FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 177–194, 2008
DOI: 10.2478/v10037-008-0024-0

Mizar Analysis of Algorithms: Algorithms over Integers[1]

Grzegorz Bancerek
Białystok Technical University
Poland

Summary. This paper is a continuation of [5] and concerns if-while algebras over integers. In these algebras the only elementary instructions are assignment instructions. The instruction assigns to a (program) variable a value which is calculated for the current state according to some arithmetic expression. The expression may include variables, constants, and a limited number of arithmetic operations. States are functions from a given set of locations into integers. A variable is a function from the states into the locations and an expression is a function from the states into integers. Additional conditions (computability) limit the set of variables and expressions and, simultaneously, allow to write algorithms in a natural way (and to prove their correctness).

As examples the proofs of full correctness of two Euclid algorithms (with modulo operation and subtraction) and algorithm of exponentiation by squaring are given.

MML identifier: AOFA_I00, version: 7.8.10 4.100.1011

The terminology and notation used in this paper are introduced in the following papers: [16], [30], [2], [31], [12], [32], [15], [13], [17], [11], [1], [3], [28], [7], [24], [29], [21], [20], [25], [9], [27], [14], [8], [18], [26], [22], [19], [10], [23], [4], [6], and [5].

1. Preliminaries

One can prove the following proposition

[1]This work has been partially supported by the Białystok Technical University grant W/WI/1/06.

ISSN 1426–2630(p), 1898-9934(e)

(1) Let x, y, z, a, b, c be sets. Suppose $a \neq b \neq c \neq a$. Then there exists a function f such that $f(a) = x$ and $f(b) = y$ and $f(c) = z$.

Let F be a non empty functional set, let x be a set, and let f be a set. The functor $F\restriction^{x}_{\neq f}$ yields a subset of F and is defined by:

(Def. 1) $F\restriction^{x}_{\neq f} = \{g \in F\colon g(x) \neq f\}$.

One can prove the following proposition

(2) Let F be a non empty functional set, x, y be sets, and g be an element of F. Then $g \in F\restriction^{x}_{\neq y}$ if and only if $g(x) \neq y$.

Let X be a set, let Y, Z be sets, and let f be a function from $\mathbb{Z}^X \times Y$ into Z.

(Def. 2) An element of X is called a variable in f.

Let f be a real-yielding function and let x be a real number. We introduce $f \cdot x$ as a synonym of $x\,f$.

Let t_1, t_2 be integer-yielding functions. The functors: $t_1 \div t_2$, t_1 mod t_2, $\mathrm{leq}(t_1, t_2)$, $\mathrm{gt}(t_1, t_2)$, and $\mathrm{eq}(t_1, t_2)$ yield integer-yielding functions and are defined as follows:

(Def. 3) $\mathrm{dom}(t_1 \div t_2) = \mathrm{dom}\, t_1 \cap \mathrm{dom}\, t_2$ and for every set s such that $s \in \mathrm{dom}(t_1 \div t_2)$ holds $(t_1 \div t_2)(s) = t_1(s) \div t_2(s)$.

(Def. 4) $\mathrm{dom}(t_1 \bmod t_2) = \mathrm{dom}\, t_1 \cap \mathrm{dom}\, t_2$ and for every set s such that $s \in \mathrm{dom}(t_1 \bmod t_2)$ holds $(t_1 \bmod t_2)(s) = t_1(s) \bmod t_2(s)$.

(Def. 5) $\mathrm{dom}\,\mathrm{leq}(t_1, t_2) = \mathrm{dom}\, t_1 \cap \mathrm{dom}\, t_2$ and for every set s such that $s \in \mathrm{dom}\,\mathrm{leq}(t_1, t_2)$ holds $(\mathrm{leq}(t_1, t_2))(s) = (t_1(s) > t_2(s) \to 0, 1)$.

(Def. 6) $\mathrm{dom}\,\mathrm{gt}(t_1, t_2) = \mathrm{dom}\, t_1 \cap \mathrm{dom}\, t_2$ and for every set s such that $s \in \mathrm{dom}\,\mathrm{gt}(t_1, t_2)$ holds $(\mathrm{gt}(t_1, t_2))(s) = (t_1(s) > t_2(s) \to 1, 0)$.

(Def. 7) $\mathrm{dom}\,\mathrm{eq}(t_1, t_2) = \mathrm{dom}\, t_1 \cap \mathrm{dom}\, t_2$ and for every set s such that $s \in \mathrm{dom}\,\mathrm{eq}(t_1, t_2)$ holds $(\mathrm{eq}(t_1, t_2))(s) = (t_1(s) = t_2(s) \to 1, 0)$.

Let X be a non empty set, let f be a function from X into $\mathbb{Z}$, and let x be an integer number. Then $f + x$, $f - x$, and $f \cdot x$ are functions from X into $\mathbb{Z}$ and they can be characterized by the conditions:

(Def. 8) For every element s of X holds $(f + x)(s) = f(s) + x$.

(Def. 9) For every element s of X holds $(f - x)(s) = f(s) - x$.

(Def. 10) For every element s of X holds $(f \cdot x)(s) = f(s) \cdot x$.

Let X be a set and let f, g be functions from X into $\mathbb{Z}$. Then $f \div g$, $f \bmod g$, $\mathrm{leq}(f, g)$, $\mathrm{gt}(f, g)$, and $\mathrm{eq}(f, g)$ are functions from X into $\mathbb{Z}$.

Let X be a non empty set and let t_1, t_2 be functions from X into $\mathbb{Z}$. Then $t_1 - t_2$ and $t_1 + t_2$ are functions from X into $\mathbb{Z}$ and they can be characterized by the conditions:

(Def. 11) For every element s of X holds $(t_1 - t_2)(s) = t_1(s) - t_2(s)$.

(Def. 12) For every element s of X holds $(t_1 + t_2)(s) = t_1(s) + t_2(s)$.

Let A be a non empty set and let B be an infinite set. Note that B^A is infinite.

Let N be a set, let v be a function, and let f be a function. The functor $v \circ_N f$ yields a function and is defined by the conditions (Def. 13).

(Def. 13)(i) There exists a set Y such that for every set y holds $y \in Y$ iff there exists a function h such that $h \in \operatorname{dom} v$ and $y \in \operatorname{rng} h$ and for every set a holds $a \in \operatorname{dom}(v \circ_N f)$ iff $a \in Y^N$ and there exists a function g such that $a = g$ and $g \cdot f \in \operatorname{dom} v$, and

(ii) for every function g such that $g \in \operatorname{dom}(v \circ_N f)$ holds $(v \circ_N f)(g) = v(g \cdot f)$.

Let X, Y, Z, N be non empty sets, let v be an element of Z^{Y^X}, and let f be a function from X into N. Then $v \circ_N f$ is an element of Z^{Y^N}.

The following three propositions are true:

(3) For all functions f_1, f_2, g such that $\operatorname{rng} g \subseteq \operatorname{dom} f_2$ holds $(f_1 +\cdot f_2) \cdot g = f_2 \cdot g$.

(4) Let X, N, I be non empty sets, s be a function from X into I, and c be a function from X into N. Suppose c is one-to-one. Let n be an element of I. Then $(N \longmapsto n) +\cdot s \cdot c^{-1}$ is a function from N into I.

(5) Let N, X, I be non empty sets and v_1, v_2 be functions. Suppose $\operatorname{dom} v_1 = \operatorname{dom} v_2 = I^X$. Let f be a function from X into N. If f is one-to-one and $v_1 \circ_N f = v_2 \circ_N f$, then $v_1 = v_2$.

Let X be a set. Observe that there exists a function from X into $\overline{\overline{X}}$ which is one-to-one and onto and there exists a function from $\overline{\overline{X}}$ into X which is one-to-one and onto.

Let X be a set. An enumeration of X is an one-to-one onto function from X into $\overline{\overline{X}}$. A denumeration of X is an one-to-one onto function from $\overline{\overline{X}}$ into X.

