A Verified Certificate Checker for Floating-Point Error Bounds

Heiko Becker, MPI-SWS, Germany
Eva Darulova, MPI-SWS, Germany
Magnus O. Myreen, Chalmers University of Technology, Sweden
Floating-Point Computations have errors

\[ f = 4 \times 0.1 - 0.1 \quad \text{f : double} = 4 \times 0.1 - 0.1; \]
Floating-Point Computations have errors

\[ f = 4 \times 0.1 - 0.1 \]

\[ 0.3 \]
Floating-Point Computations have errors

\[ f = 4 \times 0.1 - 0.1 \]

0.3 \neq 0.30000000000000004
Floating-Point Computations have errors

\[ f = 4 \times 0.1 - 0.1 \]

\[ f : \text{double} = 4 \times 0.1 - 0.1; \]

\[ 0.3 \neq 0.30000000000000004 \]

roundoff error

\[ | f - \tilde{f} | \leq \varepsilon \]
Floating-Point Computations have errors

\[ f = 4 \times x - 0.1 \quad \text{double} \quad \text{f} = 4 \times x - 0.1; \]

roundoff error

\[ \max_{x} | f - \tilde{f} | \leq \varepsilon \]
Daisy: A Static Analyzer

\[ f: \text{real valued function} \rightarrow \text{Static Analyzer} \rightarrow \tilde{f}: \text{floating point function} \]

\[ \varepsilon: \text{roundoff error} \]
Daisy: A Static Analyzer

$f$: real valued function

Static Analyzer

$\tilde{f}$: floating point function
$\varepsilon$: roundoff error

>8k Lines of Scala Code
Daisy: A Static Analyzer

$f: \text{real valued function}$ → $\tilde{f}: \text{floating point function}$

$\varepsilon: \text{roundoff error}$

$>8k \text{ Lines of Scala Code}$

Is the computed roundoff error $\varepsilon$ correct?
Checking Certificates For Floating-Point Error Bounds

\[ f: \text{real valued function} \rightarrow \text{Static Analyzer} \rightarrow \tilde{f}: \text{floating point function} \]

\[ \epsilon: \text{roundoff error} \]

Certificate for \( f, \tilde{f}, \epsilon \)
Checking Certificates For Floating-Point Error Bounds

\( f : \text{real valued function} \) → **Static Analyzer** → \( \tilde{f} : \text{floating point function} \)

**Certificate for \( f, \tilde{f}, \varepsilon \)**

**Certificate Checker**
Checking Certificates For Floating-Point Error Bounds

\( f: \text{real valued function} \)  \quad \rightarrow \quad \text{Static Analyzer} \quad \rightarrow \quad \tilde{f}: \text{floating point function} \\
\epsilon: \text{roundoff error}
Checking Certificates For Floating-Point Error Bounds

$f$: real valued function

Static Analyzer

$\tilde{f}$: floating point function
$\varepsilon$: roundoff error

Certificate for $f$, $\tilde{f}$, $\varepsilon$

Certificate Checker

$|f - \tilde{f}| \leq \varepsilon$
Extraction using the CakeML compiler toolchain

Certificate Checker

CORRECT BUT SLOW
Extraction using the CakeML compiler toolchain

Certificate Checker
CORRECT BUT SLOW

CakeML Compiler
Extraction using the CakeML compiler toolchain

Certificate Checker

CORRECT BUT SLOW

CakeML Compiler

x64 Certificate Checker
Extraction using the CakeML compiler toolchain

Certificate Checker
CORRECT BUT SLOW

CakeML Compiler

x64 Certificate Checker
Extraction using the CakeML compiler toolchain

Certificate Checker

CORRECT BUT SLOW

CakeML Compiler

FAST AND CORRECT

x64 Certificate Checker
We built a verified Certificate Checker for Floating Point roundoff errors.

Future Work:
• Use CertiCoq to extract from Coq
• Connect to CompCert and CakeML

More on:
https://mpi-sws.org/~hbecker

Come talk to me or send me a mail:
hbecker@mpi-sws.org