“A la Burstall” intermittent assertions induction principles for proving inevitability properties of programs. (English summary)


A property $\psi$ is inevitable for a program $p$ iff each execution of $p$ necessarily passes through a state satisfying $\psi$. Total correctness and termination are examples of inevitable properties. By modeling programs as sets of execution traces, which makes the study independent of any particular programming language and applicable to a wide range of parallel and nondeterministic programs, the authors formalize and generalize the original Burstall intermittent assertions method [R. M. Burstall, in *Information processing 74* (Stockholm, 1974), 308–312, North-Holland, Amsterdam, 1974; MR0448980 (56 #7285); Z. Manna and R. J. Waldinger, Comm. ACM **21** (1978), no. 2, 159–172; MR0483642 (58 #3630)]. The generalization consists primarily of using transfinite induction (to capture unbounded nondeterminism), introducing auxiliary variables, and allowing certain ternary intermittent assertions relating state values on program entry and at two time instants. Several different formulations of the induction principle are proved sound, semantically complete, and equivalent.

Reviewed by *Sergey G. Vorobyov* (Saarbrücken)

© Copyright American Mathematical Society 1995, 2008