FORMALIZED MATHEMATICS
Vol. 26, No. 2, Pages 159–164, 2018
DOI: 10.2478/forma-2018-0013

sciendo
https://www.sciendo.com/

An Inference System of an Extension of Floyd-Hoare Logic for Partial Predicates

Ievgen Ivanov
Taras Shevchenko National University
Kyiv, Ukraine

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Mykola Nikitchenko
Taras Shevchenko National University
Kyiv, Ukraine

Summary. In the paper we give a formalization in the Mizar system [2, 1] of the rules of an inference system for an extended Floyd-Hoare logic with partial pre- and post-conditions which was proposed in [7, 9]. The rules are formalized on the semantic level. The details of the approach used to implement this formalization are described in [5].

We formalize the notion of a semantic Floyd-Hoare triple (for an extended Floyd-Hoare logic with partial pre- and post-conditions) [5] which is a triple of a pre-condition represented by a partial predicate, a program, represented by a partial function which maps data to data, and a post-condition, represented by a partial predicate, which informally means that if the pre-condition on a program's input data is defined and true, and the program's output after a run on this data is defined (a program terminates successfully), and the post-condition is defined on the program's output, then the post-condition is true.

We formalize and prove the soundness of the rules of the inference system [9, 7] for such semantic Floyd-Hoare triples. For reasoning about sequential composition of programs and while loops we use the rules proposed in [3].

The formalized rules can be used for reasoning about sequential programs, and in particular, for sequential programs on nominative data [4]. Application of these rules often requires reasoning about partial predicates representing pre- and post-conditions which can be done using the formalized results on the Kleene algebra of partial predicates given in [8].

MSC: 68Q60 68T37 03B70 03B35

ISSN 1426–2630(Print), 1898-9934(Online)

Keywords: Floyd-Hoare logic; Floyd-Hoare triple; inference rule; program verification

MML identifier: NOMIN_3, version: 8.1.08 5.53.1335

From now on v, x denote objects, D, V, A denote sets, n denotes a natural number, p, q denote partial predicates of D, and f, g denote binominative functions of D.

Let us consider D, f, and p. We say that f coincides with p if and only if

(Def. 1) for every element d of D such that $d \in \operatorname{dom} p$ holds $f(d) \in \operatorname{dom} p$.

Let us consider g and q. We say that f and g coincide with p and q if and only if

(Def. 2) for every element d of D such that $d \in \operatorname{rng} f$ and $g(d) \in \operatorname{dom} q$ holds $d \in \operatorname{dom} p$.

Now we state the propositions:

(1) f coincides with $\bot_{\mathrm{PP}}(D)$.

(2) $\mathrm{id}_{\mathrm{PP}}(D)$ coincides with p.

Let us consider D, p, and q. We say that $p \models q$ if and only if

(Def. 3) for every element d of D such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ holds $d \in \operatorname{dom} q$ and $q(d) = \mathit{true}$.

Observe that the predicate is reflexive.

In the sequel D denotes a non empty set, d denotes an element of D, f, g denote binominative functions of D, and p, q, r, s denote partial predicates of D.

Now we state the propositions:

(3) If $p \models r$, then $p \wedge q \models r$.

(4) $p \wedge q \models p$.

(5) If $p \models q$ and $r \models s$, then $p \wedge r \models q \wedge s$.

(6) If $p \vee q \models r$, then $p \models r$.

(7) Suppose $p \models q \vee r$. If $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$, then $d \in \operatorname{dom} q$ and $q(d) = \mathit{true}$ or $d \in \operatorname{dom} r$ and $r(d) = \mathit{true}$.

(8) $p \vee p \models p$.

(9) If $p \models q$ and $r \models s$, then $p \vee r \models q \vee s$.

(10) If $p \vee q \models r$, then $p \wedge q \models r$.

Let us consider D. The functor SemanticFloydHoareTriples(D) yielding a set is defined by the term

(Def. 4) $\{\langle p, f, q\rangle$, where p, q are partial predicates of D, f is a binominative function of D : for every element d of D such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} f$ and $f(d) \in \operatorname{dom} q$ holds $q(f(d)) = \mathit{true}\}$.

We introduce the notation SFHTs(D) as a synonym of SemanticFloydHoareTriples(D).

