Contents

Formaliz. Math. 16 (**2**)

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 91–96, 2008

Helly Property for Subtrees[1]

Jessica Enright
University of Alberta
Edmonton, Canada

Piotr Rudnicki
University of Alberta
Edmonton, Canada

Summary. We prove, following [5, p. 92], that any family of subtrees of a finite tree satisfies the Helly property.

MML identifier: `HELLY`, version: `7.8.09 4.97.1001`

The articles [12], [4], [10], [3], [2], [1], [11], [9], [8], [7], and [6] provide the notation and terminology for this paper.

1. General Preliminaries

One can prove the following proposition

(1) For every non empty finite sequence p holds $\langle p(1)\rangle \mathbin{^\frown} p = p$.

Let p, q be finite sequences. The functor $\mathrm{maxPrefix}(p,q)$ yields a finite sequence and is defined by:

(Def. 1) $\mathrm{maxPrefix}(p,q) \preceq p$ and $\mathrm{maxPrefix}(p,q) \preceq q$ and for every finite sequence r such that $r \preceq p$ and $r \preceq q$ holds $r \preceq \mathrm{maxPrefix}(p,q)$.

Let us observe that the functor $\mathrm{maxPrefix}(p,q)$ is commutative.

Next we state several propositions:

(2) For all finite sequences p, q holds $p \preceq q$ iff $\mathrm{maxPrefix}(p,q) = p$.

(3) For all finite sequences p, q holds $\mathrm{len}\,\mathrm{maxPrefix}(p,q) \leq \mathrm{len}\, p$.

(4) For every non empty finite sequence p holds $\langle p(1)\rangle \preceq p$.

(5) For all non empty finite sequences p, q such that $p(1) = q(1)$ holds $1 \leq \mathrm{len}\,\mathrm{maxPrefix}(p,q)$.

[1] This work has been partially supported by the NSERC grant OGP 9207.

ISSN 1426–2630(p), 1898-9934(e)

(6) For all finite sequences p, q and for every natural number j such that $j \leq \operatorname{len} \operatorname{maxPrefix}(p,q)$ holds $(\operatorname{maxPrefix}(p,q))(j) = p(j)$.

(7) For all finite sequences p, q and for every natural number j such that $j \leq \operatorname{len} \operatorname{maxPrefix}(p,q)$ holds $p(j) = q(j)$.

(8) For all finite sequences p, q holds $p \not\preceq q$ iff $\operatorname{len} \operatorname{maxPrefix}(p,q) < \operatorname{len} p$.

(9) For all finite sequences p, q such that $p \not\preceq q$ and $q \not\preceq p$ holds $p(\operatorname{len} \operatorname{maxPrefix}(p,q)+1) \neq q(\operatorname{len} \operatorname{maxPrefix}(p,q)+1)$.

2. Graph Preliminaries

Next we state three propositions:

(10) For every graph G and for every walk W of G and for all natural numbers m, n holds $\operatorname{len}(W.\mathrm{cut}(m,n)) \leq \operatorname{len} W$.

(11) Let G be a graph, W be a walk of G, and m, n be natural numbers. If $W.\mathrm{cut}(m,n)$ is non trivial, then W is non trivial.

(12) Let G be a graph, W be a walk of G, and m, n, i be odd natural numbers. Suppose $m \leq n \leq \operatorname{len} W$ and $i \leq \operatorname{len}(W.\mathrm{cut}(m,n))$. Then there exists an odd natural number j such that $(W.\mathrm{cut}(m,n))(i) = W(j)$ and $j = (m+i)-1$ and $j \leq \operatorname{len} W$.

Let G be a graph. One can verify that every walk of G is non empty.

The following propositions are true:

(13) For every graph G and for all walks W_1, W_2 of G such that $W_1 \preceq W_2$ holds $W_1.\mathrm{vertices}() \subseteq W_2.\mathrm{vertices}()$.

(14) For every graph G and for all walks W_1, W_2 of G such that $W_1 \preceq W_2$ holds $W_1.\mathrm{edges}() \subseteq W_2.\mathrm{edges}()$.

(15) For every graph G and for all walks W_1, W_2 of G holds $W_1 \preceq W_1.\mathrm{append}(W_2)$.