One can prove the following propositions:

(6) Let X be a set and f be a function. Then f is an enumeration of X if and only if $\operatorname{dom} f = X$ and $\operatorname{rng} f = \overline{\overline{X}}$ and f is one-to-one.

(7) Let X be a set and f be a function. Then f is a denumeration of X if and only if $\operatorname{dom} f = \overline{\overline{X}}$ and $\operatorname{rng} f = X$ and f is one-to-one.

(8) Let X be a non empty set, x, y be elements of X, and f be an enumeration of X. Then $f +\cdot (x, f(y)) +\cdot (y, f(x))$ is an enumeration of X.

(9) For every non empty set X and for every element x of X there exists an enumeration f of X such that $f(x) = 0$.

(10) For every non empty set X and for every denumeration f of X holds $f(0) \in X$.

(11) For every countable set X and for every enumeration f of X holds $\operatorname{rng} f \subseteq \mathbb{N}$.

Let X be a set and let f be an enumeration of X. Then f^{-1} is a denumeration of X.

Let X be a set and let f be a denumeration of X. Then f^{-1} is an enumeration of X.

We now state two propositions:

(12) For all natural numbers n, m holds $0^{n+m} = 0^n \cdot 0^m$.

(13) For every real number x and for all natural numbers n, m holds $(x^n)^m = x^{n \cdot m}$.

2. If-while Algebra over Integers

Let X be a non empty set. A $\mathbb{Z}$-variable of X is a function from $\mathbb{Z}^X$ into X. A $\mathbb{Z}$-expression of X is a function from $\mathbb{Z}^X$ into $\mathbb{Z}$. A $\mathbb{Z}$-array of X is a function from $\mathbb{Z}$ into X.

In the sequel A is a pre-if-while algebra.

Let us consider A, let I be an element of A, let X be a non empty set, let T be a subset of $\mathbb{Z}^X$, and let f be an execution function of A over $\mathbb{Z}^X$ and T. We say that I is an assignment w.r.t. A, X, and f if and only if the conditions (Def. 14) are satisfied.

(Def. 14)(i) $I \in \mathrm{ElementaryInstructions}_A$, and

(ii) there exists a $\mathbb{Z}$-variable v of X and there exists a $\mathbb{Z}$-expression t of X such that for every element s of $\mathbb{Z}^X$ holds $f(s, I) = s +\cdot (v(s), t(s))$.

Let us consider A, let X be a non empty set, let T be a subset of $\mathbb{Z}^X$, let f be an execution function of A over $\mathbb{Z}^X$ and T, let v be a $\mathbb{Z}$-variable of X, and let t be a $\mathbb{Z}$-expression of X. We say that v and t form an assignment w.r.t. f if and only if:

(Def. 15) There exists an element I of A such that $I \in \mathrm{ElementaryInstructions}_A$ and for every element s of $\mathbb{Z}^X$ holds $f(s, I) = s +\cdot (v(s), t(s))$.

Let us consider A, let X be a non empty set, let T be a subset of $\mathbb{Z}^X$, and let f be an execution function of A over $\mathbb{Z}^X$ and T. Let us assume that there exists an element of A which is an assignment w.r.t. A, X, and f. A $\mathbb{Z}$-variable of X is said to be a $\mathbb{Z}$-variable of A w.r.t. f if:

(Def. 16) There exists a $\mathbb{Z}$-expression t of X such that it and t form an assignment w.r.t. f.

Let us consider A, let X be a non empty set, let T be a subset of $\mathbb{Z}^X$, and let f be an execution function of A over $\mathbb{Z}^X$ and T. Let us assume that there exists an element of A which is an assignment w.r.t. A, X, and f. A $\mathbb{Z}$-expression of X is said to be a $\mathbb{Z}$-expression of A w.r.t. f if:

(Def. 17) There exists a $\mathbb{Z}$-variable v of X such that v and it form an assignment w.r.t. f.

Let X, Y be non empty sets, let f be an element of Y^X, and let x be an element of X. Then $f(x)$ is an element of Y.

Let X be a non empty set and let x be an element of X. The functor $\dot{x}$ yielding a $\mathbb{Z}$-expression of X is defined as follows:

(Def. 18) For every element s of $\mathbb{Z}^X$ holds $(\dot{x})(s) = s(x)$.

Let X be a non empty set and let v be a $\mathbb{Z}$-variable of X. The functor $\dot{v}$ yielding a $\mathbb{Z}$-expression of X is defined by:

(Def. 19) For every element s of $\mathbb{Z}^X$ holds $(\dot{v})(s) = s(v(s))$.

Let X be a non empty set and let x be an element of X. The functor $\hat{x}$ yields a $\mathbb{Z}$-variable of X and is defined by:

(Def. 20) $\hat{x} = \mathbb{Z}^X \longmapsto x$.

The following proposition is true

(14) For every non empty set X and for every element x of X holds $\dot{x} = \dot{\hat{x}}$.

Let X be a non empty set and let i be an integer number. The functor i_X yields a $\mathbb{Z}$-expression of X and is defined by:

(Def. 21) $i_X = \mathbb{Z}^X \longmapsto i$.

One can prove the following proposition

(15) For every non empty set X and for every $\mathbb{Z}$-expression t of X holds $t + 0_X = t$ and $t\,1_X = t$.

Let us consider A, let X be a non empty set, let T be a subset of $\mathbb{Z}^X$, and let f be an execution function of A over $\mathbb{Z}^X$ and T. We say that f is Euclidean if and only if the conditions (Def. 22) are satisfied.

(Def. 22) For every $\mathbb{Z}$-variable v of A w.r.t. f and for every $\mathbb{Z}$-expression t of A w.r.t. f holds v and t form an assignment w.r.t. f and for every integer number i holds i_X is a $\mathbb{Z}$-expression of A w.r.t. f and for every $\mathbb{Z}$-variable v of A w.r.t. f holds $\dot{v}$ is a $\mathbb{Z}$-expression of A w.r.t. f and for every element x of X holds $\hat{x}$ is a $\mathbb{Z}$-variable of A w.r.t. f and there exists a $\mathbb{Z}$-array a of X such that $a\restriction\overline{\overline{X}}$ is one-to-one and for every $\mathbb{Z}$-expression t of A w.r.t. f holds $a \cdot t$ is a $\mathbb{Z}$-variable of A w.r.t. f and for every $\mathbb{Z}$-expression t of A w.r.t. f holds $-t$ is a $\mathbb{Z}$-expression of A w.r.t. f and for all $\mathbb{Z}$-expressions t_1, t_2 of A w.r.t. f holds $t_1\,t_2$ is a $\mathbb{Z}$-expression of A w.r.t. f and $t_1 + t_2$ is a $\mathbb{Z}$-expression of A w.r.t. f and $t_1 \div t_2$ is a $\mathbb{Z}$-expression of A w.r.t. f and $t_1 \bmod t_2$ is a $\mathbb{Z}$-expression of A w.r.t. f and $\mathrm{leq}(t_1, t_2)$ is a $\mathbb{Z}$-expression of A w.r.t. f and $\mathrm{gt}(t_1, t_2)$ is a $\mathbb{Z}$-expression of A w.r.t. f.

Let us consider A. We say that A is Euclidean if and only if:

(Def. 23) For every non empty countable set X and for every subset T of $\mathbb{Z}^X$ holds there exists an execution function of A over $\mathbb{Z}^X$ and T which is Euclidean.

The infinite missing $\mathbb{N}$ set $\mathbb{Z}$-ElemIns is defined by:

(Def. 24) $\mathbb{Z}\text{-ElemIns} = \mathbb{N}^{\mathbb{Z}^{\mathbb{N}}} \times \mathbb{Z}^{\mathbb{Z}^{\mathbb{N}}}$.

An execution function of $\mathfrak{F}(\mathfrak{S}, \mathbb{Z}\text{-ElemIns})$ over $\mathbb{Z}^{\mathbb{N}}$ and $\mathbb{Z}^{\mathbb{N}}{\restriction}^{0}_{\neq 0}$ is said to be a $\mathbb{Z}$-execution if it satisfies the condition (Def. 25).

