FORMALIZED MATHEMATICS
Vol. 28, No. 4, Pages 279–288, 2020
DOI: 10.2478/forma-2020-0025

sciendo
https://www.sciendo.com/

Partial Correctness of an Algorithm Computing Lucas Sequences

Adrian Jaszczak
Institute of Informatics
University of Białystok
Poland

Summary. In this paper we define some properties about finite sequences and verify the partial correctness of an algorithm computing n-th element of Lucas sequence [23], [20] with given P and Q coefficients as well as two first elements (x and y). The algorithm is encoded in nominative data language [22] in the Mizar system [3], [1].

```
i := 0
s := x
b := y
c := x
while (i <> n)
   c := s
   s := b
   ps := p*s
   qc := q*c
   b := ps - qc
   i := i + j
return s
```

This paper continues verification of algorithms [10], [14], [12], [15], [13] written in terms of simple-named complex-valued nominative data [6], [8], [19], [11], [16], [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 [18], [21], [7], [5].

MSC: 68Q60 03B70 68V20

Keywords: nominative data; program verification; Lucas sequences

MML identifier: NOMIN_9, version: 8.1.10 5.64.1388

1. Introduction about Finite Sequences

Let n be a natural number and f be an n-element finite sequence. One can verify that $f \restriction \mathrm{Seg}\, n$ reduces to f.

Let A, B be sets and f_1, f_2, f_3, f_4, f_5, f_6 be partial functions from A to B. One can check that $\langle f_1, f_2, f_3, f_4, f_5, f_6 \rangle$ is $(A \dot{\to} B)$-valued.

Let V, A be sets and f_1, f_2, f_3, f_4, f_5, f_6 be binominative functions over simple-named complex-valued nominative date of V and A.

Observe that $\langle f_1, f_2, f_3, f_4, f_5, f_6 \rangle$ is $(\mathrm{FPrg}(\mathrm{ND}_{\mathrm{SC}}(V, A)))$-valued.

Let $a_1, a_2, a_3, a_4, a_5, a_6$ be objects. One can verify that $\langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle(1)$ reduces to a_1 and $\langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle(2)$ reduces to a_2.

And $\langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle(3)$ reduces to a_3 and $\langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle(4)$ reduces to a_4 and $\langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle(5)$ reduces to a_5 and $\langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle(6)$ reduces to a_6.

Let $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ be objects. The functor $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle$ yielding a finite sequence is defined by the term

(Def. 1) $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 \rangle \frown \langle a_9 \rangle$.

Now we state the proposition:

(1) Let us consider objects a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, and a finite sequence f. Then $f = \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle$ if and only if $\mathrm{len}\, f = 9$ and $f(1) = a_1$ and $f(2) = a_2$ and $f(3) = a_3$ and $f(4) = a_4$ and $f(5) = a_5$ and $f(6) = a_6$ and $f(7) = a_7$ and $f(8) = a_8$ and $f(9) = a_9$.

Let $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ be objects. Let us observe that $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle$ is 9-element.

Let us observe that $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle(1)$ reduces to a_1 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle(2)$ reduces to a_2 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle(3)$ reduces to a_3 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle(4)$ reduces to a_4.

And $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle(5)$ reduces to a_5 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle(6)$ reduces to a_6 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle(7)$ reduces to a_7 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle(8)$ reduces to a_8 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle(9)$ reduces to a_9.

Now we state the proposition:

(2) Let us consider objects $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$. Then $\mathrm{rng}\, \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\}$.

Let X be a non empty set and a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 be elements of X. Note that the functor $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle$ yields a finite sequence of elements of X. Let a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10} be objects. The functor $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10} \rangle$ yielding a finite sequence is defined by the term

(Def. 2) $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\rangle \frown \langle a_{10}\rangle$.

Now we state the proposition:

(3) Let us consider objects a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, and a finite sequence f. Then $f = \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle$ if and only if $\operatorname{len} f = 10$ and $f(1) = a_1$ and $f(2) = a_2$ and $f(3) = a_3$ and $f(4) = a_4$ and $f(5) = a_5$ and $f(6) = a_6$ and $f(7) = a_7$ and $f(8) = a_8$ and $f(9) = a_9$ and $f(10) = a_{10}$. The theorem is a consequence of (1).

