Bulletin of the **S**ection of **L**ogic
Volume 7/3 (1978), pp. 115–119

reedition 2011 [original edition, pp. 115–120]

Hajnal Andréka
István Németi

COMPLETENESS OF FLOYD LOGIC

This is an abstract of our paper "A characterisation of Floyd-provable programs" submitted to Theoretical Computer Science.

ω denotes the set of natural numbers.

$Y =^d \{y_i : i \in \omega\}$ is the set of *variable symbols*. L denotes the set of classical first order formulas of type t (cf. [2]) possibly with free variables (elements of Y), where t is the similarity type of arithmetic, i.e. it consists of "$+, \cdot, 0, 1$" with arities "$2, 2, 0, 0$".

I. The definition of Floyd logic

1. Syntax

The set U of commands is:

$(j : y \leftarrow \tau) \in U$	if $j \in \omega, y \in Y$ and τ is a t-type term
$(j :$ IF χ THEN $v) \in U$	if $j, v \in \omega$ and $\chi \in L$ is a formula without quantifiers

These are the only elements of U.

The set P of *programs* is:

$$P =^d \{\langle (i_0 : u_0), \ldots, (i_n : u_n)\rangle \in U^n : n \in \omega, i_k \neq i_l \text{ if } k \neq l\},$$

i.e. a program is a finite sequence of commands in which no two members have the same "label".

The set of *Floyd statements* is defined as:

$$S_F =^d \{(p,\psi) : p \in P, \psi \in L \text{ and all free variables of } \psi \text{ occur in } p\}.$$

CONVENTIONS: Throughout this paper $p \in P$ is arbitrary and the letters n, i_m, u_m denote parts of p as follows:

$$p =^d \langle (i_0 : u_0), \ldots, (i_n : u_n) \rangle \text{ and } i_{n+1} =^d min(\omega \backslash \{i_m : m \leqslant n\}).$$

Further, V_p denotes the variables (elements of Y) occurring in p.

2. Semantics

First we define continuous traces of a program in a classical model of L.

Let $\underline{A}$ be a t-type model; A denotes its universe, cf. [2].

A continuous trace of a program p in $\underline{A}$ is a sequence $\langle (l_a, q_a) \rangle_{a \in A}$, indexed by the elements of A, such that (i)-(iii) below are satisfied:

(i): $l_a \in \omega$ and $q_a : V_p \to A$ is a valuation, for every $a \in A$.

(ii): $l_0 = i_0$ and for every $a \in A$

$$(l_{a+1}, q_{a+1}) = (l_a, q_a) \text{ if } l_a \notin \{i_m : m \leqslant n\},$$

else denoting by m the number for which $l_a = i_m$

a. if $u_m =$ "$y_w \leftarrow \tau$", then

$$l_{a+1} = i_{m+1} \text{ and } q_{a+1}(y_j) = \begin{cases} q_a(y_j) & \text{if } j \neq w, \\ \tau[q_a]_{\underline{A}} & \text{if } j = w \end{cases}$$

where $\tau[q_a]_{\underline{A}}$ denote the value of the term τ in $\underline{A}$ at the valuation q_a (cf. [2], p. 27).

b. if $u_m =$ "IF χ THEN v", then

$$q_{a+1} = q_a \text{ and } l_{a+1} = \begin{cases} v & \text{if } \underline{A} \models \chi[q_a] \text{ cf. [2], p. 27)} \\ i_{m+1} & \text{otherwise.} \end{cases}$$

(iii): If for every $a \in A$ the valuation g_a is defined as:

$$g_a(y_j) =^d \begin{cases} l_a & \text{if } j = min\{k : y_k \notin V_p\} \\ q_a(y_j) & \text{if } y_j \in V_p \end{cases}$$

then $\langle g_a \rangle_{a \in A}$ satisfies the induction axioms, i.e. for every $\varphi \in L$ with free variables in V_p

$$\underline{A} \models ((\varphi[g_0] \wedge \bigwedge_{a \in A} (\varphi[g_a] \rightarrow \varphi[g_{a+1}])) \rightarrow \bigwedge_{a \in A} \varphi[g_a]).$$

Now, a Floyd statement $(p, \psi) \in S_F$ is said to be *partially correct* w.r.t. continuous traces in $\underline{A}$ (denoted by $\underline{A} \models^{pc} (p, \psi)$)
iff
for any continuous trace $\langle (l_a, q_a) \rangle_{a \in A}$ of p in $\underline{A}$ and
for any $a \in A : l_a \notin \{i_m : m \leqslant n\}$ implies $\underline{A} \models \psi[q_a]$.