Now we state the propositions:

(11) Suppose $\langle p, f, q\rangle \in$ SFHTs(D). If $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} f$ and $f(d) \in \operatorname{dom} q$, then $q(f(d)) = \mathit{true}$.

(12) $\langle \emptyset, f, p\rangle \in$ SFHTs(D).

Let us consider D. Observe that SFHTs(D) is non empty.

A semantic Floyd-Hoare triple of D is an element of SemanticFloydHoareTriples(D).

An SFHT of D is an element of SFHTs(D). Now we state the propositions:

(13) $\langle p, \mathrm{id}_{\operatorname{dom} p}, p\rangle$ is an SFHT of D.

(14) $\langle p, \mathrm{id}_{\mathrm{field}\, f}, p\rangle$ is an SFHT of D.

(15) CONS$_1$ RULE:
If $\langle p, f, q\rangle$ is an SFHT of D and $r \models p$, then $\langle r, f, q\rangle$ is an SFHT of D. The theorem is a consequence of (11).

(16) CONS$_2$ RULE:
Suppose $\langle p, f, q\rangle$ is an SFHT of D and $q \models r$ and $\operatorname{dom} r \subseteq \operatorname{dom} q$. Then $\langle p, f, r\rangle$ is an SFHT of D. The theorem is a consequence of (11).

(17) SKIP RULE:
$\langle p, \mathrm{id}_{\mathrm{PP}}(D), p\rangle$ is an SFHT of D.

(18) $\langle \mathrm{false}_{\mathrm{PP}}(D), f, p\rangle$ is an SFHT of D.

(19) INVERSION RULE:
If p is total, then $\langle \sim p, f, q\rangle$ is an SFHT of D. The theorem is a consequence of (18) and (15).

(20) COMPOSITION RULE:
Suppose $\langle p, f, q\rangle$ is an SFHT of D and $\langle q, g, r\rangle$ is an SFHT of D and f and g coincide with q and r. Then $\langle p, f \bullet g, r\rangle$ is an SFHT of D.
PROOF: Set $F = f \bullet g$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} r$ holds $r(F(d)) = \mathit{true}$. $\square$

(21) IF RULE:
Suppose $\langle r \wedge p, f, q\rangle$ is an SFHT of D and $\langle \neg r \wedge p, g, q\rangle$ is an SFHT of D. Then $\langle p, \mathrm{IF}(r, f, g), q\rangle$ is an SFHT of D.
PROOF: Set $F = \mathrm{IF}(r, f, g)$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} q$ holds $q(F(d)) = \mathit{true}$. $\square$

(22) If f coincides with p and $\langle p, f, p\rangle$ is an SFHT of D, then $\langle p, f^n, p\rangle$ is an SFHT of D.
PROOF: Define $\mathcal{P}$[natural number] $\equiv \langle p, f^{\$_1}, p\rangle$ is an SFHT of D. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural

number k, $\mathcal{P}[k]$. $\square$

(23) WHILE RULE:
Suppose f coincides with p and $\operatorname{dom} p \subseteq \operatorname{dom} f$ and $\langle r \wedge p, f, p\rangle$ is an SFHT of D. Then $\langle p, \mathrm{WH}(r, f), \neg r \wedge p\rangle$ is an SFHT of D.
PROOF: Set $F = \mathrm{WH}(r, f)$. Set $q = \neg r \wedge p$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} q$ holds $q(F(d)) = \mathit{true}$. $\square$

(24) UNCONDITIONAL COMPOSITION RULE (USEQ):
Suppose $\langle p, f, q\rangle$ is an SFHT of D and $\langle q, g, r\rangle$ is an SFHT of D and $\langle \sim q, g, s\rangle$ is an SFHT of D. Then $\langle p, f \bullet g, r \vee s\rangle$ is an SFHT of D.
PROOF: Set $F = f \bullet g$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom}(r \vee s)$ holds $(r \vee s)(F(d)) = \mathit{true}$. $\square$

(25) UNCONDITIONAL WHILE RULE (UWH):
Suppose $\langle r \wedge p, f, p\rangle$ is an SFHT of D and $\langle r \wedge \sim p, f, p\rangle$ is an SFHT of D. Then $\langle p, \mathrm{WH}(r, f), \neg r \wedge p\rangle$ is an SFHT of D.
PROOF: Set $F = \mathrm{WH}(r, f)$. Set $q = \neg r \wedge p$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} q$ holds $q(F(d)) = \mathit{true}$. $\square$