(Def. 25) Let s be an element of $\mathbb{Z}^{\mathbb{N}}$, v be an element of $\mathbb{N}^{\mathbb{Z}^{\mathbb{N}}}$, and e be an element of $\mathbb{Z}^{\mathbb{Z}^{\mathbb{N}}}$. Then $\mathrm{it}(s, \text{the root tree of } \langle v, e\rangle) = s +\cdot (v(s), e(s))$.

Let X be a non empty set. The functor $\mathbb{Z}\text{-ElemIns}\, X$ yielding an infinite missing $\mathbb{N}$ set is defined as follows:

(Def. 26) $\mathbb{Z}\text{-ElemIns}\, X = X^{\mathbb{Z}^X} \times \mathbb{Z}^{\mathbb{Z}^X}$.

Let X be a non empty set and let x be an element of X. An execution function of $\mathfrak{F}(\mathfrak{S}, \mathbb{Z}\text{-ElemIns}\, X)$ over $\mathbb{Z}^X$ and $\mathbb{Z}^X{\restriction}^{x}_{\neq 0}$ is said to be a $\mathbb{Z}$-execution with x if it satisfies the condition (Def. 27).

(Def. 27) Let s be an element of $\mathbb{Z}^X$, v be an element of $X^{\mathbb{Z}^X}$, and e be an element of $\mathbb{Z}^{\mathbb{Z}^X}$. Then $\mathrm{it}(s, \text{the root tree of } \langle v, e\rangle) = s +\cdot (v(s), e(s))$.

Let X be a non empty set, let T be a subset of $\mathbb{Z}^X$, and let c be an enumeration of X. Let us assume that $\operatorname{rng} c \subseteq \mathbb{N}$. An execution function of $\mathfrak{F}(\mathfrak{S}, \mathbb{Z}\text{-ElemIns})$ over $\mathbb{Z}^X$ and T is said to be a $\mathbb{Z}$-execution with c over T if it satisfies the condition (Def. 28).

(Def. 28) Let s be an element of $\mathbb{Z}^X$, v be an element of $X^{\mathbb{Z}^X}$, and e be an element of $\mathbb{Z}^{\mathbb{Z}^X}$. Then $\mathrm{it}(s, \text{the root tree of } \langle c \cdot v \circ_{\mathbb{N}} c, e \circ_{\mathbb{N}} c\rangle) = s +\cdot (v(s), e(s))$.

We now state three propositions:

(16) Let f be a $\mathbb{Z}$-execution, v be a $\mathbb{Z}$-variable of $\mathbb{N}$, and t be a $\mathbb{Z}$-expression of $\mathbb{N}$. Then v and t form an assignment w.r.t. f.

(17) For every $\mathbb{Z}$-execution f holds every $\mathbb{Z}$-variable of $\mathbb{N}$ is a $\mathbb{Z}$-variable of $\mathfrak{F}(\mathfrak{S}, \mathbb{Z}\text{-ElemIns})$ w.r.t. f.

(18) For every $\mathbb{Z}$-execution f holds every $\mathbb{Z}$-expression of $\mathbb{N}$ is a $\mathbb{Z}$-expression of $\mathfrak{F}(\mathfrak{S}, \mathbb{Z}\text{-ElemIns})$ w.r.t. f.

Let us mention that every $\mathbb{Z}$-execution is Euclidean.

One can prove the following three propositions:

(19) Let X be a non empty countable set, T be a subset of $\mathbb{Z}^X$, c be an enumeration of X, f be a $\mathbb{Z}$-execution with c over T, v be a $\mathbb{Z}$-variable of X, and t be a $\mathbb{Z}$-expression of X. Then v and t form an assignment w.r.t. f.

(20) Let X be a non empty countable set, T be a subset of $\mathbb{Z}^X$, c be an enumeration of X, and f be a $\mathbb{Z}$-execution with c over T. Then every $\mathbb{Z}$-variable of X is a $\mathbb{Z}$-variable of $\mathfrak{F}(\mathfrak{S}, \mathbb{Z}\text{-ElemIns})$ w.r.t. f.

(21) Let X be a non empty countable set, T be a subset of $\mathbb{Z}^X$, c be an enumeration of X, and f be a $\mathbb{Z}$-execution with c over T. Then every $\mathbb{Z}$-expression of X is a $\mathbb{Z}$-expression of $\mathfrak{F}(\mathfrak{S}, \mathbb{Z}\text{-ElemIns})$ w.r.t. f.

Let X be a countable non empty set, let T be a subset of $\mathbb{Z}^X$, and let c be an enumeration of X. Observe that every $\mathbb{Z}$-execution with c over T is Euclidean.

Let us observe that $\mathfrak{F}(\mathfrak{S}, \mathbb{Z}\text{-ElemIns})$ is Euclidean.

One can check that there exists a pre-if-while algebra which is Euclidean and non degenerated.

Let A be an Euclidean pre-if-while algebra, let X be a non empty countable set, and let T be a subset of $\mathbb{Z}^X$. Observe that there exists an execution function of A over $\mathbb{Z}^X$ and T which is Euclidean.

In the sequel A is an Euclidean pre-if-while algebra, X is a non empty countable set, T is a subset of $\mathbb{Z}^X$, and f is an Euclidean execution function of A over $\mathbb{Z}^X$ and T.

Let us consider A, X, T, f and let t be a $\mathbb{Z}$-expression of A w.r.t. f. Then $-t$ is a $\mathbb{Z}$-expression of A w.r.t. f.

Let us consider A, X, T, f, let t be a $\mathbb{Z}$-expression of A w.r.t. f, and let i be an integer number. Then $t + i$, $t - i$, and $t \cdot i$ are $\mathbb{Z}$-expressions of A w.r.t. f.

Let us consider A, X, T, f and let t_1, t_2 be $\mathbb{Z}$-expressions of A w.r.t. f. Then $t_1 - t_2$, $t_1 + t_2$, and $t_1\, t_2$ are $\mathbb{Z}$-expressions of A w.r.t. f. Moreover, $t_1 \div t_2$, $t_1 \bmod t_2$, $\mathrm{leq}(t_1, t_2)$, and $\mathrm{gt}(t_1, t_2)$ are also $\mathbb{Z}$-expressions of A w.r.t. f and they can be characterized by the conditions:

(Def. 29) For every element s of $\mathbb{Z}^X$ holds $(t_1 \div t_2)(s) = t_1(s) \div t_2(s)$.

(Def. 30) For every element s of $\mathbb{Z}^X$ holds $(t_1 \bmod t_2)(s) = t_1(s) \bmod t_2(s)$.

(Def. 31) For every element s of $\mathbb{Z}^X$ holds $(\mathrm{leq}(t_1, t_2))(s) = (t_1(s) > t_2(s) \to 0, 1)$.

(Def. 32) For every element s of $\mathbb{Z}^X$ holds $(\mathrm{gt}(t_1, t_2))(s) = (t_1(s) > t_2(s) \to 1, 0)$.

Let us consider A, X, T, f and let t_1, t_2 be $\mathbb{Z}$-expressions of A w.r.t. f. Then $\mathrm{eq}(t_1, t_2)$ is a $\mathbb{Z}$-expression of A w.r.t. f and it can be characterized by the condition:

(Def. 33) For every element s of $\mathbb{Z}^X$ holds $(\mathrm{eq}(t_1, t_2))(s) = (t_1(s) = t_2(s) \to 1, 0)$.

Let us consider A, X, T, f and let v be a $\mathbb{Z}$-variable of A w.r.t. f. The functor $\dot{v}$ yields a $\mathbb{Z}$-expression of A w.r.t. f and is defined by:

(Def. 34) $\dot{v} = \dot{x}$ where $x = v$ qua $\mathbb{Z}$-variable of X.

