FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 189–195, 2019
DOI: 10.2478/forma-2019-0018

sciendo
https://www.sciendo.com/

Partial Correctness of a Power Algorithm

Adrian Jaszczak
Institute of Informatics
University of Białystok
Poland

Summary. This work continues a formal verification of algorithms written in terms of simple-named complex-valued nominative data [6],[8],[15],[11],[12],[13]. In this paper we present a formalization in the Mizar system [3],[1] of the partial correctness of the algorithm:

```
i := val.1
j := val.2
b := val.3
n := val.4
s := val.5
while (i <> n)
   i := i + j
   s := s * b
return s
```

computing the natural `n` power of given complex number `b`, where variables `i, b, n, s` are located as values of a `V-valued Function`, `loc`, as: `loc/.1 = i`, `loc/.3 = b`, `loc/.4 = n` and `loc/.5 = s`, and the constant `1` is located in the location `loc/.2 = j` (set `V` represents simple names of considered nominative data [17]).

The validity of the algorithm is presented in terms of semantic Floyd-Hoare triples over such data [9]. Proofs of the correctness are based on an inference system for an extended Floyd-Hoare logic [2],[4] with partial pre- and post-conditions [14],[16],[7],[5].

MSC: 68Q60 68T37 03B70 03B35

Keywords: power; nominative data; program verification

MML identifier: `NOMIN_6`, version: `8.1.09 5.57.1355`

Let D be a set and f_1, f_2, f_3, f_4, f_5 be binominative functions of D. The functor PP-composition$(f_1, f_2, f_3, f_4, f_5)$ yielding a binominative function of D is defined by the term

(Def. 1) PP-composition$(f_1, f_2, f_3, f_4) \bullet f_5$.

From now on D denotes a non empty set, f_1, f_2, f_3, f_4, f_5 denote binominative functions of D, and p, q, r, t, w, u denote partial predicates of D.

Now we state the proposition:

(1) Unconditional composition rule for 5 programs: Suppose $\langle p, f_1, q\rangle$ is an SFHT of D and $\langle q, f_2, r\rangle$ is an SFHT of D and $\langle r, f_3, w\rangle$ is an SFHT of D and $\langle w, f_4, t\rangle$ is an SFHT of D and $\langle t, f_5, u\rangle$ is an SFHT of D and $\langle \sim q, f_2, r\rangle$ is an SFHT of D and $\langle \sim r, f_3, w\rangle$ is an SFHT of D and $\langle \sim w, f_4, t\rangle$ is an SFHT of D and $\langle \sim t, f_5, u\rangle$ is an SFHT of D. Then $\langle p, \text{PP-composition}(f_1, f_2, f_3, f_4, f_5), u\rangle$ is an SFHT of D.

In the sequel d, v, v_1 denote objects, V, A denote sets, i, j, b, n, s, z denote elements of V, i_1, j_1, b_1, n_1, s_1 denote objects, d_1, L_2, L_3, L_1, L_4, L_5 denote non-atomic nominative data of V and A, and D_2, D_3, D_1, D_4, D_5 denote binominative functions over simple-named complex-valued nominative date of V and A.

Now we state the propositions:

(2) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $D_2 = i_1 \Rightarrow_a$ and $D_3 = j_1 \Rightarrow_a$ and $D_1 = b_1 \Rightarrow_a$ and $D_4 = n_1 \Rightarrow_a$ and $D_5 = s_1 \Rightarrow_a$ and $L_2 = d_1 \nabla_a^i D_2(d_1)$ and $L_3 = L_2 \nabla_a^j D_3(L_2)$ and $L_1 = L_3 \nabla_a^b D_1(L_3)$ and $L_4 = L_1 \nabla_a^n D_4(L_1)$ and $L_5 = L_4 \nabla_a^s D_5(L_4)$ and j_1, b_1, n_1, $s_1 \in \operatorname{dom} d_1$ and $d_1 \in \operatorname{dom} D_2$ and $s \neq n$. Then $L_5(n) = L_4(n)$.

(3) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $D_2 = i_1 \Rightarrow_a$ and $D_3 = j_1 \Rightarrow_a$ and $D_1 = b_1 \Rightarrow_a$ and $D_4 = n_1 \Rightarrow_a$ and $D_5 = s_1 \Rightarrow_a$ and $L_2 = d_1 \nabla_a^i D_2(d_1)$ and $L_3 = L_2 \nabla_a^j D_3(L_2)$ and $L_1 = L_3 \nabla_a^b D_1(L_3)$ and $L_4 = L_1 \nabla_a^n D_4(L_1)$ and $L_5 = L_4 \nabla_a^s D_5(L_4)$ and j_1, b_1, n_1, $s_1 \in \operatorname{dom} d_1$ and $d_1 \in \operatorname{dom} D_2$ and $s \neq i$. Then $L_5(i) = L_4(i)$.