(26) DP RULE:
Suppose $\langle p, f, r\rangle$ is an SFHT of D and $\langle q, f, r\rangle$ is an SFHT of D. Then $\langle p \vee q, f, r\rangle$ is an SFHT of D.
PROOF: Set $P = p \vee q$. For every d such that $d \in \operatorname{dom} P$ and $P(d) = \mathit{true}$ and $d \in \operatorname{dom} f$ and $f(d) \in \operatorname{dom} r$ holds $r(f(d)) = \mathit{true}$. $\square$

In the sequel p, q denote partial predicates over simple-named complex-valued nominative date of V and A, f, g denote binominative functions over simple-named complex-valued nominative date of V and A, E denotes a (V,A)-FPrg-yielding finite sequence, e denotes an element of $\prod E$, and d denotes a nominative data with simple names from V and complex values from A.

Now we state the proposition:

(27) Suppose for every nominative data d with simple names from V and complex values from A such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} f$ and $f(d) \in \operatorname{dom} q$ holds $q(f(d)) = \mathit{true}$. Then $\langle p, f, q\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.
PROOF: For every element d of $\mathrm{ND}_{\mathrm{SC}}(V, A)$ such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} f$ and $f(d) \in \operatorname{dom} q$ holds $q(f(d)) = \mathit{true}$. $\square$

(28) ASSIGNMENT RULE:
$\langle \mathrm{S_P}(p, f, v), \mathrm{Asg}^v(f), p\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.
PROOF: Set $P = \mathrm{S_P}(p, f, v)$. Set $F = \mathrm{Asg}^v(f)$. For every d such that $d \in \operatorname{dom} P$ and $P(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} p$ holds

$p(F(d)) = \mathit{true}$ by [6, 34]. $\square$

(29) SFID_1 RULE:
$\langle \mathrm{S}_{\mathrm{P}}(p, f, v), \mathrm{S}_{\mathrm{F}}(\mathrm{id}_{\mathrm{PP}}(\mathrm{ND}_{\mathrm{SC}}(V, A)), f, v), p\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.
PROOF: Set $I = \mathrm{id}_{\mathrm{PP}}(\mathrm{ND}_{\mathrm{SC}}(V, A))$. Set $P = \mathrm{S}_{\mathrm{P}}(p, f, v)$. Set $F = \mathrm{S}_{\mathrm{F}}(I, f, v)$. For every d such that $d \in \mathrm{dom}\, P$ and $P(d) = \mathit{true}$ and $d \in \mathrm{dom}\, F$ and $F(d) \in \mathrm{dom}\, p$ holds $p(F(d)) = \mathit{true}$. $\square$

(30) SFID RULE:
Suppose $\prod E \neq \emptyset$. Then $\langle \mathrm{S}_{\mathrm{P}}(p, e, E), \mathrm{S}_{\mathrm{F}}(\mathrm{id}_{\mathrm{PP}}(\mathrm{ND}_{\mathrm{SC}}(V, A)), e, E), p\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.
PROOF: Set $I = \mathrm{id}_{\mathrm{PP}}(\mathrm{ND}_{\mathrm{SC}}(V, A))$. Set $P = \mathrm{S}_{\mathrm{P}}(p, e, E)$. Set $F = \mathrm{S}_{\mathrm{F}}(I, e, E)$. For every d such that $d \in \mathrm{dom}\, P$ and $P(d) = \mathit{true}$ and $d \in \mathrm{dom}\, F$ and $F(d) \in \mathrm{dom}\, p$ holds $p(F(d)) = \mathit{true}$. $\square$