(16) For every graph G and for all trails W_1, W_2 of G such that $W_1.\mathrm{last}() = W_2.\mathrm{first}()$ and $W_1.\mathrm{edges}()$ misses $W_2.\mathrm{edges}()$ holds $W_1.\mathrm{append}(W_2)$ is trail-like.

(17) Let G be a graph and P_1, P_2 be paths of G. Suppose $P_1.\mathrm{last}() = P_2.\mathrm{first}()$ and P_1 is open and P_2 is open and $P_1.\mathrm{edges}()$ misses $P_2.\mathrm{edges}()$ and if $P_1.\mathrm{first}() \in P_2.\mathrm{vertices}()$, then $P_1.\mathrm{first}() = P_2.\mathrm{last}()$ and $P_1.\mathrm{vertices}() \cap P_2.\mathrm{vertices}() \subseteq \{P_1.\mathrm{first}(), P_1.\mathrm{last}()\}$. Then $P_1.\mathrm{append}(P_2)$ is path-like.

(18) Let G be a graph and P_1, P_2 be paths of G. Suppose $P_1.\mathrm{last}() = P_2.\mathrm{first}()$ and P_1 is open and P_2 is open and $P_1.\mathrm{vertices}() \cap P_2.\mathrm{vertices}() = \{P_1.\mathrm{last}()\}$. Then $P_1.\mathrm{append}(P_2)$ is open and path-like.

(19) Let G be a graph and P_1, P_2 be paths of G. Suppose $P_1.\mathrm{last}() = P_2.\mathrm{first}()$ and $P_2.\mathrm{last}() = P_1.\mathrm{first}()$ and P_1 is open and P_2 is open and $P_1.\mathrm{edges}()$

misses P_2.edges() and P_1.vertices() $\cap$ P_2.vertices() $= \{P_1.\mathrm{last}(), P_1.\mathrm{first}()\}$. Then P_1.append(P_2) is cycle-like.

(20) Let G be a simple graph, W_1, W_2 be walks of G, and k be an odd natural number. Suppose $k \leq \mathrm{len}\, W_1$ and $k \leq \mathrm{len}\, W_2$ and for every odd natural number j such that $j \leq k$ holds $W_1(j) = W_2(j)$. Let j be a natural number. If $1 \leq j \leq k$, then $W_1(j) = W_2(j)$.

(21) For every graph G and for all walks W_1, W_2 of G such that W_1.first() $=$ W_2.first() holds len maxPrefix(W_1, W_2) is odd.

(22) For every graph G and for all walks W_1, W_2 of G such that W_1.first() $=$ W_2.first() and $W_1 \not\preceq W_2$ holds len maxPrefix(W_1, W_2) $+ 2 \leq \mathrm{len}\, W_1$.

(23) For every non-multi graph G and for all walks W_1, W_2 of G such that W_1.first() $=$ W_2.first() and $W_1 \not\preceq W_2$ and $W_2 \not\preceq W_1$ holds W_1(len maxPrefix(W_1, W_2) $+ 2$) $\neq$ W_2(len maxPrefix(W_1, W_2) $+ 2$).

3. Trees

A tree is a tree-like graph. Let G be a graph. A subtree of G is a tree-like subgraph of G.

Let T be a tree. Observe that every walk of T which is trail-like is also path-like.

One can prove the following proposition

(24) For every tree T and for every path P of T such that P is non trivial holds P is open.

Let T be a tree. Note that every path of T which is non trivial is also open.

The following propositions are true:

(25) Let T be a tree, P be a path of T, and i, j be odd natural numbers. If $i < j \leq \mathrm{len}\, P$, then $P(i) \neq P(j)$.

(26) Let T be a tree, a, b be vertices of T, and P_1, P_2 be paths of T. If P_1 is walk from a to b and P_2 is walk from a to b, then $P_1 = P_2$.

Let T be a tree and let a, b be vertices of T. The functor T.pathBetween(a, b) yields a path of T and is defined as follows:

(Def. 2) T.pathBetween(a, b) is walk from a to b.

One can prove the following propositions:

(27) For every tree T and for all vertices a, b of T holds (T.pathBetween(a, b)).first() $= a$ and (T.pathBetween(a, b)).last() $= b$.

(28) For every tree T and for all vertices a, b of T holds a, b $\in$ (T.pathBetween(a, b)).vertices().

Let T be a tree and let a be a vertex of T. Observe that T.pathBetween(a, a) is closed.