In the sequel f denotes a binominative function over simple-named complex-valued nominative data of V and A, T denotes a nominative data with simple names from V and complex values from A, *loc* denotes a V-valued function, and *val* denotes a function.

Let us consider V, A, and *loc*. The functor power-loop-body(A, loc) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 2) $\text{Asg}^{(loc_{/1})}(\text{addition}(A, loc_{/1}, loc_{/2})) \bullet (\text{Asg}^{(loc_{/5})}(\text{multiplication}(A, loc_{/5}, loc_{/3})))$.

The functor power-main-loop(A, loc) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 3) $\mathrm{WH}(\neg\,\mathrm{Equality}(A, loc_{/1}, loc_{/4}), \text{power-loop-body}(A, loc))$.

Let us consider val. The functor power-var-init(A, loc, val) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 4) $\text{PP-composition}(\mathrm{Asg}^{(loc_{/1})}(val(1) \Rightarrow_a), \mathrm{Asg}^{(loc_{/2})}(val(2) \Rightarrow_a), \mathrm{Asg}^{(loc_{/3})}(val(3) \Rightarrow_a), \mathrm{Asg}^{(loc_{/4})}(val(4) \Rightarrow_a), \mathrm{Asg}^{(loc_{/5})}(val(5) \Rightarrow_a))$.

The functor power-main-part(A, loc, val) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 5) $\text{power-var-init}(A, loc, val) \bullet (\text{power-main-loop}(A, loc))$.

Let us consider z. The functor power-program(A, loc, val, z) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 6) $\text{power-main-part}(A, loc, val) \bullet (\mathrm{Asg}^{z}((loc_{/5}) \Rightarrow_a))$.

In the sequel n_0 denotes a natural number and b_0 denotes a complex number.

Let us consider V, A, val, b_0, n_0, and d. We say that b_0, n_0 and d constitute a valid input for the power w.r.t. V, A and val if and only if

(Def. 7) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and $\{val(1), val(2), val(3), val(4), val(5)\} \subseteq \mathrm{dom}\, d_1$ and $d_1(val(1)) = 0$ and $d_1(val(2)) = 1$ and $d_1(val(3)) = b_0$ and $d_1(val(4)) = n_0$ and $d_1(val(5)) = 1$.

The functor valid-power-input(V, A, val, b_0, n_0) yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 8) $\mathrm{dom}\, it = \mathrm{ND}_{\mathrm{SC}}(V, A)$ and for every object d such that $d \in \mathrm{dom}\, it$ holds if b_0, n_0 and d constitute a valid input for the power w.r.t. V, A and val, then $it(d) = \mathit{true}$ and if b_0, n_0 and d do not constitute a valid input for the power w.r.t. V, A and val, then $it(d) = \mathit{false}$.

Let us observe that valid-power-input(V, A, val, b_0, n_0) is total.

Let us consider z and d. We say that b_0, n_0 and d constitute a valid output for the power w.r.t. A and z if and only if

(Def. 9) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and $z \in \mathrm{dom}\, d_1$ and $d_1(z) = {b_0}^{n_0}$.

The functor valid-power-output(A, z, b_0, n_0) yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 10) dom it = $\{d$, where d is a nominative data with simple names from V and complex values from $A : d \in \operatorname{dom}(z \Rightarrow_a)\}$ and for every object d such that $d \in \operatorname{dom} it$ holds if b_0, n_0 and d constitute a valid output for the power w.r.t. A and z, then $it(d) = \mathit{true}$ and if b_0, n_0 and d do not constitute a valid output for the power w.r.t. A and z, then $it(d) = \mathit{false}$.

Let us consider loc and d. We say that b_0, n_0 and d constitute a valid invariant for the power w.r.t. A and loc if and only if

(Def. 11) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and $\{loc_{/1}, loc_{/2}, loc_{/3}, loc_{/4}, loc_{/5}\} \subseteq \operatorname{dom} d_1$ and $d_1(loc_{/2}) = 1$ and $d_1(loc_{/3}) = b_0$ and $d_1(loc_{/4}) = n_0$ and there exists a complex number S and there exists a natural number I such that $I = d_1(loc_{/1})$ and $S = d_1(loc_{/5})$ and $S = {b_0}^I$.