Let a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10} be objects. One can check that $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle$ is 10-element.

Let us observe that $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle(1)$ reduces to a_1 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle(2)$ reduces to a_2 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle(3)$ reduces to a_3 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle(4)$ reduces to a_4 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle(5)$ reduces to a_5.

And $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle(6)$ reduces to a_6 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle(7)$ reduces to a_7 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle(8)$ reduces to a_8 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle(9)$ reduces to a_9 and $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle(10)$ reduces to a_{10}.

Now we state the proposition:

(4) Let us consider objects a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}. Then $\operatorname{rng} \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\}$. The theorem is a consequence of (2).

Let X be a non empty set and a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10} be elements of X. One can verify that the functor $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\rangle$ yields a finite sequence of elements of X.

2. Lucas Sequences

Let i, j be integers. Let us observe that the functor $\langle i, j\rangle$ yields an element of $\mathbb{Z}\times\mathbb{Z}$. From now on x, y, P, Q denote integers, a, b, n denote natural numbers, V, A denote sets, val denotes a function, loc denotes a V-valued function, d_1 denotes a non-atomic nominative data of V and A, p denotes a partial predicate over simple-named complex-valued nominative data of V and A, d denotes an object, z denotes an element of V.

T denotes a nominative data with simple names from V and complex values from A, s_0 denotes a non zero natural number, x_0, y_0, p_0, q_0 denote integers, and n_0 denotes a natural number.

Let us consider x, y, P, and Q. The functor $\operatorname{LucasSeq}(x, y, P, Q)$ yielding a sequence of $\mathbb{Z} \times \mathbb{Z}$ is defined by

(Def. 3) $it(0) = \langle x, y \rangle$ and for every natural number n, $it(n+1) = \langle (it(n))_{\mathbf{2}}, P \cdot ((it(n))_{\mathbf{2}}) - Q \cdot ((it(n))_{\mathbf{1}}) \rangle$.

Let us consider n. The functor $\mathrm{Lucas}(x, y, P, Q, n)$ yielding an element of $\mathbb{Z}$ is defined by the term

(Def. 4) $((\mathrm{LucasSeq}(x, y, P, Q))(n))_{\mathbf{1}}$.

Now we state the propositions:

(5) (i) $\mathrm{Lucas}(x, y, P, Q, 0) = x$, and

(ii) $\mathrm{Lucas}(x, y, P, Q, 1) = y$, and

(iii) for every n, $\mathrm{Lucas}(x, y, P, Q, n+2) = P \cdot (\mathrm{Lucas}(x, y, P, Q, n+1)) - Q \cdot (\mathrm{Lucas}(x, y, P, Q, n))$.

(6) $\mathrm{LucasSeq}(0, 1, 1, -1) = \mathrm{Fib}$.

Proof: Set $L = \mathrm{LucasSeq}(0, 1, 1, -1)$. Set $F = \mathrm{Fib}$. Define $\mathcal{P}[\text{natural number}] \equiv L(\$_1) = F(\$_1)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(7) $\mathrm{Lucas}(0, 1, 1, -1, n) = \mathrm{Fib}(n)$.

(8) $\mathrm{LucasSeq}(a, b, 1, -1) = \mathrm{GenFib}(a, b)$.

Proof: Set $L = \mathrm{LucasSeq}(a, b, 1, -1)$. Set $F = \mathrm{GenFib}(a, b)$. Define $\mathcal{P}[\text{natural number}] \equiv L(\$_1) = F(\$_1)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(9) $\mathrm{Lucas}(a, b, 1, -1, n) = \mathrm{GFib}(a, b, n)$.

(10) $\mathrm{LucasSeq}(2, 1, 1, -1) = \mathrm{Lucas}$.

