HOL (Higher-order logic) systems [3] are a family of interactive theorem proving tools, widely used for creating formal specifications of systems, and for proving properties about them. They have been deployed in both industry and academia to support formal reasoning in many areas, including hardware and software verification. The underlying logic and basic facilities are completely general. In principle they can be used to support any project that can be defined in higher-order logic, an expressive logic originally developed as a foundation for mathematics. In [1] Audenaert extends this family with one more descendant: Formath. When formal methods are used to increase the reliability of software systems, the result directly depends on the correctness of the proof system that supports the application of the formal methods. It is shown that Formath is equiconsistent to Hol-4 and Hol-Light. Formath stands out from the latter, in using a deduction calculus based on sequents of the form \( \Gamma_1 \vdash \Gamma_2 \), where \( \Gamma_1 \) and \( \Gamma_2 \) represent finite sets of formulas, and in using a pert constant \( C^{\text{EXT}} \) of type \((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta) \rightarrow \alpha\) in the formulation of the Extensionality axiom: 

\[
\forall f, g. f(C^{\text{EXT}} fg) = g(C^{\text{EXT}} fg) \rightarrow f = g.
\]

Note that \( C^{\text{EXT}} fg \) represents a term \( t \) such that \( ft \) differs from \( gt \) (if such a \( t \) exists). Hence Extensionality reads as follows: two functions are equal if they coincide on their “difference”. In [1] Formath is used for the specification and verification of Alfred programs (see [2]).

References


Ghent University, Galglaan 2, B-9000 Gent, Belgium