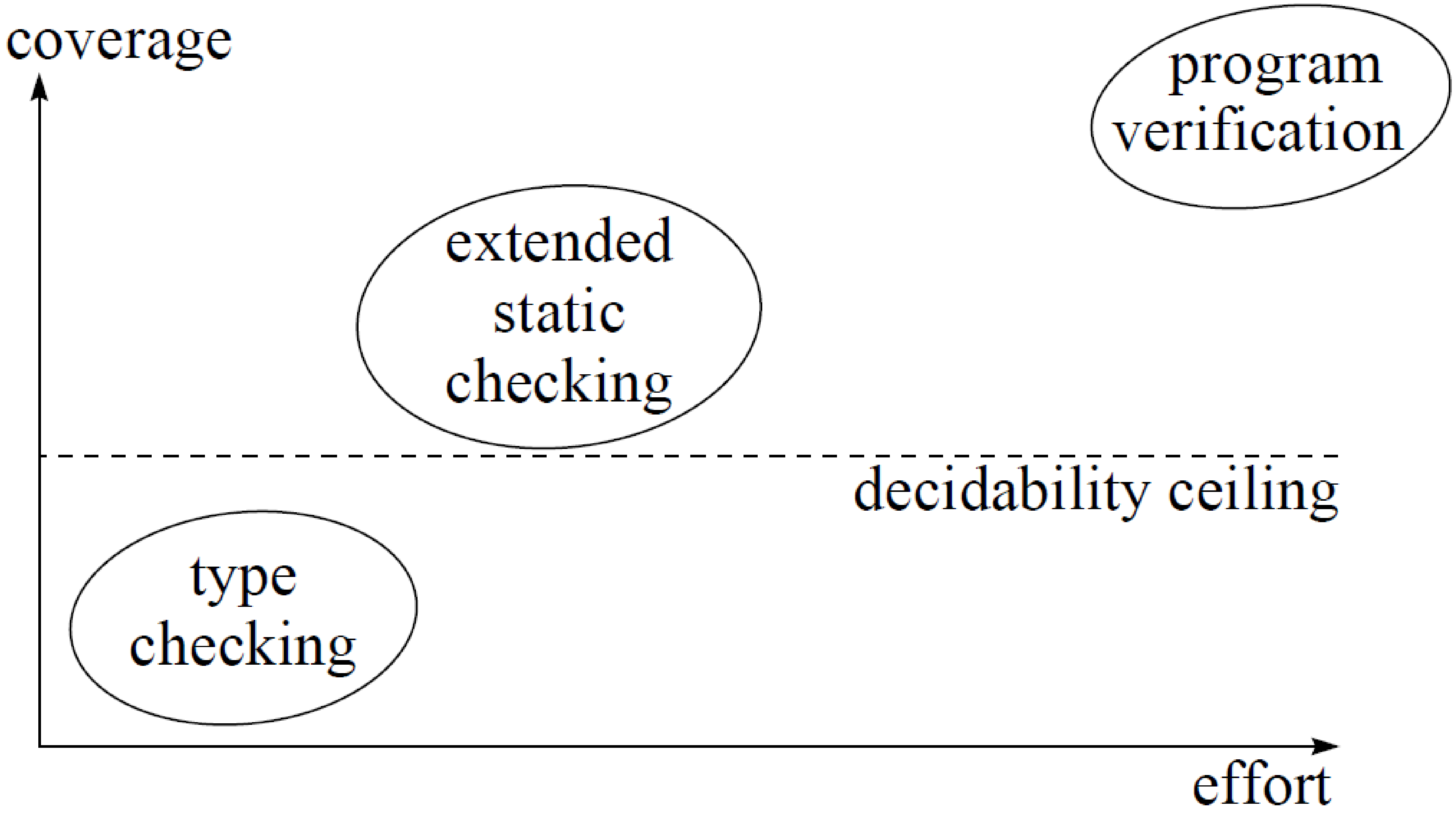
Program Verification with Dafny

Benedikt Maderbacher

IAIK – Graz University of Technology
firstname.lastname@iaik.tugraz.at


coverage
program verification
extended static checking
decidability ceiling
type checking
effort

Interactive Theorem Prover

- Checks if a program is correct
  - with help of from the user
- User provides:
  - annotations
  - manual proofs for some properties

Interactive Theorem Provers

- Dafny
  - Hoare Logic
- Coq, Lean, Agda, F*
  - Depended Type Theory
- Isabelle/HOL, HOL Light
  - Higher Order Logic

Applications

- CompCert
  - A verified compiler (Coq)
- seL4
  - A verified micro kernel (Isabelle/HOL)
- Project Everest
  - A verified network stack (multiple)

Demo: Dafny

Total Correctness

- Proof that a program is correct and terminates.
- Show that a loop can't run forever.