Proof: Set $L = \mathrm{LucasSeq}(2, 1, 1, -1)$. Set $F = \mathrm{Lucas}$. Define $\mathcal{P}[\text{natural number}] \equiv L(\$_1) = F(\$_1)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(11) $\mathrm{Lucas}(2, 1, 1, -1, n) = \mathrm{Luc}(n)$.

3. Main Algorithm

Now we state the proposition:

(12) Suppose $\mathrm{Seg}\,10 \subseteq \mathrm{dom}\, loc$ and loc is valid w.r.t. d_1. Then $\{loc_{/1}, loc_{/2}, loc_{/3}, loc_{/4}, loc_{/5}, loc_{/6}, loc_{/7}, loc_{/8}, loc_{/9}, loc_{/10}\} \subseteq \mathrm{dom}\, d_1$.

Let us consider V, A, and loc. The functor $\mathrm{LucasLoopBody}(A, loc)$ yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 5) $\text{PP-composition}(\mathrm{Asg}^{(loc_{/6})}((loc_{/4}) \Rightarrow_a), \mathrm{Asg}^{(loc_{/4})}((loc_{/5}) \Rightarrow_a), \mathrm{Asg}^{(loc_{/9})}(\mathrm{multiplication}(A, loc_{/7}, loc_{/4})), \mathrm{Asg}^{(loc_{/10})}(\mathrm{multiplication}(A, loc_{/8}, loc_{/6})), \mathrm{Asg}^{(loc_{/5})}(\mathrm{subtraction}(A, (loc_{/9}), (loc_{/10}))), \mathrm{Asg}^{(loc_{/1})}(\mathrm{addition}(A, loc_{/1}, loc_{/2})))$.

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

(Def. 6) $\mathrm{WH}(\neg\,\mathrm{Equality}(A, loc_{/1}, loc_{/3}), \mathrm{LucasLoopBody}(A, loc))$.

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

(Def. 7) $\text{initial-assignments}(A, loc, val, 10) \bullet (\mathrm{LucasMainLoop}(A, loc))$.

Let us consider z. The functor LucasProg(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. 8) $\mathrm{LucasMainPart}(A, loc, val) \bullet (\mathrm{Asg}^{z}((loc_{/4}) \Rightarrow_{a}))$.

Let us consider x_0, y_0, p_0, q_0, and n_0. The functor LucasInp$(x_0, y_0, p_0, q_0, n_0)$ yielding a finite sequence is defined by the term

(Def. 9) $\langle 0, 1, n_0, x_0, y_0, x_0, p_0, q_0, 0, 0\rangle$.

Observe that LucasInp$(x_0, y_0, p_0, q_0, n_0)$ is 10-element.

Let us consider V, A, and d. Let val be a finite sequence. We say that x_0, y_0, p_0, q_0, n_0 and d constitute a valid Lucas input w.r.t. V, A and val if and only if

(Def. 10) LucasInp$(x_0, y_0, p_0, q_0, n_0)$ is a valid input of V, A, val and d.

The functor validLucasInp$(V, A, val, x_0, y_0, p_0, q_0, n_0)$ yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 11) $\mathrm{ValInp}(V, A, val, \mathrm{LucasInp}(x_0, y_0, p_0, q_0, n_0))$.

One can check that validLucasInp$(V, A, val, x_0, y_0, p_0, q_0, n_0)$ is total.

Let us consider z and d. We say that x_0, y_0, p_0, q_0, n_0 and d constitute a valid Lucas output w.r.t. A and z if and only if

(Def. 12) $\langle \mathrm{Lucas}(x_0, y_0, p_0, q_0, n_0)\rangle$ is a valid output of V, A, $\langle z\rangle$ and d.

The functor validLucasOut$(A, z, x_0, y_0, p_0, q_0, n_0)$ yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 13) $\mathrm{ValOut}(V, A, z, \mathrm{Lucas}(x_0, y_0, p_0, q_0, n_0))$.