Let us consider A, X, T, f and let x be an element of X. The functor $\hat{x}_{A,f}$ yields a $\mathbb{Z}$-variable of A w.r.t. f and is defined as follows:

(Def. 35) $\hat{x}_{A,f} = \hat{x}$.

Let us consider A, X, T, f and let x be a variable in f. We introduce $\hat{x}$ as a synonym of $\hat{x}_{A,f}$.

Let us consider A, X, T, f and let x be a variable in f. The functor $\dot{x}$ yielding a $\mathbb{Z}$-expression of A w.r.t. f is defined as follows:

(Def. 36) $\dot{x} = \dot{\hat{x}}$.

The following proposition is true

(22) For every variable x in f and for every element s of $\mathbb{Z}^X$ holds $(\dot{x})(s) = s(x)$.

Let us consider A, X, T, f and let i be an integer number. The functor $i_{A,f}$ yields a $\mathbb{Z}$-expression of A w.r.t. f and is defined as follows:

(Def. 37) $i_{A,f} = i_X$.

Let us consider A, X, T, f, let v be a $\mathbb{Z}$-variable of A w.r.t. f, and let t be a $\mathbb{Z}$-expression of A w.r.t. f. The functor $v\,\mathtt{:=}\,t$ yielding an element of A is defined as follows:

(Def. 38) $v\,\mathtt{:=}\,t = \mathrm{choose}(\{I \in A\colon I \in \mathrm{ElementaryInstructions}_A \wedge \bigwedge_{s\,:\,\text{element of } \mathbb{Z}^X} f(s, I) = s +\cdot (v(s), t(s))\})$.

One can prove the following proposition

(23) Let v be a $\mathbb{Z}$-variable of A w.r.t. f and t be a $\mathbb{Z}$-expression of A w.r.t. f. Then $v\,\mathtt{:=}\,t \in \mathrm{ElementaryInstructions}_A$.

Let us consider A, X, T, f, let v be a $\mathbb{Z}$-variable of A w.r.t. f, and let t be a $\mathbb{Z}$-expression of A w.r.t. f. Observe that $v\,\mathtt{:=}\,t$ is absolutely-terminating.

Let us consider A, X, T, f, let v be a $\mathbb{Z}$-variable of A w.r.t. f, and let t be a $\mathbb{Z}$-expression of A w.r.t. f. The functors $v\mathtt{+=}t$ and $v\mathtt{*=}t$ yielding absolutely-terminating elements of A are defined by:

(Def. 39) $v\mathtt{+=}t = v\,\mathtt{:=}\,(\dot{v} + t)$.

(Def. 40) $v\mathtt{*=}t = v\,\mathtt{:=}\,(\dot{v}\,t)$.

Let us consider A, X, T, f, let x be an element of X, and let t be a $\mathbb{Z}$-expression of A w.r.t. f. The functor $x\,\mathtt{:=}\,t$ yielding an absolutely-terminating element of A is defined as follows:

(Def. 41) $x\,\mathtt{:=}\,t = \hat{x}_{A,f}\,\mathtt{:=}\,t$.

Let us consider A, X, T, f, let x be an element of X, and let y be a variable in f. The functor $x\,\mathtt{:=}\,y$ yields an absolutely-terminating element of A and is defined by:

(Def. 42) $x\,\mathtt{:=}\,y = x\,\mathtt{:=}\,\dot{y}$.

Let us consider A, X, T, f, let x be an element of X, and let v be a $\mathbb{Z}$-variable of A w.r.t. f. The functor $x\,\mathtt{:=}\,v$ yields an absolutely-terminating element of A and is defined by:

(Def. 43) $x\,\mathtt{:=}\,v = x\,\mathtt{:=}\,\dot{v}$.

Let us consider A, X, T, f and let v, w be $\mathbb{Z}$-variables of A w.r.t. f. The functor $v\,\mathtt{:=}\,w$ yielding an absolutely-terminating element of A is defined as follows:

(Def. 44) $v\,\mathtt{:=}\,w = v\,\mathtt{:=}\,\dot{w}$.

Let us consider A, X, T, f, let x be a variable in f, and let i be an integer number. The functor $x\,\mathtt{:=}\,i$ yielding an absolutely-terminating element of A is defined by:

(Def. 45) $x\,\mathtt{:=}\,i = x\,\mathtt{:=}\,(i_{A,f})$.

Let us consider A, X, T, f, let v_1, v_2 be $\mathbb{Z}$-variables of A w.r.t. f, and let x be a variable in f. The functor $\mathrm{swap}(v_1, x, v_2)$ yields an absolutely-terminating element of A and is defined by:

(Def. 46) $\mathrm{swap}(v_1, x, v_2) = x\,\mathtt{:=}\,v_1; v_1\,\mathtt{:=}\,v_2; v_2\,\mathtt{:=}\,\dot{x}$.

Let us consider A, X, T, f, let x be a variable in f, and let t be a $\mathbb{Z}$-expression of A w.r.t. f. The functors $x\mathtt{+=}t$, $x\mathtt{*=}t$, $x\mathtt{\%=}t$, and $x\mathtt{/=}t$ yielding absolutely-terminating elements of A are defined by:

(Def. 47) $x\mathtt{+=}t = x\,\mathtt{:=}\,(\dot{x} + t)$.

(Def. 48) $x\mathtt{*=}t = x\,\mathtt{:=}\,(\dot{x}\,t)$.

(Def. 49) $x\mathtt{\%=}t = x\,\mathtt{:=}\,(\dot{x} \bmod t)$.

(Def. 50) $x\mathtt{/=}t = x\,\mathtt{:=}\,(\dot{x} \div t)$.

Let us consider A, X, T, f, let x be a variable in f, and let i be an integer number. The functor $x\mathtt{+=}i$, $x\mathtt{*=}i$, $x\mathtt{\%=}i$, and $x\mathtt{/=}i$ yield absolutely-terminating elements of A and are defined as follows:

(Def. 51) $x\mathtt{+=}i = x\,\mathtt{:=}\,(\dot{x} + i)$.

(Def. 52) $x\mathtt{*=}i = x\,\mathtt{:=}\,(\dot{x} \cdot i)$.

(Def. 53) $x\mathtt{\%=}i = x\,\mathtt{:=}\,(\dot{x} \bmod i_{A,f})$.

(Def. 54) $x\mathtt{/=}i = x\,\mathtt{:=}\,(\dot{x} \div i_{A,f})$.

The functor $x \div i$ yields a $\mathbb{Z}$-expression of A w.r.t. f and is defined as follows:

(Def. 55) $x \div i = \dot{x} \div i_{A,f}$.

Let us consider A, X, T, f, let v be a $\mathbb{Z}$-variable of A w.r.t. f, and let i be an integer number. The functors $v\,\mathtt{:=}\,i$, $v\mathtt{+=}i$, and $v\mathtt{*=}i$ yield absolutely-terminating elements of A and are defined by:

(Def. 56) $v\,\mathtt{:=}\,i = v\,\mathtt{:=}\,(i_{A,f})$.

(Def. 57) $v\mathtt{+=}i = v\,\mathtt{:=}\,(\dot{v} + i)$.

(Def. 58) $v\mathtt{*=}i = v\,\mathtt{:=}\,(\dot{v} \cdot i)$.

Let us consider A, X, let b be an element of X, let g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X\restriction^b_{\neq 0}$, and let t_1 be a $\mathbb{Z}$-expression of A w.r.t. g. Absolutely-terminating elements "t_1 is odd" and "t_1 is even" of A are defined by:

(Def. 59) t_1 is odd $= b\,\mathtt{:=}\,(t_1 \bmod 2_{A,g})$.

(Def. 60) t_1 is even $= b\,\mathtt{:=}\,((t_1 + 1) \bmod 2_{A,g})$.