Let T be a tree and let a be a vertex of T.

One can check that T.pathBetween(a, a) is trivial.

We now state a number of propositions:

(29) For every tree T and for every vertex a of T holds $(T.\mathrm{pathBetween}(a, a)).\mathrm{vertices}() = \{a\}$.

(30) For every tree T and for all vertices a, b of T holds $(T.\mathrm{pathBetween}(a, b)).\mathrm{reverse}() = T.\mathrm{pathBetween}(b, a)$.

(31) For every tree T and for all vertices a, b of T holds $(T.\mathrm{pathBetween}(a, b)).\mathrm{vertices}() = (T.\mathrm{pathBetween}(b, a)).\mathrm{vertices}()$.

(32) Let T be a tree, a, b be vertices of T, t be a subtree of T, and a', b' be vertices of t. If $a = a'$ and $b = b'$, then $T.\mathrm{pathBetween}(a, b) = t.\mathrm{pathBetween}(a', b')$.

(33) Let T be a tree, a, b be vertices of T, and t be a subtree of T. Suppose $a \in$ the vertices of t and $b \in$ the vertices of t. Then $(T.\mathrm{pathBetween}(a, b)).\mathrm{vertices}() \subseteq$ the vertices of t.

(34) Let T be a tree, P be a path of T, a, b be vertices of T, and i, j be odd natural numbers. If $i \leq j \leq \mathrm{len}\, P$ and $P(i) = a$ and $P(j) = b$, then $T.\mathrm{pathBetween}(a, b) = P.\mathrm{cut}(i, j)$.

(35) For every tree T and for all vertices a, b, c of T holds $c \in (T.\mathrm{pathBetween}(a, b)).\mathrm{vertices}()$ iff $T.\mathrm{pathBetween}(a, b) = (T.\mathrm{pathBetween}(a, c)).\mathrm{append}((T.\mathrm{pathBetween}(c, b)))$.

(36) For every tree T and for all vertices a, b, c of T holds $c \in (T.\mathrm{pathBetween}(a, b)).\mathrm{vertices}()$ iff $T.\mathrm{pathBetween}(a, c) \preceq T.\mathrm{pathBetween}(a, b)$.

(37) For every tree T and for all paths P_1, P_2 of T such that $P_1.\mathrm{last}() = P_2.\mathrm{first}()$ and $P_1.\mathrm{vertices}() \cap P_2.\mathrm{vertices}() = \{P_1.\mathrm{last}()\}$ holds $P_1.\mathrm{append}(P_2)$ is path-like.

(38) For every tree T and for all vertices a, b, c of T holds $c \in (T.\mathrm{pathBetween}(a, b)).\mathrm{vertices}()$ iff $(T.\mathrm{pathBetween}(a, c)).\mathrm{vertices}() \cap (T.\mathrm{pathBetween}(c, b)).\mathrm{vertices}() = \{c\}$.

(39) Let T be a tree, a, b, c, d be vertices of T, and P_1, P_2 be paths of T. Suppose $P_1 = T.\mathrm{pathBetween}(a, b)$ and $P_2 = T.\mathrm{pathBetween}(a, c)$ and $P_1 \not\preceq P_2$ and $P_2 \not\preceq P_1$ and $d = P_1(\mathrm{len}\,\mathrm{maxPrefix}(P_1, P_2))$. Then $(T.\mathrm{pathBetween}(d, b)).\mathrm{vertices}() \cap (T.\mathrm{pathBetween}(d, c)).\mathrm{vertices}() = \{d\}$.

Let T be a tree and let a, b, c be vertices of T. The functor middleVertex(a, b, c) yielding a vertex of T is defined as follows:

(Def. 3) $(T.\mathrm{pathBetween}(a, b)).\mathrm{vertices}() \cap (T.\mathrm{pathBetween}(b, c)).\mathrm{vertices}() \cap (T.\mathrm{pathBetween}(c, a)).\mathrm{vertices}() = \{\mathrm{middleVertex}(a, b, c)\}$.

We now state a number of propositions:

(40) For every tree T and for all vertices a, b, c of T holds $\mathrm{middleVertex}(a,b,c) = \mathrm{middleVertex}(a,c,b)$.

(41) For every tree T and for all vertices a, b, c of T holds $\mathrm{middleVertex}(a,b,c) = \mathrm{middleVertex}(b,a,c)$.