Total Correctness

Assignment axiom for total correctness

$$\vdash \ [P[E/V]]\ V := E\ [P]$$

Precondition strengthening for total correctness

$$\frac{\vdash\ P \Rightarrow P', \qquad \vdash\ [P']\ C\ [Q]}{\vdash\ [P]\ C\ [Q]}$$

Postcondition weakening for total correctness

$$\frac{\vdash\ [P]\ C\ [Q'], \qquad \vdash\ Q' \Rightarrow Q}{\vdash\ [P]\ C\ [Q]}$$

Conditional rule for total correctness

$$\frac{\vdash\ [P \wedge S]\ C_1\ [Q], \qquad \vdash\ [P \wedge \neg S]\ C_2\ [Q]}{\vdash\ [P]\ \texttt{IF}\ S\ \texttt{THEN}\ C_1\ \texttt{ELSE}\ C_2\ [Q]}$$

Sequencing rule for total correctness

$$\frac{\vdash\ [P]\ C_1\ [Q], \qquad \vdash\ [Q]\ C_2\ [R]}{\vdash\ [P]\ C_1 ; C_2\ [R]}$$

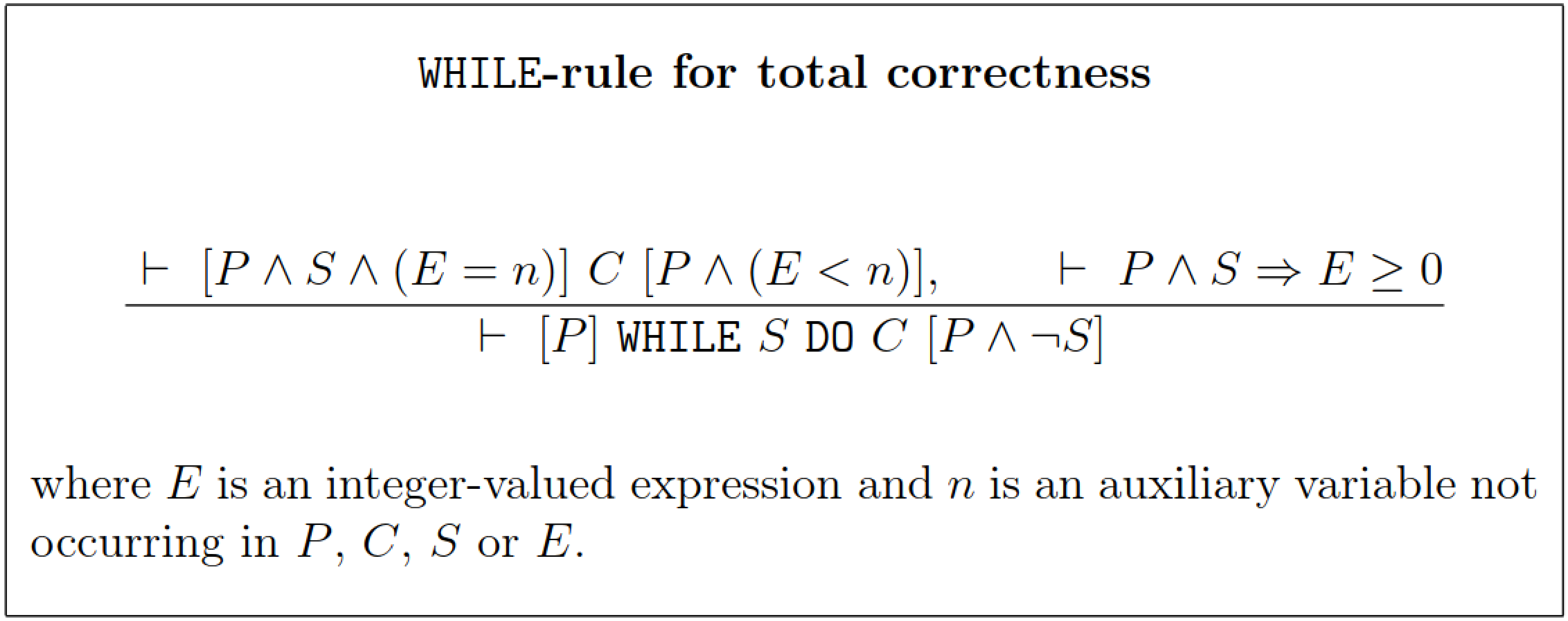
Total Correctness

- Proof that a program is correct and terminates.

- Use a *variant* to show a loop can’t run forever.

- In Dafny this is annotated with `decreases`.

Total Correctness



WHILE-rule for total correctness

$$\frac{\vdash\ [P \wedge S \wedge (E = n)]\ C\ [P \wedge (E < n)], \qquad \vdash\ P \wedge S \Rightarrow E \geq 0}{\vdash\ [P]\ \texttt{WHILE}\ S\ \texttt{DO}\ C\ [P \wedge \neg S]}$$

where E is an integer-valued expression and n is an auxiliary variable not occurring in P, C, S or E.

Total Correctness

Assignment axiom for total correctness

$$\vdash \; [P[E/V]] \; V := E \; [P]$$

- Only works if E terminates!
- All functions calls must terminate.
  - Can be done similar to while loops.

Frame Rules

- Define what areas of the heap a method/function may access.
- `reads`
  - What a function/predicate can read.
- `modifies`
  - What a method can write

Frame Rules

- Local reasoning over mutable state.
- Make proofing larger programs feasible.