Let t_2 be a $\mathbb{Z}$-expression of A w.r.t. g. The functors $t_1\,\mathrm{leq}\,t_2$, $t_1\,\mathrm{gt}\,t_2$, and $t_1\,\mathrm{eq}\,t_2$ yield absolutely-terminating elements of A and are defined as follows:

(Def. 61) $t_1\,\mathrm{leq}\,t_2 = b\,\mathtt{:=}\,\mathrm{leq}(t_1, t_2)$.

The functor $t_1\,\mathrm{gt}\,t_2$ yields an absolutely-terminating element of A and is defined as follows:

(Def. 62) $t_1\,\mathrm{gt}\,t_2 = b\,\mathtt{:=}\,\mathrm{gt}(t_1, t_2)$.

(Def. 63) $t_1 \operatorname{eq} t_2 = b \mathbin{:=} \operatorname{eq}(t_1, t_2)$.

Let us consider A, X, let b be an element of X, let g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X \restriction^b_{\neq 0}$, and let t_1, t_2 be $\mathbb{Z}$-expressions of A w.r.t. g. We introduce $t_2 \operatorname{geq} t_1$ as a synonym of $t_1 \operatorname{leq} t_2$ and $t_2 \operatorname{lt} t_1$ as a synonym of $t_1 \operatorname{gt} t_2$.

Let us consider A, X, let b be an element of X, let g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X \restriction^b_{\neq 0}$, and let v_1, v_2 be $\mathbb{Z}$-variables of A w.r.t. g. The functors $v_1 \operatorname{leq} v_2$ and $v_1 \operatorname{gt} v_2$ yield absolutely-terminating elements of A and are defined as follows:

(Def. 64) $v_1 \operatorname{leq} v_2 = \dot{v_1} \operatorname{leq} \dot{v_2}$.

(Def. 65) $v_1 \operatorname{gt} v_2 = \dot{v_1} \operatorname{gt} \dot{v_2}$.

Let us consider A, X, let b be an element of X, let g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X \restriction^b_{\neq 0}$, and let v_1, v_2 be $\mathbb{Z}$-variables of A w.r.t. g. We introduce $v_2 \operatorname{geq} v_1$ as a synonym of $v_1 \operatorname{leq} v_2$ and $v_2 \operatorname{lt} v_1$ as a synonym of $v_1 \operatorname{gt} v_2$.

Let us consider A, X, let b be an element of X, let g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X \restriction^b_{\neq 0}$, and let x_1 be a variable in g. Absolutely-terminating elements "x_1 is odd" and "x_1 is even" of A are defined by:

(Def. 66) x_1 is odd $= (\dot{x_1})$ is odd.

(Def. 67) x_1 is even $= (\dot{x_1})$ is even.

Let x_2 be a variable in g. The functors $x_1 \operatorname{leq} x_2$ and $x_1 \operatorname{gt} x_2$ yield absolutely-terminating elements of A and are defined by:

(Def. 68) $x_1 \operatorname{leq} x_2 = \dot{x_1} \operatorname{leq} \dot{x_2}$.

(Def. 69) $x_1 \operatorname{gt} x_2 = \dot{x_1} \operatorname{gt} \dot{x_2}$.

Let us consider A, X, let b be an element of X, let g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X \restriction^b_{\neq 0}$, and let x_1, x_2 be variables in g. We introduce $x_2 \operatorname{geq} x_1$ as a synonym of $x_1 \operatorname{leq} x_2$ and $x_2 \operatorname{lt} x_1$ as a synonym of $x_1 \operatorname{gt} x_2$.

Let us consider A, X, let b be an element of X, let g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X \restriction^b_{\neq 0}$, let x be a variable in g, and let i be an integer number. The functors $x \operatorname{leq} i$, $x \operatorname{geq} i$, $x \operatorname{gt} i$, and $x \operatorname{lt} i$ yielding absolutely-terminating elements of A are defined as follows:

(Def. 70) $x \operatorname{leq} i = \dot{x} \operatorname{leq} i_{A,g}$.

(Def. 71) $x \operatorname{geq} i = \dot{x} \operatorname{geq} i_{A,g}$.

(Def. 72) $x \operatorname{gt} i = \dot{x} \operatorname{gt} i_{A,g}$.

(Def. 73) $x \operatorname{lt} i = \dot{x} \operatorname{lt} i_{A,g}$.

The functor $\frac{x}{i}$ yielding a $\mathbb{Z}$-expression of A w.r.t. g is defined as follows:

(Def. 74) $\frac{x}{i} = \dot{x} \div i_{A,g}$.

Let us consider A, X, T, f and let x_1, x_2 be variables in f. The functors $x_1\texttt{+=}x_2$, $x_1\texttt{*=}x_2$, $x_1\texttt{\%=}x_2$, and $x_1\texttt{/=}x_2$ yielding absolutely-terminating elements of A are defined as follows:

(Def. 75) $x_1\texttt{+=}x_2 = x_1\texttt{+=}\dot{x_2}$.

(Def. 76) $x_1\texttt{*=}x_2 = x_1\texttt{*=}\dot{x_2}$.

(Def. 77) $x_1\texttt{\%=}x_2 = x_1\texttt{:=}(\dot{x_1} \bmod \dot{x_2})$.

(Def. 78) $x_1\texttt{/=}x_2 = x_1\texttt{:=}(\dot{x_1} \div \dot{x_2})$.

The functors $x_1 + x_2$, $x_1 \cdot x_2$, $x_1 \bmod x_2$, and $x_1 \div x_2$ yield $\mathbb{Z}$-expressions of A w.r.t. f and are defined as follows:

(Def. 79) $x_1 + x_2 = \dot{x_1} + \dot{x_2}$.

(Def. 80) $x_1 \cdot x_2 = \dot{x_1}\,\dot{x_2}$.

(Def. 81) $x_1 \bmod x_2 = \dot{x_1} \bmod \dot{x_2}$.

(Def. 82) $x_1 \div x_2 = \dot{x_1} \div \dot{x_2}$.

For simplicity, we follow the rules: A denotes an Euclidean pre-if-while algebra, X denotes a non empty countable set, x, y, z denote elements of X, s denotes an element of $\mathbb{Z}^X$, T denotes a subset of $\mathbb{Z}^X$, f denotes an Euclidean execution function of A over $\mathbb{Z}^X$ and T, v denotes a $\mathbb{Z}$-variable of A w.r.t. f, t denotes a $\mathbb{Z}$-expression of A w.r.t. f, and i denotes an integer number.

Next we state a number of propositions:

(24) $f(s, v\texttt{:=}t)(v(s)) = t(s)$ and for every z such that $z \neq v(s)$ holds $f(s, v\texttt{:=}t)(z) = s(z)$.

(25) Let x be a variable in f and i be an integer number. Then $f(s, x\texttt{:=}i)(x) = i$ and for every z such that $z \neq x$ holds $f(s, x\texttt{:=}i)(z) = s(z)$.

(26) Let x be a variable in f and t be a $\mathbb{Z}$-expression of A w.r.t. f. Then $f(s, x\texttt{:=}t)(x) = t(s)$ and for every z such that $z \neq x$ holds $f(s, x\texttt{:=}t)(z) = s(z)$.

(27) For all variables x, y in f holds $f(s, x\texttt{:=}y)(x) = s(y)$ and for every z such that $z \neq x$ holds $f(s, x\texttt{:=}y)(z) = s(z)$.

(28) For every variable x in f holds $f(s, x\texttt{+=}i)(x) = s(x) + i$ and for every z such that $z \neq x$ holds $f(s, x\texttt{+=}i)(z) = s(z)$.

(29) Let x be a variable in f and t be a $\mathbb{Z}$-expression of A w.r.t. f. Then $f(s, x\texttt{+=}t)(x) = s(x) + t(s)$ and for every z such that $z \neq x$ holds $f(s, x\texttt{+=}t)(z) = s(z)$.

(30) For all variables x, y in f holds $f(s, x\texttt{+=}y)(x) = s(x) + s(y)$ and for every z such that $z \neq x$ holds $f(s, x\texttt{+=}y)(z) = s(z)$.

