Dutle, Aaron; Moscato, Mariano; Titolo, Laura; Muñoz, César; Anderson, Gregory; Bobot, François

**Formal analysis of the compact position reporting algorithm.** (English) Zbl 1458.68273


Summary: The Automatic Dependent Surveillance-Broadcast (ADS-B) system allows aircraft to communicate current state information, including position and velocity messages, to other aircraft in their vicinity and to ground stations. The Compact Position Reporting (CPR) algorithm is the ADS-B protocol responsible for the encoding and decoding of aircraft positions. CPR is sensitive to computer arithmetic since it relies on functions that are intrinsically unstable such as floor and modulus. In this paper, a formal verification of the CPR algorithm is presented. In contrast to previous work, the algorithm presented here encompasses the entire range of message types supported by ADS-B. The paper also presents two implementations of the CPR algorithm, one in double-precision floating-point and one in 32-bit unsigned integers, which are both formally verified against the real-number algorithm. The verification proceeds in three steps. For each implementation, a version of CPR, which is simplified and manipulated to reduce numerical instability and leverage features of the datatypes, is proposed. Then, the Prototype Verification System (PVS) is used to formally prove real conformance properties, which assert that the ideal real-number counterpart of the improved algorithm is mathematically equivalent to the standard CPR definition. Finally, the static analyzer Frama-C is used to verify software conformance properties, which say that the software implementation of the improved algorithm is correct with respect to its idealized real-number counterpart. In concert, the two properties guarantee that the implementation meets the original specification. The two implementations will be included in the revised version of the ADS-B standards document as the reference implementation of the CPR algorithm.

**MSC:**
- 68U35 Computing methodologies for information systems (hypertext navigation, interfaces, decision support, etc.)
- 65Y04 Numerical algorithms for computer arithmetic, etc.
- 68P30 Coding and information theory (compaction, compression, models of communication, encoding schemes, etc.) (aspects in computer science)
- 68Q60 Specification and verification (program logics, model checking, etc.)
- 68W40 Analysis of algorithms

**Keywords:**
- formal analysis; finite precision computation; compact position reporting algorithm; Frama-C; PVS

**Software:**
- PVS; Gappa; ACSL; Frama-C; PRECiSA; cvc3; z3; ASTREE

**Full Text:** DOI

**References:**