(42) For every tree T and for all vertices a, b, c of T holds $\mathrm{middleVertex}(a,b,c) = \mathrm{middleVertex}(b,c,a)$.

(43) For every tree T and for all vertices a, b, c of T holds $\mathrm{middleVertex}(a,b,c) = \mathrm{middleVertex}(c,a,b)$.

(44) For every tree T and for all vertices a, b, c of T holds $\mathrm{middleVertex}(a,b,c) = \mathrm{middleVertex}(c,b,a)$.

(45) For every tree T and for all vertices a, b, c of T such that $c \in (T.\mathrm{pathBetween}(a,b)).\mathrm{vertices}()$ holds $\mathrm{middleVertex}(a,b,c) = c$.

(46) For every tree T and for every vertex a of T holds $\mathrm{middleVertex}(a,a,a) = a$.

(47) For every tree T and for all vertices a, b of T holds $\mathrm{middleVertex}(a,a,b) = a$.

(48) For every tree T and for all vertices a, b of T holds $\mathrm{middleVertex}(a,b,a) = a$.

(49) For every tree T and for all vertices a, b of T holds $\mathrm{middleVertex}(a,b,b) = b$.

(50) Let T be a tree, P_1, P_2 be paths of T, and a, b, c be vertices of T. If $P_1 = T.\mathrm{pathBetween}(a,b)$ and $P_2 = T.\mathrm{pathBetween}(a,c)$ and $b \notin P_2.\mathrm{vertices}()$ and $c \notin P_1.\mathrm{vertices}()$, then $\mathrm{middleVertex}(a,b,c) = P_1(\mathrm{len}\,\mathrm{maxPrefix}(P_1,P_2))$.

(51) Let T be a tree, P_1, P_2, P_3, P_4 be paths of T, and a, b, c be vertices of T. Suppose $P_1 = T.\mathrm{pathBetween}(a,b)$ and $P_2 = T.\mathrm{pathBetween}(a,c)$ and $P_3 = T.\mathrm{pathBetween}(b,a)$ and $P_4 = T.\mathrm{pathBetween}(b,c)$ and $b \notin P_2.\mathrm{vertices}()$ and $c \notin P_1.\mathrm{vertices}()$ and $a \notin P_4.\mathrm{vertices}()$. Then $P_1(\mathrm{len}\,\mathrm{maxPrefix}(P_1,P_2)) = P_3(\mathrm{len}\,\mathrm{maxPrefix}(P_3,P_4))$.

(52) Let T be a tree, a, b, c be vertices of T, and S be a non empty set. Suppose that for every set s such that $s \in S$ holds there exists a subtree t of T such that $s =$ the vertices of t but a, $b \in s$ or a, $c \in s$ or b, $c \in s$. Then $\bigcap S \neq \emptyset$.

4. The Helly Property

Let F be a set. We say that F has Helly property if and only if:

(Def. 4) For every non empty set H such that $H \subseteq F$ and for all sets x, y such that x, $y \in H$ holds x meets y holds $\bigcap H \neq \emptyset$.

One can prove the following proposition

(53) Let T be a tree and X be a finite set such that for every set x such that $x \in X$ there exists a subtree t of T such that $x =$ the vertices of t. Then X has Helly property.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[4] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[5] M. Ch. Golumbic. *Algorithmic Graph Theory and Perfect Graphs.* Academic Press, New York, 1980.

[6] Gilbert Lee. Trees and graph components. *Formalized Mathematics*, 13(**2**):271–277, 2005.

[7] Gilbert Lee. Walks in graphs. *Formalized Mathematics*, 13(**2**):253–269, 2005.

[8] Gilbert Lee and Piotr Rudnicki. Alternative graph structures. *Formalized Mathematics*, 13(**2**):235–252, 2005.

[9] Yatsuka Nakamura and Piotr Rudnicki. Vertex sequences induced by chains. *Formalized Mathematics*, 5(**3**):297–304, 1996.

[10] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[11] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[12] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received January 10, 2008

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 97–101, 2008

Heron's Formula and Ptolemy's Theorem

Marco Riccardi
Casella Postale 49
54038 Montignoso, Italy

Summary. The goal of this article is to formalize some theorems that are in the [17] on the web. These are elementary theorems included in every handbook of Euclidean geometry and trigonometry: the law of cosines, the Heron's formula, the isosceles triangle theorem, the intersecting chords theorem and the Ptolemy's theorem.