(31) For every variable x in f holds $f(s, x\texttt{*=}i)(x) = s(x) \cdot i$ and for every z such that $z \neq x$ holds $f(s, x\texttt{*=}i)(z) = s(z)$.

(32) Let x be a variable in f and t be a $\mathbb{Z}$-expression of A w.r.t. f. Then $f(s, x\texttt{*=}t)(x) = s(x) \cdot t(s)$ and for every z such that $z \neq x$ holds $f(s,$

$x\mathbin{*=}t)(z) = s(z)$.

(33) For all variables x, y in f holds $f(s, x\mathbin{*=}y)(x) = s(x) \cdot s(y)$ and for every z such that $z \neq x$ holds $f(s, x\mathbin{*=}y)(z) = s(z)$.

(34) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X\restriction^b_{\neq 0}$, x be a variable in g, and i be an integer number. Then

(i) if $s(x) \leq i$, then $g(s, x \operatorname{leq} i)(b) = 1$,

(ii) if $s(x) > i$, then $g(s, x \operatorname{leq} i)(b) = 0$,

(iii) if $s(x) \geq i$, then $g(s, x \operatorname{geq} i)(b) = 1$,

(iv) if $s(x) < i$, then $g(s, x \operatorname{geq} i)(b) = 0$, and

(v) for every z such that $z \neq b$ holds $g(s, x \operatorname{leq} i)(z) = s(z)$ and $g(s, x \operatorname{geq} i)(z) = s(z)$.

(35) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X\restriction^b_{\neq 0}$, and x, y be variables in g. Then if $s(x) \leq s(y)$, then $g(s, x \operatorname{leq} y)(b) = 1$ and if $s(x) > s(y)$, then $g(s, x \operatorname{leq} y)(b) = 0$ and for every z such that $z \neq b$ holds $g(s, x \operatorname{leq} y)(z) = s(z)$.

(36) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X\restriction^b_{\neq 0}$, x be a variable in g, and i be an integer number. Then

(i) $s(x) \leq i$ iff $g(s, x \operatorname{leq} i) \in \mathbb{Z}^X\restriction^b_{\neq 0}$, and

(ii) $s(x) \geq i$ iff $g(s, x \operatorname{geq} i) \in \mathbb{Z}^X\restriction^b_{\neq 0}$.

(37) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X\restriction^b_{\neq 0}$, and x, y be variables in g. Then

(i) $s(x) \leq s(y)$ iff $g(s, x \operatorname{leq} y) \in \mathbb{Z}^X\restriction^b_{\neq 0}$, and

(ii) $s(x) \geq s(y)$ iff $g(s, x \operatorname{geq} y) \in \mathbb{Z}^X\restriction^b_{\neq 0}$.

(38) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X\restriction^b_{\neq 0}$, x be a variable in g, and i be an integer number. Then

(i) if $s(x) > i$, then $g(s, x \operatorname{gt} i)(b) = 1$,

(ii) if $s(x) \leq i$, then $g(s, x \operatorname{gt} i)(b) = 0$,

(iii) if $s(x) < i$, then $g(s, x \operatorname{lt} i)(b) = 1$,

(iv) if $s(x) \geq i$, then $g(s, x \operatorname{lt} i)(b) = 0$, and

(v) for every z such that $z \neq b$ holds $g(s, x \operatorname{gt} i)(z) = s(z)$ and $g(s, x \operatorname{lt} i)(z) = s(z)$.

(39) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X\restriction^b_{\neq 0}$, and x, y be variables in g. Then

(i) if $s(x) > s(y)$, then $g(s, x \operatorname{gt} y)(b) = 1$,

(ii) if $s(x) \leq s(y)$, then $g(s, x \operatorname{gt} y)(b) = 0$,

(iii) if $s(x) < s(y)$, then $g(s, x \operatorname{lt} y)(b) = 1$,

(iv) if $s(x) \geq s(y)$, then $g(s, x \operatorname{lt} y)(b) = 0$, and

(v) for every z such that $z \neq b$ holds $g(s, x \operatorname{gt} y)(z) = s(z)$ and $g(s, x \operatorname{lt} y)(z) = s(z)$.

(40) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X \restriction^b_{\neq 0}$, x be a variable in g, and i be an integer number. Then

(i) $s(x) > i$ iff $g(s, x \operatorname{gt} i) \in \mathbb{Z}^X \restriction^b_{\neq 0}$, and

(ii) $s(x) < i$ iff $g(s, x \operatorname{lt} i) \in \mathbb{Z}^X \restriction^b_{\neq 0}$.

(41) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X \restriction^b_{\neq 0}$, and x, y be variables in g. Then

(i) $s(x) > s(y)$ iff $g(s, x \operatorname{gt} y) \in \mathbb{Z}^X \restriction^b_{\neq 0}$, and

(ii) $s(x) < s(y)$ iff $g(s, x \operatorname{lt} y) \in \mathbb{Z}^X \restriction^b_{\neq 0}$.

(42) For every variable x in f holds $f(s, x\%{=}\, i)(x) = s(x) \bmod i$ and for every z such that $z \neq x$ holds $f(s, x\%{=}\, i)(z) = s(z)$.

(43) Let x be a variable in f and t be a $\mathbb{Z}$-expression of A w.r.t. f. Then $f(s, x\%{=}\, t)(x) = s(x) \bmod t(s)$ and for every z such that $z \neq x$ holds $f(s, x\%{=}\, t)(z) = s(z)$.

(44) For all variables x, y in f holds $f(s, x\%{=}\, y)(x) = s(x) \bmod s(y)$ and for every z such that $z \neq x$ holds $f(s, x\%{=}\, y)(z) = s(z)$.

(45) For every variable x in f holds $f(s, x/{=}\, i)(x) = s(x) \div i$ and for every z such that $z \neq x$ holds $f(s, x/{=}\, i)(z) = s(z)$.

(46) Let x be a variable in f and t be a $\mathbb{Z}$-expression of A w.r.t. f. Then $f(s, x/{=}\, t)(x) = s(x) \div t(s)$ and for every z such that $z \neq x$ holds $f(s, x/{=}\, t)(z) = s(z)$.

(47) For all variables x, y in f holds $f(s, x/{=}\, y)(x) = s(x) \div s(y)$ and for every z such that $z \neq x$ holds $f(s, x/{=}\, y)(z) = s(z)$.

(48) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X \restriction^b_{\neq 0}$, and t be a $\mathbb{Z}$-expression of A w.r.t. g. Then

(i) $g(s, t \text{ is odd})(b) = t(s) \bmod 2$,

(ii) $g(s, t \text{ is even})(b) = (t(s) + 1) \bmod 2$, and

(iii) for every z such that $z \neq b$ holds $g(s, t \text{ is odd})(z) = s(z)$ and $g(s, t \text{ is even})(z) = s(z)$.

(49) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X \restriction^b_{\neq 0}$, and x be a variable in g. Then

(i) $g(s, x \text{ is odd})(b) = s(x) \bmod 2$,

(ii) $g(s, x \text{ is even})(b) = (s(x) + 1) \bmod 2$, and

(iii) for every z such that $z \neq b$ holds $g(s, x \text{ is odd})(z) = s(z)$.

(50) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X \restriction^b_{\neq 0}$, and t be a $\mathbb{Z}$-expression of A w.r.t. g. Then

(i) $t(s)$ is odd iff $g(s, t \text{ is odd}) \in \mathbb{Z}^X \restriction^b_{\neq 0}$, and

(ii) $t(s)$ is even iff $g(s, t \text{ is even}) \in \mathbb{Z}^X \restriction^b_{\neq 0}$.

(51) Let b be an element of X, g be an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X{\restriction}^b_{\neq 0}$, and x be a variable in g. Then

(i) $s(x)$ is odd iff $g(s,\ x \text{ is odd}) \in \mathbb{Z}^X{\restriction}^b_{\neq 0}$, and

(ii) $s(x)$ is even iff $g(s,\ x \text{ is even}) \in \mathbb{Z}^X{\restriction}^b_{\neq 0}$.

