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 \([3], [1]\).

\[
i := 0
s := x
b := y
c := x
\]
\[\text{while (} i <> n \text{)} \]
\[c := s
s := b
c := x
b := ps - qc
i := i + j
\]
\[\text{return } s\]

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 \([18], [21], [7], [9]\).

MSC: 68Q60 03B70 68V20

Keywords: nominative data; program verification; Lucas sequences

MML identifier: NOMIN9 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 $f \upharpoonright \text{Seg} n$ 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 $(A \rightarrow B)$-valued.

Let $V$, $A$ be sets and $f_1$, $f_2$, $f_3$, $f_4$, $f_5$, $f_6$ be binominal 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 $(\text{FPrg(ND}_{\text{SC}}(V, A)))$-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) $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 \rangle \sim \langle a_9 \rangle$.

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 $\text{len } f = 9$ 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 $\text{rng } \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 \rangle = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\}$.

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

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 \( \text{len} \ f = 10 \) 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 \( \text{rng} \\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10} \rangle = \{ a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10} \} \). 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, \( \text{val} \) denotes a function, \( \text{loc} \) 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 LucasSeq\( (x, y, P, Q) \) yielding a sequence of \( \mathbb{Z} \times \mathbb{Z} \) is defined by
\( (\text{Def. 3}) \quad \text{it}(0) = \langle x, y \rangle \) and for every natural number \( n \), \( \text{it}(n+1) = \langle (\text{it}(n))_2, P \cdot ((\text{it}(n))_2) - Q \cdot ((\text{it}(n))_1) \rangle \).

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

\( (\text{Def. 4}) \quad ((\text{LucasSeq}(x, y, P, Q))(n))_1. \)

Now we state the propositions:

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

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

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

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

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

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

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

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

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

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

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

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

3. Main Algorithm

Now we state the proposition:

(12) \( \) Suppose \( \text{Seg}10 \subseteq \text{dom loc} \) and \( \text{loc} \) is valid w.r.t. \( d_1 \). Then \{\( \text{loc}/_1, \text{loc}/_2, \text{loc}/_3, \text{loc}/_4, \text{loc}/_5, \text{loc}/_6, \text{loc}/_7, \text{loc}/_8, \text{loc}/_9, \text{loc}/_{10} \} \subseteq \text{dom } d_1 \).

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

\( (\text{Def. 5}) \quad \text{PP-composition}(\text{Asg}^{(\text{loc}/_6)}((\text{loc}/_4) \Rightarrow a), \text{Asg}^{(\text{loc}/_4)}((\text{loc}/_5) \Rightarrow a), \text{Asg}^{(\text{loc}/_9)} \text{(multiplication}(A, \text{loc}/_7, \text{loc}/_4)), \text{Asg}^{(\text{loc}/_{10})} \text{(multiplication}(A, \text{loc}/_8, \text{loc}/_6)), \text{Asg}^{(\text{loc}/_5)} \text{(subtraction}(A, (\text{loc}/_7), (\text{loc}/_{10}))), \text{Asg}^{(\text{loc}/_1)} \text{(addition}(A, \text{loc}/_1, \text{loc}/_2))). \)
The functor $\text{LucasMainLoop}(A, \text{loc})$ yielding a binominative function over simple-named complex-valued nominative data of $V$ and $A$ is defined by the term

$(\text{Def. 6})$ \quad $\text{WH}(\neg \text{Equality}(A, \text{loc}/_1, \text{loc}/_3), \text{LucasLoopBody}(A, \text{loc}))$.

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

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

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

$(\text{Def. 8})$ \quad $\text{LucasMainPart}(A, \text{loc}, \text{val}) \circ (\text{Asg}^\ast((\text{loc}/_4) \Rightarrow a))$.