Let us consider loc and d. We say that x_0, y_0, p_0, q_0, n_0 and d constitute a Lucas inverse w.r.t. A and loc if and only if

(Def. 14) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and $\{loc_{/1}, loc_{/2}, loc_{/3}, loc_{/4}, loc_{/5}, loc_{/6}, loc_{/7}, loc_{/8}, loc_{/9}, loc_{/10}\} \subseteq \operatorname{dom} d_1$ and $d_1(loc_{/2}) = 1$ and $d_1(loc_{/3}) = n_0$ and $d_1(loc_{/7}) = p_0$ and

$d_1(loc_{/8}) = q_0$ and there exists a natural number I such that $I = d_1(loc_{/1})$ and $d_1(loc_{/4}) = \mathrm{Lucas}(x_0, y_0, p_0, q_0, I)$ and $d_1(loc_{/5}) = \mathrm{Lucas}(x_0, y_0, p_0, q_0, I+1)$.

The functor $\mathrm{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0)$ yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 15) $\mathrm{dom}\, it = \mathrm{ND_{SC}}(V, A)$ and for every object d such that $d \in \mathrm{dom}\, it$ holds if x_0, y_0, p_0, q_0, n_0 and d constitute a Lucas inverse w.r.t. A and loc, then $it(d) = \mathit{true}$ and if x_0, y_0, p_0, q_0, n_0 and d do not constitute a Lucas inverse w.r.t. A and loc, then $it(d) = \mathit{false}$.

Let us observe that $\mathrm{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0)$ is total. Let us consider a 10-element finite sequence val. Now we state the propositions:

(13) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $\mathrm{Seg}\, 10 \subseteq \mathrm{dom}\, loc$ and $loc \restriction \mathrm{Seg}\, 10$ is one-to-one and loc and val are different w.r.t. 10.

Then $\mathrm{validLucasInp}(V, A, val, x_0, y_0, p_0, q_0, n_0) \models (\mathrm{ScPsuperposSeq}(loc, val, \mathrm{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0)))(\mathrm{len}\, \mathrm{ScPsuperposSeq}(loc, val, \mathrm{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0))))$.

Proof: Set $s_0 = 10$. Set $n = loc_{/3}$. Set $i_0 = \mathrm{LucasInp}(x_0, y_0, p_0, q_0, n_0)$. Consider d_1 being a non-atomic nominative data of V and A such that $d = d_1$ and val is valid w.r.t. d_1 and for every natural number n such that $1 \leqslant n \leqslant \mathrm{len}\, i_0$ holds $d_1(val(n)) = i_0(n)$.

Set $F = \mathrm{LocalOverlapSeq}(A, loc, val, d_1, s_0)$. Reconsider $L_6 = F(10)$ as a non-atomic nominative data of V and A. x_0, y_0, p_0, q_0, n_0 and L_6 constitute a Lucas inverse w.r.t. A and loc. $\square$

(14) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $\mathrm{Seg}\, 10 \subseteq \mathrm{dom}\, loc$ and $loc \restriction \mathrm{Seg}\, 10$ is one-to-one and loc and val are different w.r.t. 10. Then $\langle \mathrm{validLucasInp}(V, A, val, x_0, y_0, p_0, q_0, n_0), \mathrm{initial\text{-}assignments}(A, loc, val, 10), \mathrm{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0) \rangle$ is an SFHT of $\mathrm{ND_{SC}}(V, A)$. The theorem is a consequence of (13).

(15) Suppose V is not empty and A is complex containing and V is without nonatomic nominative data w.r.t. A and $d_1 \in \mathrm{dom}(\mathrm{LucasLoopBody}(A, loc))$ and loc is valid w.r.t. d_1 and $\mathrm{Seg}\, 10 \subseteq \mathrm{dom}\, loc$ and for every T, T is a value on $loc_{/1}$ and T is a value on $loc_{/2}$ and T is a value on $loc_{/4}$ and T is a value on $loc_{/6}$ and T is a value on $loc_{/7}$ and T is a value on $loc_{/8}$ and T is a value on $loc_{/9}$ and T is a value on $loc_{/10}$.