(31) SF_1 RULE:
Suppose $\langle p, \mathrm{S}_{\mathrm{F}}(\mathrm{id}_{\mathrm{PP}}(\mathrm{ND}_{\mathrm{SC}}(V, A)), g, v) \bullet f, q\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. Then $\langle p, \mathrm{S}_{\mathrm{F}}(f, g, v), q\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.
PROOF: Set $I = \mathrm{id}_{\mathrm{PP}}(\mathrm{ND}_{\mathrm{SC}}(V, A))$. Set $F = \mathrm{S}_{\mathrm{F}}(f, g, v)$. Set $G = \mathrm{S}_{\mathrm{F}}(I, g, v)$. Set $C = G \bullet f$. For every d such that $d \in \mathrm{dom}\, p$ and $p(d) = \mathit{true}$ and $d \in \mathrm{dom}\, C$ and $C(d) \in \mathrm{dom}\, q$ holds $q(C(d)) = \mathit{true}$. For every d such that $d \in \mathrm{dom}\, p$ and $p(d) = \mathit{true}$ and $d \in \mathrm{dom}\, F$ and $F(d) \in \mathrm{dom}\, q$ holds $q(F(d)) = \mathit{true}$. $\square$

(32) SF RULE:
Suppose $\prod E \neq \emptyset$ and $\langle p, \mathrm{S}_{\mathrm{F}}(\mathrm{id}_{\mathrm{PP}}(\mathrm{ND}_{\mathrm{SC}}(V, A)), e, E) \bullet f, q\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. Then $\langle p, \mathrm{S}_{\mathrm{F}}(f, e, E), q\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.
PROOF: Set $I = \mathrm{id}_{\mathrm{PP}}(\mathrm{ND}_{\mathrm{SC}}(V, A))$. Set $F = \mathrm{S}_{\mathrm{F}}(f, e, E)$. Set $G = \mathrm{S}_{\mathrm{F}}(I, e, E)$. Set $C = G \bullet f$. For every d such that $d \in \mathrm{dom}\, p$ and $p(d) = \mathit{true}$ and $d \in \mathrm{dom}\, C$ and $C(d) \in \mathrm{dom}\, q$ holds $q(C(d)) = \mathit{true}$. For every d such that $d \in \mathrm{dom}\, p$ and $p(d) = \mathit{true}$ and $d \in \mathrm{dom}\, F$ and $F(d) \in \mathrm{dom}\, q$ holds $q(F(d)) = \mathit{true}$. $\square$

REFERENCES

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[3] Ievgen Ivanov and Mykola Nikitchenko. On the sequence rule for the Floyd-Hoare logic with partial pre- and post-conditions. In *Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume II: Workshops, Kyiv, Ukraine, May 14–17, 2018*, volume 2104 of *CEUR Workshop Proceedings*, pages 716–724, 2018.

[4] Ievgen Ivanov, Mykola Nikitchenko, Andrii Kryvolap, and Artur Korniłowicz. Simple-named complex-valued nominative data – definition and basic operations. *Formalized Mathematics*, 25(**3**):205–216, 2017. doi:10.1515/forma-2017-0020.

[5] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. Implementation of the composition-nominative approach to program formalization in Mizar. *The Computer Science Journal of Moldova*, 26(1):59–76, 2018.

[6] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. On an algorithmic algebra over simple-named complex-valued nominative data. *Formalized Mathematics*, 26(2):149–158, 2018. doi:10.2478/forma-2018-0012.

[7] Artur Korniłowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. An approach to formalization of an extension of Floyd-Hoare logic. In Vadim Ermolayev, Nick Bassiliades, Hans-Georg Fill, Vitaliy Yakovyna, Heinrich C. Mayr, Vyacheslav Kharchenko, Vladimir Peschanenko, Mariya Shyshkina, Mykola Nikitchenko, and Aleksander Spivakovsky, editors, *Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, Kyiv, Ukraine, May 15–18, 2017*, volume 1844 of *CEUR Workshop Proceedings*, pages 504–523. CEUR-WS.org, 2017.

[8] Artur Korniłowicz, Ievgen Ivanov, and Mykola Nikitchenko. Kleene algebra of partial predicates. *Formalized Mathematics*, 26(**1**):11–20, 2018. doi:10.2478/forma-2018-0002.

[9] Andrii Kryvolap, Mykola Nikitchenko, and Wolfgang Schreiner. Extending Floyd-Hoare logic for partial pre- and postconditions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications: 9th International Conference, ICTERI 2013, Kherson, Ukraine, June 19–22, 2013, Revised Selected Papers*, pages 355–378. Springer International Publishing, 2013. ISBN 978-3-319-03998-5. doi:10.1007/978-3-319-03998-5_18.

Accepted June 29, 2018