Notre Dame Journal of Formal Logic
Volume 26, Number 1, January 1985

A Completeness Theorem for Dynamic Logic

LÁSZLÓ CSIRMAZ

Introduction Let t be a similarity type and denote by F_t^n the set of first-order formulas of type t which have their free variables among $\{x_i : i < n\}$. Let $\theta \subset F_t^0$ be a fixed consistent theory. A program (or rather a program scheme as defined in [11]) is a prescription which defines the possible next moment states from the present state, i.e., the program is a state transducer. (A state can be imagined as the collection of the contents of the memory registers used by the program.) If this prescription is not unique, i.e., if the program executor may choose more than one possibility, then the program is said to be nondeterministic. We are interested only in programs which can be represented by a formula $\phi \in F_t^{2n}$ with $n > 0$ and $\theta \vdash \forall x \exists y \phi(x,y)$. The states are the n-tuples of the elements of the underlying set A of some t-type structure $\mathbf{A}$ for which $\mathbf{A} \models \theta$ holds. The state $y \in A^n$ is a possible successor of the state $x \in A^n$ iff $\mathbf{A} \models \phi(x,y)$. The constraints $\mathbf{A} \models \theta$ and $\theta \vdash \forall x \exists y \phi(x,y)$ ensure that for every state there exists at least one successor state.

Particularly, the so-called *while*-programs with random assignments of the form $x := ?$ (meaning: set x to any value in the domain; cf. [9]) are of this kind, provided there are infinitely many definable elements in θ (cf. [1], [2], [12]).

The function $R : \omega \to A^n$ is a *standard run* of the program ϕ, if $\mathbf{A} \models \phi(R(i), R(i+1))$ for every $i \in \omega$. The run *halts* at the i-th step if $R(i) = R(i+1)$. A run, of course, may have several different halting configurations. Detailed intuitive motivations for these definitions can be found in [3], [5], and [12].

Given two formulas, ϕ_{in} and ϕ_{out} of F_t^n (called the input and output assertion, respectively), the program ϕ is partially correct with respect to ϕ_{in} and ϕ_{out} if for every t-type model $\mathbf{A}$ of θ and for every run $R : \omega \to A^n$, $\mathbf{A} \models \phi_{in}(R(0))$ and $R(i) = R(i+1)$ imply $\mathbf{A} \models \phi_{out}(R(i))$.

The inductive assertion method introduced by Floyd [7] and reformulated later by Hoare [10] is the most commonly used method for proving partial

Received June 6, 1982; revised January 9, 1984