Then $\langle\!\langle (loc_{/4}) \Rightarrow_a, (loc_{/5}) \Rightarrow_a, \mathrm{multiplication}(A, loc_{/7}, loc_{/4}), \mathrm{multiplication}(A, loc_{/8}, loc_{/6}), \mathrm{subtraction}(A, (loc_{/9}), (loc_{/10})), \mathrm{addition}(A, loc_{/1}, loc_{/2}) \rangle\!\rangle$ is domain closed w.r.t. loc, d_1 and $\langle\!\langle 6, 4, 9, 10, 5, 1 \rangle\!\rangle$. The theorem is a consequence of (12).

Let us consider a non empty set V and a V-valued, 10-element finite sequence loc. Now we state the propositions:

(16) Suppose A is complex containing and V is without nonatomic nominative data w.r.t. A and for every nominative data T with simple names from V and complex values from A, T is a value on $loc_{/1}$ and T is a value on $loc_{/2}$ and T is a value on $loc_{/4}$ and T is a value on $loc_{/6}$ and T is a value on $loc_{/7}$ and T is a value on $loc_{/8}$ and T is a value on $loc_{/9}$ and T is a value on $loc_{/10}$ and loc is one-to-one. Then $\langle \mathrm{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0), \mathrm{LucasLoopBody}(A, loc), \mathrm{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0)\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V, A)$. The theorem is a consequence of (15) and (5).

(17) Suppose A is complex containing and V is without nonatomic nominative data w.r.t. A and for every nominative data T with simple names from V and complex values from A, T is a value on $loc_{/1}$ and T is a value on $loc_{/2}$ and T is a value on $loc_{/4}$ and T is a value on $loc_{/6}$ and T is a value on $loc_{/7}$ and T is a value on $loc_{/8}$ and T is a value on $loc_{/9}$ and T is a value on $loc_{/10}$ and loc is one-to-one.

Then $\langle \mathrm{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0), \mathrm{LucasMainLoop}(A, loc), \mathrm{Equality}(A, loc_{/1}, loc_{/3}) \wedge \mathrm{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0)\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V, A)$. The theorem is a consequence of (16).

(18) Let us consider a non empty set V, a V-valued, 10-element finite sequence loc, and a 10-element finite sequence val. Suppose A is complex containing and V is without nonatomic nominative data w.r.t. A and for every nominative data T with simple names from V and complex values from A, T is a value on $loc_{/1}$ and T is a value on $loc_{/2}$ and T is a value on $loc_{/4}$ and T is a value on $loc_{/6}$ and T is a value on $loc_{/7}$ and T is a value on $loc_{/8}$ and T is a value on $loc_{/9}$ and T is a value on $loc_{/10}$ and loc is one-to-one and loc and val are different w.r.t. 10.

Then $\langle \mathrm{validLucasInp}(V, A, val, x_0, y_0, p_0, q_0, n_0), \mathrm{LucasMainPart}(A, loc, val), \mathrm{Equality}(A, loc_{/1}, loc_{/3}) \wedge \mathrm{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0)\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V, A)$. The theorem is a consequence of (14) and (17).

(19) 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 T is a value on $loc_{/3}$. Then $\mathrm{Equality}(A, loc_{/1}, loc_{/3}) \wedge \mathrm{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0) \models \mathrm{S_P}(\mathrm{validLucasOut}(A, z, x_0, y_0, p_0, q_0, n_0), (loc_{/4}) \Rightarrow_a, z)$.

PROOF: Set $i = loc_{/1}$. Set $j = loc_{/2}$. Set $n = loc_{/3}$. Set $s = loc_{/4}$. Set $b = loc_{/5}$. Set $c = loc_{/6}$. Set $p = loc_{/7}$. Set $q = loc_{/8}$. Set $p_1 = loc_{/9}$. Set $q_1 = loc_{/10}$. Set $D_{12} = s \Rightarrow_a$. Set $E_1 = \{i, j, n, s, b, c, p, q, p_1, q_1\}$.