MML identifier: `EUCLID_6`, version: `7.8.09 4.97.1001`

The terminology and notation used here are introduced in the following articles: [5], [16], [2], [1], [13], [14], [15], [18], [12], [6], [8], [7], [11], [4], [9], [10], and [3].

1. Law of Cosines and Meister-Gauss Formula

We adopt the following rules: p_1, p_2, p_3, p_4, p_5, p_6, p, p_7 denote points of $\mathcal{E}^2_{\rm T}$ and a, b, c, r, s denote real numbers.

Next we state four propositions:

(1) If $\sin\measuredangle(p_1,p_2,p_3) = \sin\measuredangle(p_4,p_5,p_6)$ and $\cos\measuredangle(p_1,p_2,p_3) = \cos\measuredangle(p_4,p_5,p_6)$, then $\measuredangle(p_1,p_2,p_3) = \measuredangle(p_4,p_5,p_6)$.

(2) $\sin\measuredangle(p_1,p_2,p_3) = -\sin\measuredangle(p_3,p_2,p_1)$.

(3) $\cos\measuredangle(p_1,p_2,p_3) = \cos\measuredangle(p_3,p_2,p_1)$.

(4) $\measuredangle(p_1,p_4,p_2)+\measuredangle(p_2,p_4,p_3) = \measuredangle(p_1,p_4,p_3)$ or $\measuredangle(p_1,p_4,p_2)+\measuredangle(p_2,p_4,p_3) = \measuredangle(p_1,p_4,p_3) + 2\cdot\pi$.

Let us consider p_1, p_2, p_3. The area of $\triangle(p_1,p_2,p_3)$ yields a real number and is defined by:

(Def. 1) The area of $\triangle(p_1,p_2,p_3) = \frac{1}{2}\cdot(((p_1)_{\mathbf{1}}\cdot(p_2)_{\mathbf{2}} - (p_2)_{\mathbf{1}}\cdot(p_1)_{\mathbf{2}}) + ((p_2)_{\mathbf{1}}\cdot(p_3)_{\mathbf{2}} - (p_3)_{\mathbf{1}}\cdot(p_2)_{\mathbf{2}}) + ((p_3)_{\mathbf{1}}\cdot(p_1)_{\mathbf{2}} - (p_1)_{\mathbf{1}}\cdot(p_3)_{\mathbf{2}}))$.

Let us consider p_1, p_2, p_3. The perimeter of $\triangle(p_1, p_2, p_3)$ yields a real number and is defined by:

(Def. 2) The perimeter of $\triangle(p_1, p_2, p_3) = |p_2 - p_1| + |p_3 - p_2| + |p_1 - p_3|$.

One can prove the following three propositions:

(5) The area of $\triangle(p_1, p_2, p_3) = \frac{|p_1-p_2| \cdot |p_3-p_2| \cdot \sin \measuredangle(p_3,p_2,p_1)}{2}$.

(6) If $p_2 \neq p_1$, then $|p_3 - p_2| \cdot \sin \measuredangle(p_3, p_2, p_1) = |p_3 - p_1| \cdot \sin \measuredangle(p_2, p_1, p_3)$.

(7) $(|p_3 - p_1|)^{\mathbf{2}} = ((|p_1 - p_2|)^{\mathbf{2}} + (|p_3 - p_2|)^{\mathbf{2}}) - 2 \cdot (|p_1 - p_2|) \cdot (|p_3 - p_2|) \cdot \cos \measuredangle(p_1, p_2, p_3)$.

2. Some Elementary Facts about Euclidean geometry

Next we state a number of propositions:

(8) If $p \in \mathcal{L}(p_1, p_2)$ and $p \neq p_1$ and $p \neq p_2$, then $\measuredangle(p_1, p, p_2) = \pi$.

(9) If $p \in \mathcal{L}(p_2, p_3)$ and $p \neq p_2$, then $\measuredangle(p_3, p_2, p_1) = \measuredangle(p, p_2, p_1)$.

(10) If $p \in \mathcal{L}(p_2, p_3)$ and $p \neq p_2$, then $\measuredangle(p_1, p_2, p_3) = \measuredangle(p_1, p_2, p)$.