In this article we present several logical schemes. The scheme *ForToIteration* deals with an Euclidean pre-if-while algebra $\mathcal{A}$, a countable non empty set $\mathcal{B}$, an element $\mathcal{C}$ of $\mathcal{B}$, elements $\mathcal{D}$, $\mathcal{E}$ of $\mathcal{A}$, an Euclidean execution function $\mathcal{F}$ of $\mathcal{A}$ over $\mathbb{Z}^{\mathcal{B}}$ and $\mathbb{Z}^{\mathcal{B}}{\restriction}^{\mathcal{C}}_{\neq 0}$, variables $\mathcal{G}$, $\mathcal{H}$ in $\mathcal{F}$, an element $\mathcal{I}$ of $\mathbb{Z}^{\mathcal{B}}$, a $\mathbb{Z}$-expression $\mathcal{J}$ of $\mathcal{A}$ w.r.t. $\mathcal{F}$, and a unary predicate $\mathcal{P}$, and states that:

$\mathcal{P}[\mathcal{F}(\mathcal{I},\ \mathcal{E})]$ and if $\mathcal{J}(\mathcal{I}) \leq \mathcal{I}(\mathcal{H})$, then $\mathcal{F}(\mathcal{I},\ \mathcal{E})(\mathcal{G}) = \mathcal{I}(\mathcal{H}) + 1$ and if $\mathcal{J}(\mathcal{I}) > \mathcal{I}(\mathcal{H})$, then $\mathcal{F}(\mathcal{I},\ \mathcal{E})(\mathcal{G}) = \mathcal{J}(\mathcal{I})$ and $\mathcal{F}(\mathcal{I},\ \mathcal{E})(\mathcal{H}) = \mathcal{I}(\mathcal{H})$

provided the following conditions are met:

- $\mathcal{E} = \texttt{for}\ \mathcal{G}\ \texttt{:=}\ \mathcal{J}\ \texttt{until}\ \mathcal{G} \operatorname{leq} \mathcal{H}\ \texttt{step}\ \mathcal{G}\ \texttt{+=}\ 1\ \texttt{do}\ \mathcal{D}\ \texttt{done}$,
- $\mathcal{P}[\mathcal{F}(\mathcal{I},\ \mathcal{G}\ \texttt{:=}\ \mathcal{J})]$,
- For every element s of $\mathbb{Z}^{\mathcal{B}}$ such that $\mathcal{P}[s]$ holds $\mathcal{P}[\mathcal{F}(s,\ \mathcal{D}; \mathcal{G}\ \texttt{+=}\ 1)]$ and $\mathcal{P}[\mathcal{F}(s,\ \mathcal{G} \operatorname{leq} \mathcal{H})]$,
- For every element s of $\mathbb{Z}^{\mathcal{B}}$ such that $\mathcal{P}[s]$ holds $\mathcal{F}(s,\ \mathcal{D})(\mathcal{G}) = s(\mathcal{G})$ and $\mathcal{F}(s,\ \mathcal{D})(\mathcal{H}) = s(\mathcal{H})$, and
- $\mathcal{H} \neq \mathcal{G}$ and $\mathcal{H} \neq \mathcal{C}$ and $\mathcal{G} \neq \mathcal{C}$.

The scheme *ForDowntoIteration* deals with an Euclidean pre-if-while algebra $\mathcal{A}$, a countable non empty set $\mathcal{B}$, an element $\mathcal{C}$ of $\mathcal{B}$, elements $\mathcal{D}$, $\mathcal{E}$ of $\mathcal{A}$, an Euclidean execution function $\mathcal{F}$ of $\mathcal{A}$ over $\mathbb{Z}^{\mathcal{B}}$ and $\mathbb{Z}^{\mathcal{B}}{\restriction}^{\mathcal{C}}_{\neq 0}$, variables $\mathcal{G}$, $\mathcal{H}$ in $\mathcal{F}$, an element $\mathcal{I}$ of $\mathbb{Z}^{\mathcal{B}}$, a $\mathbb{Z}$-expression $\mathcal{J}$ of $\mathcal{A}$ w.r.t. $\mathcal{F}$, and a unary predicate $\mathcal{P}$, and states that:

$\mathcal{P}[\mathcal{F}(\mathcal{I},\ \mathcal{E})]$ and if $\mathcal{J}(\mathcal{I}) \geq \mathcal{I}(\mathcal{H})$, then $\mathcal{F}(\mathcal{I},\ \mathcal{E})(\mathcal{G}) = \mathcal{I}(\mathcal{H}) - 1$ and if $\mathcal{J}(\mathcal{I}) < \mathcal{I}(\mathcal{H})$, then $\mathcal{F}(\mathcal{I},\ \mathcal{E})(\mathcal{G}) = \mathcal{J}(\mathcal{I})$ and $\mathcal{F}(\mathcal{I},\ \mathcal{E})(\mathcal{H}) = \mathcal{I}(\mathcal{H})$

provided the following conditions are satisfied:

- $\mathcal{E} = \texttt{for}\ \mathcal{G}\ \texttt{:=}\ \mathcal{J}\ \texttt{until}\ \dot{\mathcal{H}} \operatorname{leq} \dot{\mathcal{G}}\ \texttt{step}\ \mathcal{G}\ \texttt{+=}\ (-1)\ \texttt{do}\ \mathcal{D}\ \texttt{done}$,
- $\mathcal{P}[\mathcal{F}(\mathcal{I},\ \mathcal{G}\ \texttt{:=}\ \mathcal{J})]$,
- For every element s of $\mathbb{Z}^{\mathcal{B}}$ such that $\mathcal{P}[s]$ holds $\mathcal{P}[\mathcal{F}(s,\ \mathcal{D}; \mathcal{G}\ \texttt{+=}\ (-1))]$ and $\mathcal{P}[\mathcal{F}(s,\ \mathcal{H} \operatorname{leq} \mathcal{G})]$,
- For every element s of $\mathbb{Z}^{\mathcal{B}}$ such that $\mathcal{P}[s]$ holds $\mathcal{F}(s,\ \mathcal{D})(\mathcal{G}) = s(\mathcal{G})$ and $\mathcal{F}(s,\ \mathcal{D})(\mathcal{H}) = s(\mathcal{H})$, and
- $\mathcal{H} \neq \mathcal{G}$ and $\mathcal{H} \neq \mathcal{C}$ and $\mathcal{G} \neq \mathcal{C}$.

3. Termination in If-while Algebras over Integers

In the sequel b denotes an element of X and g denotes an Euclidean execution function of A over $\mathbb{Z}^X$ and $\mathbb{Z}^X{\restriction}^b_{\neq 0}$.

One can prove the following four propositions:

(52) Let I be an element of A and i, n be variables in g. Suppose there exists a function d such that $d(b) = 0$ and $d(n) = 1$ and $d(i) = 2$ and for every s holds $g(s, I)(n) = s(n)$ and $g(s, I)(i) = s(i)$. Then iteration of g started in $I; i\texttt{+=}1; i \operatorname{leq} n$ terminates w.r.t. $g(s, i \operatorname{leq} n)$.

(53) Let P be a set, I be an element of A, and i, n be variables in g. Suppose that

(i) there exists a function d such that $d(b) = 0$ and $d(n) = 1$ and $d(i) = 2$, and

(ii) for every s such that $s \in P$ holds $g(s, I)(n) = s(n)$ and $g(s, I)(i) = s(i)$ and $g(s, I)$, $g(s, i \operatorname{leq} n)$, $g(s, i\texttt{+=}1) \in P$.

Suppose $s \in P$. Then iteration of g started in $I; i\texttt{+=}1; i \operatorname{leq} n$ terminates w.r.t. $g(s, i \operatorname{leq} n)$.