Consider d_1 being a non-atomic nominative data of V and A such that $d = d_1$ and $E_1 \subseteq \mathrm{dom}\, d_1$ and $d_1(j) = 1$ and $d_1(n) = n_0$ and $d_1(p) = p_0$

and $d_1(q) = q_0$ and there exists a natural number I such that $I = d_1(i)$ and $d_1(s) = \text{Lucas}(x_0, y_0, p_0, q_0, I)$ and $d_1(b) = \text{Lucas}(x_0, y_0, p_0, q_0, I+1)$.

Reconsider $d_2 = d$ as a nominative data with simple names from V and complex values from A. Set $L = d_2 \nabla_a^z D_{12}(d_2)$. x_0, y_0, p_0, q_0, n_0 and L constitute a valid Lucas output w.r.t. A and z. $\square$

(20) 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 T is a value on $loc_{/3}$. Then $\langle \text{Equality}(A, loc_{/1}, loc_{/3}) \wedge \text{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0)$, $\text{Asg}^z((loc_{/4}) \Rightarrow_a), \text{validLucasOut}(A, z, x_0, y_0, p_0, q_0, n_0)\rangle$ is an SFHT of $\text{ND}_{\text{SC}}(V, A)$. The theorem is a consequence of (19).

(21) Suppose for every T, T is a value on $loc_{/1}$ and T is a value on $loc_{/3}$. Then $\langle \sim (\text{Equality}(A, loc_{/1}, loc_{/3}) \wedge \text{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0))$, $\text{Asg}^z((loc_{/4}) \Rightarrow_a), \text{validLucasOut}(A, z, x_0, y_0, p_0, q_0, n_0)\rangle$ is an SFHT of $\text{ND}_{\text{SC}}(V, A)$.

(22) Partial correctness of a Lucas algorithm:
Let us consider a non empty set V, a V-valued, 10-element finite sequence loc, a 10-element finite sequence val, and an element z of V. Suppose A is complex containing and V is without nonatomic nominative data w.r.t. A and for every nominative data T with simple names from V and complex values from A, T is a value on $loc_{/1}$ and T is a value on $loc_{/2}$ and T is a value on $loc_{/3}$ and T is a value on $loc_{/4}$ and T is a value on $loc_{/6}$ and T is a value on $loc_{/7}$ and T is a value on $loc_{/8}$ and T is a value on $loc_{/9}$ and T is a value on $loc_{/10}$ and loc is one-to-one and loc and val are different w.r.t. 10.

Then $\langle \text{validLucasInp}(V, A, val, x_0, y_0, p_0, q_0, n_0), \text{LucasProg}(A, loc, val, z), \text{validLucasOut}(A, z, x_0, y_0, p_0, q_0, n_0)\rangle$ is an SFHT of $\text{ND}_{\text{SC}}(V, A)$. The theorem is a consequence of (18), (20), and (21).

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] Adrian Jaszczak. Partial correctness of a power algorithm. *Formalized Mathematics*, 27(**2**):189–195, 2019. doi:10.2478/forma-2019-0018.

[13] Adrian Jaszczak. General theory and tools for proving algorithms in nominative data systems. *Formalized Mathematics*, 28(**4**):269–278, 2020. doi:10.2478/forma-2020-0024.

[14] Adrian Jaszczak and Artur Korniłowicz. Partial correctness of a factorial algorithm. *Formalized Mathematics*, 27(**2**):181–187, 2019. doi:10.2478/forma-2019-0017.

[15] Artur Korniłowicz. Partial correctness of a Fibonacci algorithm. *Formalized Mathematics*, 28(**2**):187–196, 2020. doi:10.2478/forma-2020-0016.

[16] Artur Korniłowicz, 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.

[17] Artur Korniłowicz, 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.

[18] 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.

[19] 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.

[20] Thomas Koshy. *Fibonacci and Lucas Numbers with Applications, Volume 1*. John Wiley & Sons, Inc., 2017. ISBN 978-1118742129. doi:10.1002/9781118742327.

[21] 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.

[22] 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.

[23] Steven Vajda. *Fibonacci & Lucas Numbers, and the Golden Section: Theory and Applications.* Dover Publications, 2007. ISBN 978-0486462769.

Accepted October 25, 2020