(11) If $\measuredangle(p_1, p, p_2) = \pi$, then $p \in \mathcal{L}(p_1, p_2)$.

(12) If $p \in \mathcal{L}(p_1, p_3)$ and $p \in \mathcal{L}(p_1, p_4)$ and $p_3 \neq p_4$ and $p \neq p_1$, then $p_3 \in \mathcal{L}(p_1, p_4)$ or $p_4 \in \mathcal{L}(p_1, p_3)$.

(13) If $p \in \mathcal{L}(p_1, p_3)$ and $p \neq p_1$ and $p \neq p_3$, then $\measuredangle(p_1, p, p_2) + \measuredangle(p_2, p, p_3) = \pi$ or $\measuredangle(p_1, p, p_2) + \measuredangle(p_2, p, p_3) = 3 \cdot \pi$.

(14) If $p \in \mathcal{L}(p_1, p_2)$ and $p \neq p_1$ and $p \neq p_2$ and $\measuredangle(p_3, p, p_1) = \frac{\pi}{2}$ or $\measuredangle(p_3, p, p_1) = \frac{3}{2} \cdot \pi$, then $\measuredangle(p_1, p, p_3) = \measuredangle(p_3, p, p_2)$.

(15) If $p \in \mathcal{L}(p_1, p_3)$ and $p \in \mathcal{L}(p_2, p_4)$ and $p \neq p_1$ and $p \neq p_2$ and $p \neq p_3$ and $p \neq p_4$, then $\measuredangle(p_1, p, p_2) = \measuredangle(p_3, p, p_4)$.

(16) If $|p_3 - p_1| = |p_2 - p_3|$ and $p_1 \neq p_2$, then $\measuredangle(p_3, p_1, p_2) = \measuredangle(p_1, p_2, p_3)$.

(17) For all p_1, p_2, p_3, p such that $p \in \mathcal{L}(p_1, p_2)$ and $p \neq p_2$ holds $|(p_3 - p, p_2 - p_1)| = 0$ iff $|(p_3 - p, p_2 - p)| = 0$.

(18) If $|p_1 - p_3| = |p_2 - p_3|$ and $p \in \mathcal{L}(p_1, p_2)$ and $p \neq p_3$ and $p \neq p_1$ and $\measuredangle(p_3, p, p_1) = \frac{\pi}{2}$ or $\measuredangle(p_3, p, p_1) = \frac{3}{2} \cdot \pi$, then $\measuredangle(p_1, p_3, p) = \measuredangle(p, p_3, p_2)$.

(19) Let given p_1, p_2, p_3, p such that $|p_1 - p_3| = |p_2 - p_3|$ and $p \in \mathcal{L}(p_1, p_2)$ and $p \neq p_3$. Then

(i) if $\measuredangle(p_1, p_3, p) = \measuredangle(p, p_3, p_2)$, then $|p_1 - p| = |p - p_2|$,

(ii) if $|p_1 - p| = |p - p_2|$, then $|(p_3 - p, p_2 - p_1)| = 0$, and

(iii) if $|(p_3 - p, p_2 - p_1)| = 0$, then $\measuredangle(p_1, p_3, p) = \measuredangle(p, p_3, p_2)$.

Let us consider p_1, p_2, p_3. We say that p_1, p_2 and p_3 are collinear if and only if:

(Def. 3) $p_1 \in \mathcal{L}(p_2, p_3)$ or $p_2 \in \mathcal{L}(p_3, p_1)$ or $p_3 \in \mathcal{L}(p_1, p_2)$.

Let us consider p_1, p_2, p_3. We introduce p_1, p_2, p_3 form a triangle as an antonym of p_1, p_2 and p_3 are collinear.

The following propositions are true:

(20) p_1, p_2, p_3 form a triangle iff p_1, p_2, p_3 are mutually different and $\measuredangle(p_1,p_2,p_3) \neq \pi$ and $\measuredangle(p_2,p_3,p_1) \neq \pi$ and $\measuredangle(p_3,p_1,p_2) \neq \pi$.

(21) Suppose p_1, p_2, p_3 form a triangle and p_4, p_5, p_6 form a triangle and $\measuredangle(p_1,p_2,p_3) = \measuredangle(p_4,p_5,p_6)$ and $\measuredangle(p_3,p_1,p_2) = \measuredangle(p_6,p_4,p_5)$. Then $|p_3 - p_2| \cdot |p_4 - p_6| = |p_1 - p_3| \cdot |p_6 - p_5|$ and $|p_3 - p_2| \cdot |p_5 - p_4| = |p_2 - p_1| \cdot |p_6 - p_5|$ and $|p_1 - p_3| \cdot |p_5 - p_4| = |p_2 - p_1| \cdot |p_4 - p_6|$.