3. Derivation system (rules of inference)

In the following we recall the so called Floyd-Hoare derivation system. This system serves to derive pairs (p, ψ) from theories $T \subseteq L$.

Let $(p, \psi) \in S_F$ and $T \subseteq L$.

The set of labels of p is defined as:

$$lab(p) =^d \{i_m : m \leqslant n+1\} \cup \{v : (\exists m \leqslant n) u_m = \text{"IF } \chi \text{ THEN } v\text{"}\}.$$

Note that $lab(p)$ is finite.

Now, a *Floyd-Hoare derivation* of (p, ψ) from T consists of:
a mapping $\Phi : lab(p) \rightarrow L$
together with classical first order derivations listed in (i)-(iv) below:

(i): A derivation
$T \vdash \Phi(i_0)$

(ii): To each command $(i_m : y_j \leftarrow \tau)$ occurring in p a derivation:
$T \vdash (\Phi(i_m) \rightarrow \Phi(i_{m+1})(y_j/\tau))$
where $\varphi(y/\tau)$ denotes the formula obtained from φ by substituting τ in place of y in the usual way.

(iii): To each command $(i_m : \text{IF } \chi \text{ THEN } v)$ occurring in p derivations:
$T \vdash ((\chi \wedge \Phi(i_m)) \rightarrow \Phi(v))$
$T \vdash ((\neg\chi \wedge \Phi(i_m)) \rightarrow \Phi(i_{m+1}))$

(iv): To each $z \in (lab(p) \backslash \{i_m : m \leqslant n\})$ a derivation:
$T \vdash (\Phi(z) \rightarrow \psi)$

Now the existence of a Floyd-Hoare derivation of (p, ψ) from T is denoted by $T \vdash^{FH} (p, \psi)$.

II. Completeness of Floyd logic

Let PA'consist of the Peano axioms (cf. [2], p. 42) together with the additional axiom

$$\begin{aligned}
\Pi =^d \text{“}(\forall x, b, t, n)(\exists x', b')\\
((\forall i \leqslant t)(\forall r, r')\,((\exists z[(1{+}(i{+}1)b)z + r = x \wedge r < 1{+}(i{+}1)b] \wedge\\
\wedge \exists z[(1{+}(i{+}1)b')z + r' = x' \wedge r' < 1{+}(i{+}1)b'] \rightarrow\\
\rightarrow r = r')) \wedge\\
\wedge \exists z[(1{+}(t{+}2)b')z{+}n = x' \wedge n < 1{+}(t{+}2)b'])\text{”}.
\end{aligned}$$

$\underline{N}$ denotes the standard model of arithmetic.

Note that $\Pi \in L$ and $\underline{N} \models PA'$.

Theorem 1. (Completeness) *Let $T \supseteq PA'$ be arbitrary.*

Now, for every $(p, \psi) \in S_F$:

(p, ψ) is Floyd-Hoare derivable from T iff
(p, ψ) is partially correct w.r.t. continuous traces in every model of T, i.e.
$T \vdash^{FH} (p, \psi)$ if and only if $T \models^{pc} (p, \psi)$.

Definition. Let $(p, \psi) \in S_F$.

1. (p, ψ) is *partially correct w.r.t. standard traces* in $\underline{A}$
   iff
   for any trace $\langle (l_a, q_a) \rangle_{a \in A}$ of p in $\underline{A}$ and for any standard element m of A,
   if $l_m \notin \{i_z : z \leqslant n\}$ then $\underline{A} \models \psi[q_m]$.
2. p *terminates* in $\underline{A}$ for standard data *in standard time*
   iff
   for any trace $\langle (l_a, q_a) \rangle_{a \in A}$ of p in $\underline{A}$ such that all values of the function $q_0 : V_p \rightarrow A$ are standard there is a standard element m of A such that
   $l_m \notin \{i_z : z \leqslant n\}$.

Theorem 2. (Necessity of nonstandard time) *Let $T \subseteq L$ be recursively enumerable and let $\underline{N} \models T$, $T \supseteq PA$. Now there exists $(p,\psi) \in S_F$ such that (i)-(iii) below are true.*

(i): (p,ψ) *is partially correct w.r.t. standard traces in every model of T.*
(ii): *p terminates in every model of T for standard data in standard time.*
(iii): $T \not\vdash^{FH} (p,\psi)$,
i.e. there is no Floyd-Hoare derivation of (p,ψ) from T.

References

[1] Z. Manna, **Mathematical theory of computation**, McGraw-Hill 1974.
[2] C. C. Chang and H. J. Keisler, **Model Theory**, North-Holland 1973.

Mathematical Institute of the
Hungarian Academy of Sciences