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

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

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

Let us consider $V$, $A$, and $d$. Let $\text{val}$ 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 $\text{val}$ if and only if

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

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

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

One can check that $\text{validLucasInp}(V, A, \text{val}, x_0, y_0, p_0, q_0, n_0)$ 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 $\text{z}$ if and only if

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

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

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

Let us consider $\text{loc}$ 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 $\text{loc}$ if and only if

$(\text{Def. 14})$ \quad there exists a non-atomic nominative data $d_1$ of $V$ and $A$ such that $d = d_1$ and \{\text{loc}/_1, \text{loc}/_2, \text{loc}/_3, \text{loc}/_4, \text{loc}/_5, \text{loc}/_6, \text{loc}/_7, \text{loc}/_8, \text{loc}/_9, \text{loc}/_{10} \} \subseteq \text{dom} d_1$ and $d_1(\text{loc}/_2) = 1$ and $d_1(\text{loc}/_3) = n_0$ and $d_1(\text{loc}/_7) = p_0$ and
\[ d_1(\text{loc}/8) = q_0 \text{ and there exists a natural number } I \text{ such that } I = d_1(\text{loc}/1) \text{ and } d_1(\text{loc}/A) = \text{Lucas}(x_0, y_0, p_0, q_0, I) \text{ and } d_1(\text{loc}/5) = \text{Lucas}(x_0, y_0, p_0, q_0, I + 1). \]

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

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

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

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

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

\text{Proof:} Set \( s_0 = 10 \). Set \( n = \text{loc}/3 \). Set \( i_0 = \text{LucasInv}(x_0, y_0, p_0, q_0, n_0) \).
Consider \( d_1 \) being a nonatomic nominative data of \( V \) and \( A \) such that \( d = d_1 \) and \( \text{val} \) is valid w.r.t. \( d_1 \) and for every natural number \( n \) such that \( 1 \leq n \leq \text{len } i_0 \) holds \( d_1(\text{val}(n)) = i_0(n) \).

Set \( F = \text{LocalOverlapSeq}(A, \text{loc}, \text{val}, d_1, s_0) \). Reconsider \( L_6 = F(10) \) as a nonatomic 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 \( \text{loc} \). \( \square \)

(14) Suppose \( V \) is not empty and \( V \) is without nonatomic nominative data w.r.t. \( A \) and \( \text{Seg}10 \subseteq \text{dom } \text{loc} \) and \( \text{Seg}10 \) is one-to-one and \( \text{loc} \) and \( \text{val} \) are different w.r.t. \( 10 \). Then \( \text{validLucasInv}(V, A, \text{val}, x_0, y_0, p_0, q_0, n_0) \), initial-assignments\((A, \text{loc}, \text{val}, 10), \text{LucasInv}(A, \text{loc}, x_0, y_0, p_0, q_0, n_0)) \) is an SFHT of \( \text{NDSC}(V, A) \). 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 \( d_1 \in \text{dom}(\text{LucasLoopBody}(A, \text{loc})) \) and \( \text{loc} \) is valid w.r.t. \( d_1 \) and \( \text{Seg}10 \subseteq \text{dom } \text{loc} \) and for every \( T, T \) is a value on \( \text{loc}/1 \) and \( T \) is a value on \( \text{loc}/2 \) and \( T \) is a value on \( \text{loc}/4 \) and \( T \) is a value on \( \text{loc}/6 \) and \( T \) is a value on \( \text{loc}/7 \) and \( T \) is a value on \( \text{loc}/8 \) and \( T \) is a value on \( \text{loc}/9 \) and \( T \) is a value on \( \text{loc}/10 \).

Then \( \langle (\text{loc}/4) \Rightarrow_a, (\text{loc}/5) \Rightarrow_a, \text{multiplication}(A, \text{loc}/7, \text{loc}/4), \text{multiplication}(A, \text{loc}/8, \text{loc}/6), \text{subtraction}(A, (\text{loc}/9), (\text{loc}/10)), \text{addition}(A, \text{loc}/1, \text{loc}/2) \rangle \) is domain closed w.r.t. \( \text{loc}, d_1 \) and \( \{6, 4, 9, 10, 5, 1\} \). The theorem is a consequence of (12).
Let us consider a non empty set \( V \) and a \( V \)-valued, 10-element finite sequence \( \text{loc} \). 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 \( \text{loc}/1 \) and \( T \) is a value on \( \text{loc}/2 \) and \( T \) is a value on \( \text{loc}/4 \) and \( T \) is a value on \( \text{loc}/6 \) and \( T \) is a value on \( \text{loc}/7 \) and \( T \) is a value on \( \text{loc}/8 \) and \( T \) is a value on \( \text{loc}/9 \) and \( T \) is a value on \( \text{loc}/10 \) and \( \text{loc} \) is one-to-one. Then \( \langle \text{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0), \text{LucasLoopBody}(A, loc) \rangle \) is an SFHT of \( \text{ND}_{SC}(V, A) \). 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 \( \text{loc}/1 \) and \( T \) is a value on \( \text{loc}/2 \) and \( T \) is a value on \( \text{loc}/4 \) and \( T \) is a value on \( \text{loc}/6 \) and \( T \) is a value on \( \text{loc}/7 \) and \( T \) is a value on \( \text{loc}/8 \) and \( T \) is a value on \( \text{loc}/9 \) and \( T \) is a value on \( \text{loc}/10 \) and \( \text{loc} \) is one-to-one.