(22) Suppose p_1, p_2, p_3 form a triangle and p_4, p_5, p_6 form a triangle and $\measuredangle(p_1,p_2,p_3) = \measuredangle(p_4,p_5,p_6)$ and $\measuredangle(p_3,p_1,p_2) = \measuredangle(p_5,p_6,p_4)$. Then $|p_2 - p_3| \cdot |p_4 - p_6| = |p_3 - p_1| \cdot |p_5 - p_4|$ and $|p_2 - p_3| \cdot |p_6 - p_5| = |p_1 - p_2| \cdot |p_5 - p_4|$ and $|p_3 - p_1| \cdot |p_6 - p_5| = |p_1 - p_2| \cdot |p_4 - p_6|$.

(23) If p_1, p_2, p_3 are mutually different and $\measuredangle(p_1,p_2,p_3) \leq \pi$, then $\measuredangle(p_2,p_3,p_1) \leq \pi$ and $\measuredangle(p_3,p_1,p_2) \leq \pi$.

(24) If p_1, p_2, p_3 are mutually different and $\measuredangle(p_1,p_2,p_3) > \pi$, then $\measuredangle(p_2,p_3,p_1) > \pi$ and $\measuredangle(p_3,p_1,p_2) > \pi$.

(25) If $p \in \mathcal{L}(p_1,p_2)$ and p_1, p_2, p_3 form a triangle and $\measuredangle(p_1,p_3,p_2) = \measuredangle(p,p_3,p_2)$, then $p = p_1$.

(26) If $p \in \mathcal{L}(p_1,p_2)$ and $p_3 \notin \mathcal{L}(p_1,p_2)$ and $\measuredangle(p_1,p_3,p_2) \leq \pi$, then $\measuredangle(p,p_3,p_2) \leq \measuredangle(p_1,p_3,p_2)$.

(27) If $p \in \mathcal{L}(p_1,p_2)$ and $p_3 \notin \mathcal{L}(p_1,p_2)$ and $\measuredangle(p_1,p_3,p_2) > \pi$ and $p \neq p_2$, then $\measuredangle(p,p_3,p_2) \geq \measuredangle(p_1,p_3,p_2)$.

(28) If $p \in \mathcal{L}(p_1,p_2)$ and $p_3 \notin \mathcal{L}(p_1,p_2)$, then there exists p_4 such that $p_4 \in \mathcal{L}(p_1,p_2)$ and $\measuredangle(p_1,p_3,p_4) = \measuredangle(p,p_3,p_2)$.

(29) If $p_1 \in \mathrm{InsideOfCircle}(a,b,r)$ and $p_2 \in \mathrm{OutsideOfCircle}(a,b,r)$, then there exists p such that $p \in \mathcal{L}(p_1,p_2) \cap \mathrm{Circle}(a,b,r)$.

(30) If p_1, p_3, $p_4 \in \mathrm{Circle}(a,b,r)$ and $p \in \mathcal{L}(p_1,p_3)$ and $p \in \mathcal{L}(p_1,p_4)$ and $p_3 \neq p_4$, then $p = p_1$.

(31) If p_1, p_2, $p \in \mathrm{Circle}(a,b,r)$ and $p_7 = [a,b]$ and $p_7 \in \mathcal{L}(p,p_2)$ and $p_1 \neq p$, then $2 \cdot \measuredangle(p_1,p,p_2) = \measuredangle(p_1,p_7,p_2)$ or $2 \cdot (\measuredangle(p_1,p,p_2) - \pi) = \measuredangle(p_1,p_7,p_2)$.

(32) If $p_1 \in \mathrm{Circle}(a,b,r)$ and $r > 0$, then there exists p_2 such that $p_1 \neq p_2$ and $p_2 \in \mathrm{Circle}(a,b,r)$ and $[a,b] \in \mathcal{L}(p_1,p_2)$.