(54) Let I be an element of A. Suppose I is terminating w.r.t. g. Let i, n be variables in g. Suppose there exists a function d such that $d(b) = 0$ and $d(n) = 1$ and $d(i) = 2$ and for every s holds $g(s, I)(n) = s(n)$ and $g(s, I)(i) = s(i)$. Then $\texttt{for}\, i\texttt{:=}t\ \texttt{until}\ i \operatorname{leq} n\ \texttt{step}\ i\texttt{+=}1\ \texttt{do}\ I\ \texttt{done}$ is terminating w.r.t. g.

(55) Let P be a set and I be an element of A. Suppose I is terminating w.r.t. g and P. Let i, n be variables in g. Suppose that

(i) there exists a function d such that $d(b) = 0$ and $d(n) = 1$ and $d(i) = 2$,

(ii) for every s such that $s \in P$ holds $g(s, I)(n) = s(n)$ and $g(s, I)(i) = s(i)$, and

(iii) P is invariant w.r.t. $i\texttt{:=}t$ and g, invariant w.r.t. I and g, invariant w.r.t. $i \operatorname{leq} n$ and g, and invariant w.r.t. $i\texttt{+=}1$ and g.

Then $\texttt{for}\, i\texttt{:=}t\ \texttt{until}\ i \operatorname{leq} n\ \texttt{step}\ i\texttt{+=}1\ \texttt{do}\ I\ \texttt{done}$ is terminating w.r.t. g and P.

4. Examples

Let us consider X, A, T, f, s and let I be an element of A. Then $f(s, I)$ is an element of $\mathbb{Z}^X$.

One can prove the following propositions. Let F denotes the program:

```
s:=1;
for i:=2 until i leq n step i+=1 do
  s*=i
done
```

(56) Let n, s, i be variables in g. Given a function d such that $d(n) = 1$ and $d(s) = 2$ and $d(i) = 3$ and $d(b) = 4$. Then F is terminating w.r.t. g.

(57) Let n, s, i be variables in g. Given a function d such that $d(n) = 1$ and $d(s) = 2$ and $d(i) = 3$ and $d(b) = 4$. Let q be an element of $\mathbb{Z}^X$ and N be a natural number. If $N = q(n)$, then $g(q, F)(s) = N!$.

Let P_0 denotes the program:

```
s:=1;
for i:=1 until i leq n step i+=1 do
  s*=x
done
```

(58) Let x, n, s, i be variables in g. Given a function d such that $d(x) = 0$ and $d(n) = 1$ and $d(s) = 2$ and $d(i) = 3$ and $d(b) = 4$. Then P_0 is terminating w.r.t. g.

(59) Let x, n, s, i be variables in g. Given a function d such that $d(x) = 0$ and $d(n) = 1$ and $d(s) = 2$ and $d(i) = 3$ and $d(b) = 4$. Let q be an element of $\mathbb{Z}^X$ and N be a natural number. If $N = q(n)$, then $g(q, P_0)(s) = q(x)^N$.

Let Fib denotes the program:

```
x:=0;
y:=1;
for i:=1 until i leq n step i+=1 do
  z:=x; x:=y; y+=z
done
```

(60) Let n, x, y, z, i be variables in g. Given a function d such that $d(b) = 0$ and $d(n) = 1$ and $d(x) = 2$ and $d(y) = 3$ and $d(z) = 4$ and $d(i) = 5$. Then Fib is terminating w.r.t. g.

(61) Let n, x, y, z, i be variables in g. Given a function d such that $d(b) = 0$ and $d(n) = 1$ and $d(x) = 2$ and $d(y) = 3$ and $d(z) = 4$ and $d(i) = 5$. Let s be an element of $\mathbb{Z}^X$ and N be an element of $\mathbb{N}$. If $N = s(n)$, then $g(s, Fib)(x) = \mathrm{Fib}(N)$.

Let GCD_1 denotes the program:

```
while y gt 0 do
  z:=x; z%=y;
  x:=y; y:=z
done
```

(62) Let x, y, z be variables in g. Given a function d such that $d(b) = 0$ and $d(x) = 1$ and $d(y) = 2$ and $d(z) = 3$. Then GCD_1 is terminating w.r.t. g and $\{s : s(x) > s(y) \ \wedge \ s(y) \geq 0\}$.

(63) Let x, y, z be variables in g. Given a function d such that $d(b) = 0$ and $d(x) = 1$ and $d(y) = 2$ and $d(z) = 3$. Let s be an element of $\mathbb{Z}^X$ and n, m be elements of $\mathbb{N}$. If $n = s(x)$ and $m = s(y)$ and $n > m$, then $g(s, GCD_1)(x) = \gcd(n, m)$.

Let GCD_2 denotes the program:

```
while y gt 0 do
  z := (x˙ − y˙);
  if z lt 0 then z*= −1 fi;
  x := y;
  y := z
done
```

(64) Let x, y, z be variables in g. Given a function d such that $d(b) = 0$ and $d(x) = 1$ and $d(y) = 2$ and $d(z) = 3$. Then GCD_2 is terminating w.r.t. g and $\{s : s(x) \geq 0 \ \wedge \ s(y) \geq 0\}$.

(65) Let x, y, z be variables in g. Given a function d such that $d(b) = 0$ and $d(x) = 1$ and $d(y) = 2$ and $d(z) = 3$. Let s be an element of $\mathbb{Z}^X$ and n, m be elements of $\mathbb{N}$. Suppose $n = s(x)$ and $m = s(y)$ and $n > 0$. Then $g(s, GCD_2)(x) = \gcd(n, m)$.

Let P_1 denotes the program:

```
y := 1;
while m gt 0 do
  if m is odd then y*= x fi;
  m/= 2;
  x*= x
done
```

(66) Let x, y, m be variables in g. Given a function d such that $d(b) = 0$ and $d(x) = 1$ and $d(y) = 2$ and $d(m) = 3$. Then P_1 is terminating w.r.t. g and $\{s : s(m) \geq 0\}$.

(67) Let x, y, m be variables in g. Given a function d such that $d(b) = 0$ and $d(x) = 1$ and $d(y) = 2$ and $d(m) = 3$. Let s be an element of $\mathbb{Z}^X$ and n be a natural number. If $n = s(m)$, then $g(s, P_1)(y) = s(x)^n$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek. Countable sets and Hessenberg's theorem. *Formalized Mathematics*, 2(**1**):65–69, 1991.
[4] Grzegorz Bancerek. Joining of decorated trees. *Formalized Mathematics*, 4(**1**):77–82, 1993.
[5] Grzegorz Bancerek. Mizar analysis of algorithms: Preliminaries. *Formalized Mathematics*, 15(**3**):87–110, 2007.
[6] Grzegorz Bancerek and Piotr Rudnicki. On defining functions on trees. *Formalized Mathematics*, 4(**1**):91–101, 1993.
[7] Grzegorz Bancerek and Piotr Rudnicki. Two programs for **scm**. Part I – preliminaries. *Formalized Mathematics*, 4(**1**):69–72, 1993.
[8] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.
[9] Józef Białas. Infimum and supremum of the set of real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):163–171, 1991.
[10] Ewa Burakowska. Subalgebras of the universal algebra. Lattices of subalgebras. *Formalized Mathematics*, 4(**1**):23–27, 1993.

[11] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[12] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[13] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[14] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.
[15] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[16] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[17] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[18] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definitions and basic properties of measurable functions. *Formalized Mathematics*, 9(**3**):495–500, 2001.
[19] Jarosław Kotowicz, Beata Madras, and Małgorzata Korolkiewicz. Basic notation of universal algebra. *Formalized Mathematics*, 3(**2**):251–253, 1992.
[20] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[21] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[22] Yatsuka Nakamura and Andrzej Trybulec. On a mathematical model of programs. *Formalized Mathematics*, 3(**2**):241–250, 1992.
[23] Beata Perkowska. Free universal algebra construction. *Formalized Mathematics*, 4(**1**):115–120, 1993.
[24] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.
[25] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.
[26] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[27] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[28] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.
[29] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[30] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[31] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[32] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received March 18, 2008