The functor PP-composition(A, loc, b_0, n_0) yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 12) dom $it = \mathrm{ND}_{\mathrm{SC}}(V, A)$ and for every object d such that $d \in \operatorname{dom} it$ holds if b_0, n_0 and d constitute a valid invariant for the power w.r.t. A and loc, then $it(d) = \mathit{true}$ and if b_0, n_0 and d do not constitute a valid invariant for the power w.r.t. A and loc, then $it(d) = \mathit{false}$.

Observe that PP-composition(A, loc, b_0, n_0) is total.

Let us consider val. We say that loc and val are compatible w.r.t. 5 locations if and only if

(Def. 13) $val(5) \neq loc_{/4}$ and $val(5) \neq loc_{/3}$ and $val(5) \neq loc_{/2}$ and $val(5) \neq loc_{/1}$ and $val(4) \neq loc_{/3}$ and $val(4) \neq loc_{/2}$ and $val(4) \neq loc_{/1}$ and $val(3) \neq loc_{/2}$ and $val(3) \neq loc_{/1}$ and $val(2) \neq loc_{/1}$.

Now we state the propositions:

(4) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$,$loc_{/2}$,$loc_{/3}$,$loc_{/4}$,$loc_{/5}$ are mutually different and loc and val are compatible w.r.t. 5 locations. Then $\langle$valid-power-input(V, A, val, b_0, n_0), power-var-init(A, loc, val), PP-composition$(A, loc, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

Proof: Set $i = loc_{/1}$. Set $j = loc_{/2}$. Set $b = loc_{/3}$. Set $n = loc_{/4}$. Set $s = loc_{/5}$. Set $i_1 = val(1)$. Set $j_1 = val(2)$. Set $b_1 = val(3)$. Set $n_1 = val(4)$. Set $s_1 = val(5)$. Set I = valid-power-input(V, A, val, b_0, n_0). Set i_2 = PP-composition(A, loc, b_0, n_0). Set $D_2 = i_1 \Rightarrow_a$. Set $D_3 = j_1 \Rightarrow_a$. Set $D_1 = b_1 \Rightarrow_a$. Set $D_4 = n_1 \Rightarrow_a$. Set $D_5 = s_1 \Rightarrow_a$. Set $T_1 = \mathrm{S_P}(i_2, D_5, s)$. Set $S_1 = \mathrm{S_P}(T_1, D_4, n)$. Set $R_1 = \mathrm{S_P}(S_1, D_1, b)$. Set $Q_1 = \mathrm{S_P}(R_1, D_3, j)$. Set $P_1 = \mathrm{S_P}(Q_1, D_2, i)$. $I \models P_1$ by [6, (39)], [8, (9)], [10, (4)]. $\square$

(5) Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$,$loc_{/2}$,$loc_{/3}$,$loc_{/4}$,$loc_{/5}$ are

mutually different. Then $\langle$PP-composition(A, loc, b_0, n_0), power-loop-body (A, loc), PP-composition$(A, loc, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

(6) $\langle\sim$ PP-composition(A, loc, b_0, n_0), power-loop-body(A, loc), PP-composition$(A, loc, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

(7) Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$,$loc_{/2}$,$loc_{/3}$,$loc_{/4}$,$loc_{/5}$ are mutually different. Then $\langle$PP-composition(A, loc, b_0, n_0), power-main-loop (A, loc), Equality$(A, loc_{/1}, loc_{/4})\wedge$PP-composition$(A, loc, b_0, n_0)\rangle$ is an SF-HT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (5) and (6).

(8) Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$,$loc_{/2}$,$loc_{/3}$,$loc_{/4}$,$loc_{/5}$ are mutually different and loc and val are compatible w.r.t. 5 locations. Then $\langle$valid-power-input(V, A, val, b_0, n_0), power-main-part(A, loc, val), Equality $(A, loc_{/1}, loc_{/4})\wedge$PP-composition$(A, loc, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (4) and (7).

(9) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and for every T, T is a value on $loc_{/1}$ and for every T, T is a value on $loc_{/4}$. Then Equality$(A, loc_{/1}, loc_{/4}) \wedge$ PP-composition$(A, loc, b_0, n_0) \models$ $\mathrm{S_P}$(valid-power-output(A, z, b_0, n_0), $(loc_{/5}) \Rightarrow_a, z)$.

