Refutation of differential Hoare logics with Isabelle/HOL

Abstract: We evaluate the ordering of $K$ essential to Kleene algebra with test (KAT). It is not tautologous, but the basis for other conjectures: differential dynamic logic (dL); differential Hoare logic; Morgan-style differential refinement calculus; reasoning with evolution; and verification conjectures formalized in Isabelle/HOL. These results form a non tautologous fragment of the universal logic $VŁŁ$. We assume the method and apparatus of Meth8/VŁŁ with $T$ autology as the designated proof value, $F$ as contradiction, $N$ as truthity (non-contingency), and $C$ as falsity (contingency). The 16-valued truth table is row-major and horizontal, or repeating fragments of 128-tables, sometimes with table counts, for more variables. (See ersatz-systems.com.)

We present simple new Hoare logics and refinement calculi for hybrid systems in the style of differential dynamic logic. (Refinement) Kleene algebra with tests is used for reasoning about the program structure and generating verification conditions at this level. Lenses capture hybrid program stores in a generic algebraic way. The approach has been formalised with the Isabelle/HOL proof assistant.

1 Introduction Differential dynamic logic (dL) is a prominent deductive method for verifying hybrid systems. It extends dynamic logic with domain-specific inference rules for reasoning about the discrete control and continuous dynamics that characterise such systems. Continuous evolutions are modelled by dL’s evolution commands within a hybrid program syntax. These declare a vector field and a guard, which is meant to hold along the evolution. Reasoning with evolution commands in dL requires either explicit solutions to differential equations represented by the vector field, or invariant sets that describe these evolutions implicitly. Verification components inspired by dL have already been formalised in the Isabelle proof assistant.

2 Kleene algebra with tests A Kleene algebra with tests (KAT) is a structure $(K,B,+,:,0,1,\cdot,\neg)$ where $(B,+,:,0,1,\neg)$ is a boolean algebra with meet $\cdot$, complementation $\neg$, least element 0 and greatest element 1, $B \subseteq K$, and $(K,+,::0,1,\cdot)$ is a Kleene algebra—a semiring with idempotent addition equipped with a star operation that satisfies the axioms $1+\alpha \cdot \alpha \leq \alpha \cdot \alpha$ and $\gamma+\alpha \cdot \beta \leq \beta \rightarrow \alpha \cdot \gamma \leq \beta$, as well as their opposities [sic], with multiplication swapped. As idempotent semirings are semilattices the ordering on $K$ is defined by

$$\alpha \leq \beta \leftrightarrow \alpha + \beta = \beta$$
LET \( p, q \): \( \alpha, \beta \).

\[(\neg (q \prec p) = ((p + q) = q) \mid \text{TFFT TFFT TFFT TFFT} \quad (2.5.2)\]

**Remark 2.5.2:** Eq. 2.5.2 as rendered is *not* tautologous. The refutes the ordering of \( K \), essential to Kleene algebra with test (KAT) as the basis for other conjectures: differential dynamic logic (dL); differential Hoare logic; Morgan-style differential refinement calculus; “reasoning with evolution”; and verification conjectures formalized in Isabelle/HOL.