Verification of Numerical Programs

From Real Numbers to Floating Point Numbers

Alwyn Goodloe, César Muñoz
(NASA)

Florent Kirchner, Löıc Correnson
(CEA)

Long Term Objective

In the domain of separation assurance systems for Air Traffic Management, transform, **in a cost effective way**, a formally verified algorithm that uses real arithmetic into a formally verified software code that uses floating point arithmetic.

Preliminary Approach

1. Transform **PVS** algorithms and specifications into C code and ACSL annotations.
2. Instrument the code with computation errors.
3. Find correct values for these errors using **Gappa**.
4. Lift PVS real-number proofs as axioms in ACSL and verify C code in **Frama-C**.

Case study: Airborne Coordinated Conflict Resolution and Detection (**ACCoRD**)

- ACCoRD is a framework for designing, verifying, and implementing separation assurance algorithms, e.g., Conflict Detection, Conflict Resolution, Conflict Prevention, Conflict Recovery.
- ACCoRD consists of more 9K lines of PVS (including 1500 lemmas) and 21K lines of code (Java, C++).

Current Status

- Formally verified soundness of 2D conflict detection algorithm implemented in C (IEEE 754 Floating Point Standard).
- Working on more sophisticated algorithms.
- Automation, automation, automation.