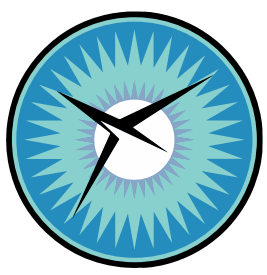
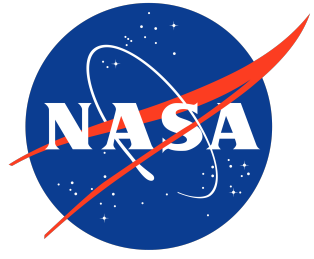
VSCode-PRECiSA: a Toolkit for Floating-Point Round-Off Error Analysis

Paolo Masci

joint work with
Laura Titolo, Mariano Moscato, Marco A. Feliu,
and Aaron Dutle





NIA/NASA LaRC

Motivations

- Round-off errors = difference between $\mathbb{R}$ and its $\mathbb{F}$ representation
  $\Rightarrow$ computed $\mathbb{F}$ result $\neq$ expected $\mathbb{R}$ result
- Unstable guards = $\mathbb{F}$ control-flow $\neq$ $\mathbb{R}$ control-flow
- Possible catastrophic consequences in safety-critical aviation software:
  - ADS-B Compact Position Reporting (CPR) $\Rightarrow$ position errors as large as 360 nmi
  - Air traffic conflict and collision avoidance systems $\Rightarrow$ resolution maneuvers that are not implicitly coordinated
  - Geofencing in autonomous UAS $\Rightarrow$ incorrect determination of being inside/outside a geofence, even when the aircraft is far from the boundary

PRECiSA

- PRECiSA is a framework for the analysis of floating-point programs
  - computes round-off error bounds
    + formal proof of their correctness
  - generates stable C code from a real specification instrumented to detect unstable guards
- PRECiSA command line not appropriate to
  - test different inputs
  - run the analysis with different options
  - inspect analysis results

PRECiSA Analysis

Input: program $\widetilde{P}$ = set of floating-point function declarations $\tilde{f}$

Output: for each $\tilde{f}$ find a round-off error bound e such that

$$|\tilde{f} - f_{\mathbb{R}}| \leq e$$

PRECiSA Analysis

Input: program $\widetilde{P}$ = set of floating-point function declarations $\tilde{f}$

Output: for each $\tilde{f}$ find a round-off error bound e such that

$$|\tilde{f} - f_{\mathbb{R}}| \leq e$$

Challenges:

- e should be tight (no coarse over-estimations)

  $\Rightarrow$ symbolic expressions + Kodiak global optimizer

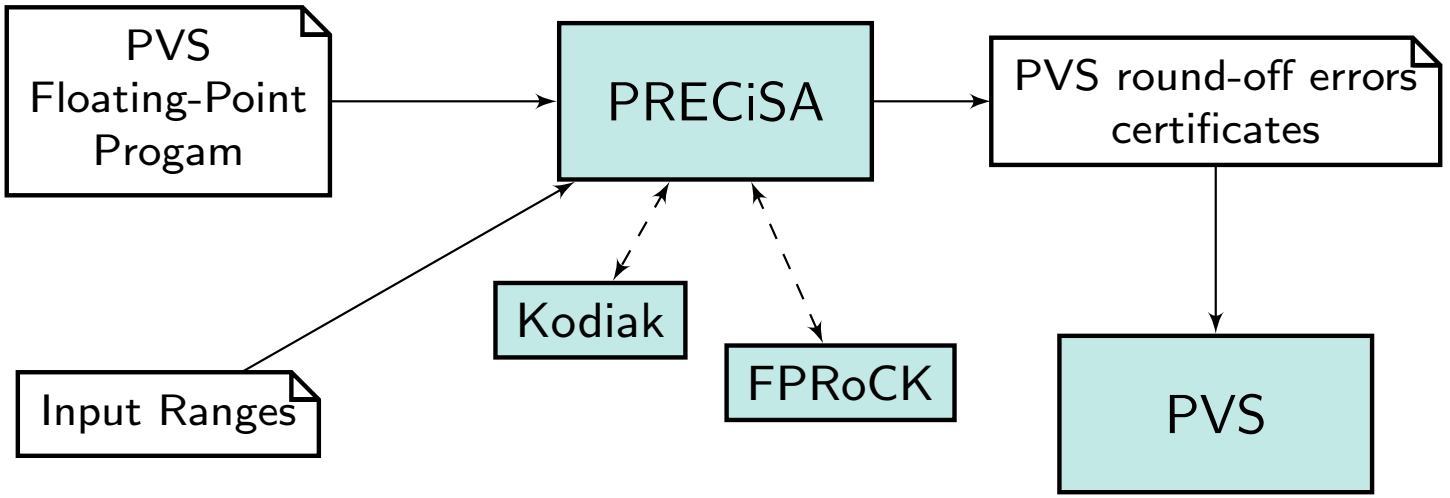
- correctly bound the rounding errors in conditionals