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

(18) Let us consider a non empty set \( V \), a \( V \)-valued, 10-element finite sequence \( \text{loc} \), and a 10-element finite sequence \( \text{val} \). 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 \( \text{loc}/1 \) and \( T \) is a value on \( \text{loc}/2 \) and \( T \) is a value on \( \text{loc}/4 \) and \( T \) is a value on \( \text{loc}/6 \) and \( T \) is a value on \( \text{loc}/7 \) and \( T \) is a value on \( \text{loc}/8 \) and \( T \) is a value on \( \text{loc}/9 \) and \( T \) is a value on \( \text{loc}/10 \) and \( \text{loc} \) is one-to-one and \( \text{loc} \) and \( \text{val} \) are different w.r.t. 10.

Then \( \langle \text{validLucasInv}(V, A, \text{val}, x_0, y_0, p_0, q_0, n_0), \text{LucasMainPart}(A, loc, \text{val}), \text{Equality}(A, \text{loc}/1, \text{loc}/3) \rangle \langle \text{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0) \rangle \) is an SFHT of \( \text{ND}_{SC}(V, A) \). 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 \( \text{loc}/1 \) and \( T \) is a value on \( \text{loc}/3 \). Then \( \text{Equality}(A, \text{loc}/1, \text{loc}/3) \wedge \text{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0) \models \text{Sp}(\text{validLucasOut}(A, z, x_0, y_0, p_0, q_0, n_0), \langle \text{loc}/4 \rangle \Rightarrow a, z) \).

**Proof:** Set \( i = \text{loc}/1 \). Set \( j = \text{loc}/2 \). Set \( n = \text{loc}/3 \). Set \( s = \text{loc}/4 \). Set \( b = \text{loc}/5 \). Set \( c = \text{loc}/6 \). Set \( p = \text{loc}/7 \). Set \( q = \text{loc}/8 \). Set \( p_1 = \text{loc}/9 \). Set \( q_1 = \text{loc}/10 \). 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 \( E_1 \subseteq \text{dom} \ d_1 \) 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 \( L = d_2 \nabla_2 D_{12}(d_2) \). \( x_0, y_0, p_0, q_0, n_0 \) and \( L \) constitute a valid Lucas output w.r.t. \( A \) and \( z \). □

(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 \( \langle \text{Equality}(A, loc/1, loc/3) \land \text{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0), \text{Asg}^z((loc/4) \Rightarrow_a), \text{validLucasOut}(A, z, x_0, y_0, p_0, q_0, n_0) \rangle \) is an SFHT of \( \text{ND}_{SC}(V, A) \). 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 \( \langle \sim (\text{Equality}(A, loc/1, loc/3) \land \text{LucasInv}(A, loc, x_0, y_0, p_0, q_0, n_0)), \text{Asg}^z((loc/4) \Rightarrow_a), \text{validLucasOut}(A, z, x_0, y_0, p_0, q_0, n_0) \rangle \) is an SFHT of \( \text{ND}_{SC}(V, A) \).

(22) **PARTIAL CORRECTNESS OF A LUCAS ALGORITHM:**

Let us consider a non empty set \( V \), a \( V \)-valued, 10-element finite sequence \( \text{loc} \), a 10-element finite sequence \( \text{val} \), 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 \( \text{val} \) are different w.r.t. 10.

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

**References**


*Accepted October 25, 2020*