PROOF: Set $i = loc_{/1}$. Set $j = loc_{/2}$. Set $b = loc_{/3}$. Set $n = loc_{/4}$. Set $s = loc_{/5}$. Set $D_5 = s \Rightarrow_a$. Consider d_1 being a non-atomic nominative data of V and A such that $d = d_1$ and $\{i, j, b, n, s\} \subseteq \operatorname{dom} d_1$ and $d_1(n) = n_0$ and $d_1(b) = b_0$ and there exists a complex number S and there exists a natural number I such that $I = d_1(i)$ and $S = d_1(s)$ and $S = {b_0}^I$. Reconsider $d_2 = d$ as a nominative data with simple names from V and complex values from A. Set $L = d_2 \nabla_a^z D_5(d_2)$. b_0, n_0 and L constitute a valid output for the power w.r.t. A and z. $\square$

(10) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and for every T, T is a value on $loc_{/1}$ and for every T, T is a value on $loc_{/4}$. Then $\langle$Equality$(A, loc_{/1}, loc_{/4}) \wedge$ PP-composition(A, loc, b_0, n_0), $\mathrm{Asg}^z((loc_{/5}) \Rightarrow_a)$, valid-power-output$(A, z, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (9).

(11) Suppose for every T, T is a value on $loc_{/1}$ and for every T, T is a value on $loc_{/4}$. Then $\langle\sim$ (Equality$(A, loc_{/1}, loc_{/4}) \wedge$ PP-composition(A, loc, b_0, n_0)), $\mathrm{Asg}^z((loc_{/5}) \Rightarrow_a)$, valid-power-output$(A, z, b_0, n_0)\rangle$
is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

(12) PARTIAL CORRECTNESS OF A POWER ALGORITHM:
Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $loc_{/1}$,$loc_{/2}$,$loc_{/3}$,$loc_{/4}$,$loc_{/5}$ are

mutually different and loc and val are compatible w.r.t. 5 locations and for every T, T is a value on $loc_{/1}$ and for every T, T is a value on $loc_{/4}$. Then $\langle$valid-power-input(V, A, val, b_0, n_0), power-program(A, loc, val, z), valid-power-output$(A, z, b_0, n_0)\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V, A)$. The theorem is a consequence of (8), (10), and (11).

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] R.W. Floyd. Assigning meanings to programs. *Mathematical aspects of computer science*, 19(19–32), 1967.

[3] 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.

[4] C.A.R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10): 576–580, 1969.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. An inference system of an extension of Floyd-Hoare logic for partial predicates. *Formalized Mathematics*, 26(**2**): 159–164, 2018. doi:10.2478/forma-2018-0013.

[10] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. Partial correctness of GCD algorithm. *Formalized Mathematics*, 26(**2**):165–173, 2018. doi:10.2478/forma-2018-0014.

[11] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. On algebras of algorithms and specifications over uninterpreted data. *Formalized Mathematics*, 26(**2**):141–147, 2018. doi:10.2478/forma-2018-0011.

[12] Artur Kornilowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the algebra of nominative data in Mizar. In Maria Ganzha, Leszek A. Maciaszek, and Marcin Paprzycki, editors, *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, FedCSIS 2017, Prague, Czech Republic, September 3–6, 2017.*, pages 237–244, 2017. ISBN 978-83-946253-7-5. doi:10.15439/2017F301.

[13] Artur Kornilowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the nominative algorithmic algebra in Mizar. In Leszek Borzemski, Jerzy Świątek, and Zofia Wilimowska, editors, *Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017 – Part II, Szklarska Poręba, Poland, September 17–19, 2017*, volume 656 of *Advances in Intelligent Systems and Computing*, pages 176–186. Springer, 2017. ISBN 978-3-319-67228-1. doi:10.1007/978-3-319-67229-8_16.

[14] 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 Kharchen-

ko, 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.

[15] 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.

[16] 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.

[17] Volodymyr G. Skobelev, Mykola Nikitchenko, and Ievgen Ivanov. On algebraic properties of nominative data and functions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications – 10th International Conference, ICTERI 2014, Kherson, Ukraine, June 9–12, 2014, Revised Selected Papers*, volume 469 of *Communications in Computer and Information Science*, pages 117–138. Springer, 2014. ISBN 978-3-319-13205-1. doi:10.1007/978-3-319-13206-8_6.

Accepted May 27, 2019