  $\Rightarrow$ generation of PVS certificates

- sound approximation of if-then-else

  $\Rightarrow$ abstract domain that collect the information on both real and fp path conditions

PRECiSA-Round-off Error Static Analysis



- PRECiSA supports basic arithmetic operators, trigonometric functions, log, exp, let-in expressions, conditionals, and function calls
- abstraction α to avoid the combinatorial explosion due to nested conditionals
- widening ∇_k to converge for recursive programs
- PVS certificates ensuring the correctness of the bounds
- FPRoCK checks for UNSAT conditions that can be discarded

VSCode-PRECiSA

- VSCode-PRECiSA is a toolkit that integrates PRECiSA in Visual Studio Code
- User-friendly graphical interface
- It provides different analysis views:
  - sensitivity analysis
  - interval analysis
  - comparative analysis
  - unstable conditionals analysis

VSCode-PRECiSA: Demo

nl_comp.pvs > nl_comp

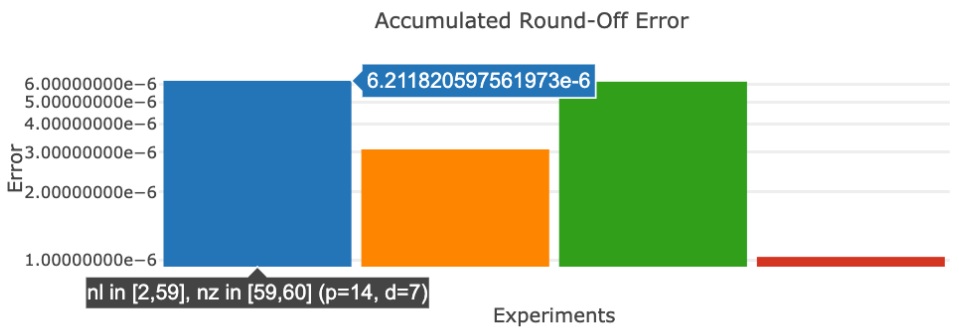
typecheck-file | evaluate-in-pvsio

```
1   nl_comp: THEORY
2
3   BEGIN
4
5   IMPORTING float@aerr754dp
6
7   % @fp-function
8   % @fp-range nl in [2,59], nz in [59,60]
    estimate-error-bounds | compare-error-bounds
9   nl_comp(nl, nz: double): double =
10    (180/3.14) *
11        acos(sqrt((1-cos(3.14/(2*nz)))
12                  /(1-cos(2*3.14/nl))))
13
14  END nl_comp
```

INPUT	MIN	MAX
nl	2	59
nz	59	60

Analyze

Save Results



Experiment	Accumulated Round-Off Error
nl in [2,59], nz in [59,60] (p=14, d=7)	6.211820597561973e-6
nl in [2,30], nz in [59,60] (p=14, d=7)	3.0859761662809845e-6
nl in [30,59], nz in [60,60] (p=14, d=7)	6.155897062805878e-6
nl in [2,10], nz in [60,60] (p=14, d=7)	1.0310720739119004e-6

Conclusions

VSCode-PRECiSA is tool that integrates PRECiSA in VSCode

- round-off error bounds + formal proof of their correctness
- different analysis views to help the developer understand how rounding-error affect the result
- NASA Open Source Agreement (`https://github.com/nasa/PRECiSA/tree/master/vscode-precisa`)
- What's next? Support PRECiSA stable C code generation from a PVS real specification

Thanks for your attention!