Bulletin of the **S**ection of **L**ogic
Volume 9/3 (1980), pp. 131–133

reedition 2010 [original edition, pp. 131–135]

László Csirmaz

REMARKS ON FLOYD-HOARE DERIVABILITY

This is an abstract of my paper "Programs and program verification in a general setting" submitted to Theoretical Computer Science.

ω denotes the set of natural numbers. Let $X = \{x_i : i \in \omega\}$ be the set of variables, L_t be the set of classical first order formulas of some type t (cf. [2]) possibly with free variables (elements of X). Let $L_t^n \subseteq L_t$ be the set of formulas the free variables of which are among $\{x_i : i < n\}$, in particular L_t^0 denotes the set of formulas without free variables (the set of sentences). Let $T \subset L_t^0$ be a consistent theory.

Definition 1. The formula $\varphi \in L_t^{2n}$ is a *program* if

$$T \vdash \forall x_1 \ldots \forall x_n \exists! y_1 \ldots \exists! y_n \varphi(x_1, \ldots, y_n).$$

In the sequel we shall use vector notations and we write, for example, $\forall \overrightarrow{x} \exists! \overrightarrow{y} \varphi(\overrightarrow{x}, \overrightarrow{y})$ instead of the formula above.

Evidently, our definition of program generalizes the usual notion of flow-chart programs, cf. [3]. Roughly speaking, this definition expresses the fact that if the program uses exactly n registers (including the statement counter) then their content at some moment determines uniquely the content of the registers at the next moment.

By this definition every program φ defines a function p_φ which assigns n-tuples to n-tuples in such a way that $p_\varphi(\overrightarrow{x}) = \overrightarrow{y}$ iff $\varphi(\overrightarrow{x}, \overrightarrow{y})$. From now on we identify the programs with these functions and write "let p be a program", etc. which means "let φ be a program and denote by p the function defined by φ", The function symbol p will occur in formulas, but these formulas can evidently be rewritten using φ instead.

Let $\underline{A}$ be a t-type model of T, i.e. $\underline{A} \models T$. Let A be the universe of $\underline{A}$, and $[A]^n$ be the set of n-tuples of elements of A.

DEFINITION 2. Let p be a program, $\overrightarrow{q_0} = \langle q_0^1, \ldots, q_0^n \rangle \in [A]^n$ and $R \subseteq [A]^n$. R is a *run* of the program p starting from $\overrightarrow{q_0}$ if

(i): $\overrightarrow{q_0} \in R$ and $p(\overrightarrow{q}) \in R$ for every $\overrightarrow{q} \in R$

(ii): for every formula $\Phi \in L_t^n$, $\underline{A} \models \Phi(\overrightarrow{q_0})$ and $\underline{A} \models \Phi(\overrightarrow{q}) \to \Phi(p(\overrightarrow{q}))$ for every $\overrightarrow{q} \in R$ implies $\underline{A} \models \Phi(\overrightarrow{q})$ for every $\overrightarrow{q} \in R$.

The $\overrightarrow{q} \in R$ is a *haltingpoint* of R if $p(\overrightarrow{q}) = \overrightarrow{q}$.

Evidently, this definition of run generalizes the definition of continuous trace in [1] which cannot be formulated in general in the lack of any ordering.

DEFINITION 3. Let φ_{in} and $\varphi_{out} \in L_t^n$ be arbitrary. The program p is *partially correct* w.r.t. φ_{in} and φ_{out} denoted by $\models^{pc} (\varphi_{in}, p, \varphi_{out}))$ if for every model $\underline{A}$ of T and for every run $R \subseteq [A]^n$ of p starting from $\overrightarrow{q_0} \in R$, $\underline{A} \models \varphi_{in}(\overrightarrow{q_0})$ implies $\underline{A} \models \varphi_{out}(\overrightarrow{q})$ for every halting point $\overrightarrow{q}$ of R.

DEFINITION 4. Let φ_{in} and φ_{out} as above. The program p is Floyd-Hoare derivable w.r.t. φ_{in} and φ_{out} (Denoted by $\vdash^{FH} (\varphi_{in}, p, \varphi_{out})$) if there exists a formula $p \in L_t^n$ such that

$T \vdash \forall \overrightarrow{x} (\varphi_{in}(\overrightarrow{x}) \to \Phi(\overrightarrow{x}))$
$T \vdash \forall x (\Phi(\overrightarrow{x}) \to \Phi(p(\overrightarrow{x})))$
$T \vdash \forall x (\Phi(\overrightarrow{x})\ \&\ p(\overrightarrow{x}) = \overrightarrow{x} \to \varphi_{out}(\overrightarrow{x}))$

THEOREM 1. *For every theory T, every program p and every formula φ_{in} and φ_{out}*

$$\models^{pc} (\varphi_{in}, p, \varphi_{out}) \text{ iff } \vdash^{FH} (\varphi_{in}, p, \varphi_{out}).$$

Let PA consist of the Peano axioms ([2], p. 41). In [1] this theorem was proved in that special case when $PA \subset T$ (and of course, the type t contains the type of arithmetic). The following theorem tells why the Peano axioms have played such a distinguished role previously.

THEOREM 2. *Suppose the type t contains the type of arithmetic and $PA \subset T$. Let p be a program, $R \subseteq [A]^n$ be a run of p starting from $\overrightarrow{q_0}$ in the model $\underline{A}$ of T. Then the halting points of R have the same type. (I.e. if $\overrightarrow{q}$, $\overrightarrow{r} \in R$ are halting points then for every $\psi \in L_t^n$. $\underline{A} \models \psi(\overrightarrow{q}) \leftrightarrow \psi(\overrightarrow{r})$.) Moreover if we have a formula $\varphi_0 \in L_t^n$ such that $T \vdash \exists! \overrightarrow{x} \varphi_0(\overrightarrow{x})$ and $\underline{A} \models \varphi_0(\overrightarrow{q_0})$ then R has at most one halting point.*

Finally we give an example (without proof) for a run which has two halting points of different type. Let the type t consist of "$+, S, O, \tau$" with arities "$2, 1, 0, 0$" (i.e. t is the type of additive number theory, cf. [2], p. 43 with a new constant symbol) and let $T = PA \cap L_t^0$ (i.e. just the axioms of PA which does not contain the symbol "$\cdot$"). The program p operates on pairs and is defined by

$$p(x, y) = \begin{cases} (x - 2y - 1, y + 1) & \text{if } x - 2y - 1 \geqq 0 \\ (x, y) & \text{otherwise.} \end{cases}$$

It is trivial that p is a program in T. Now let $\underline{A}$ be any non-standard model of PA, and $a \in A$ be divisible by every standard element. We interpret τ as to be a^2, this gives a t-type model for T. Let

$$R = \{(2ia + a - i^2, a - i) : i \in \omega\} \cup \{(2ia - i^2, a - i) : 0 \leqq i \leqq a\}.$$

We claim that R is the wanted run. It starts from tha pair $(a^2, 0)$ which is defined uniquely by the formula $(x = \tau \ \& \ y = 0) \in L_t^2$, and it has two halting points, namely (a, a) and $(0, a)$.

References

[1] H. Andréka and I. Németi, *Completeness of Floyd Logic*, **Bulletin of the Section of Logic**, Vol. 7 (1978), pp. 115–120.

[2] C. C. Chang and H. J. Keisler, **Model theory**, North Holland, 1973.

[3] Z. Mann, **Mathematical theory of computation**, McGraw Hill, 1974.

Mathematical Institute of the
Hunagarian Academy of Sciences
Budapest, Reáltanoda u. 13–15
Hungary