(33) If p_1, p_2, $p \in \mathrm{Circle}(a,b,r)$ and $p_7 = [a,b]$ and $p_1 \neq p$ and $p_2 \neq p$, then $2 \cdot \measuredangle(p_1,p,p_2) = \measuredangle(p_1,p_7,p_2)$ or $2 \cdot (\measuredangle(p_1,p,p_2) - \pi) = \measuredangle(p_1,p_7,p_2)$.

(34) Suppose p_1, p_2, p_3, $p_4 \in \mathrm{Circle}(a,b,r)$ and $p_1 \neq p_3$ and $p_1 \neq p_4$ and $p_2 \neq p_3$ and $p_2 \neq p_4$. Then $\measuredangle(p_1,p_3,p_2) = \measuredangle(p_1,p_4,p_2)$ or $\measuredangle(p_1,p_3,p_2) = \measuredangle(p_1,p_4,p_2) - \pi$ or $\measuredangle(p_1,p_3,p_2) = \measuredangle(p_1,p_4,p_2) + \pi$.

(35) If p_1, p_2, $p_3 \in \mathrm{Circle}(a,b,r)$ and $p_1 \neq p_2 \neq p_3$, then $\measuredangle(p_1,p_2,p_3) \neq \pi$.

(36) Suppose $p_1, p_2, p_3, p_4 \in \mathrm{Circle}(a, b, r)$ and $p \in \mathcal{L}(p_1, p_3)$ and $p \in \mathcal{L}(p_2, p_4)$ and p_1, p_2, p_3, p_4 are mutually different. Then $\measuredangle(p_1, p_4, p_2) = \measuredangle(p_1, p_3, p_2)$.

(37) If p_1, p_2, $p_3 \in \mathrm{Circle}(a, b, r)$ and $\measuredangle(p_1, p_2, p_3) = 0$ and $p_1 \neq p_2 \neq p_3$, then $p_1 = p_3$.

(38) If p_1, p_2, p_3, $p_4 \in \mathrm{Circle}(a, b, r)$ and $p \in \mathcal{L}(p_1, p_3)$ and $p \in \mathcal{L}(p_2, p_4)$, then $|p_1 - p| \cdot |p - p_3| = |p_2 - p| \cdot |p - p_4|$.

3. Heron's Formula and Ptolemy's Theorem

One can prove the following propositions:

(39) Suppose $a = |p_2 - p_1|$ and $b = |p_3 - p_2|$ and $c = |p_1 - p_3|$ and $s = \frac{1}{2} \cdot$ the perimeter of $\triangle(p_1, p_2, p_3)$. Then |the area of $\triangle(p_1, p_2, p_3)| = \sqrt{s \cdot (s - a) \cdot (s - b) \cdot (s - c)}$.

(40) If p_1, p_2, p_3, $p_4 \in \mathrm{Circle}(a, b, r)$ and $p \in \mathcal{L}(p_1, p_3)$ and $p \in \mathcal{L}(p_2, p_4)$, then $|p_3 - p_1| \cdot |p_4 - p_2| = |p_2 - p_1| \cdot |p_4 - p_3| + |p_3 - p_2| \cdot |p_4 - p_1|$.

4. Appendix

In the sequel c_1, c_2, c_3 denote elements of $\mathbb{C}$.

One can prove the following propositions:

(41) $(p_1 - p_2)_{\mathbf{1}} = (p_1)_{\mathbf{1}} - (p_2)_{\mathbf{1}}$ and $(p_1 - p_2)_{\mathbf{2}} = (p_1)_{\mathbf{2}} - (p_2)_{\mathbf{2}}$.

(42) $|p_1 - p_2| = 0$ iff $p_1 = p_2$.

(43) $|p_1 - p_2| = |p_2 - p_1|$.

(44) $\measuredangle(p_1, p_2, p_3) \neq 2 \cdot \measuredangle(p_4, p_5, p_6) + 2 \cdot \pi$.

(45) $\measuredangle(p_1, p_2, p_3) \neq 2 \cdot \measuredangle(p_4, p_5, p_6) + 4 \cdot \pi$.

(46) $\measuredangle(p_1, p_2, p_3) \neq 2 \cdot \measuredangle(p_4, p_5, p_6) - 4 \cdot \pi$.

(47) $\measuredangle(p_1, p_2, p_3) \neq 2 \cdot \measuredangle(p_4, p_5, p_6) - 6 \cdot \pi$.

(48) $\measuredangle(p_1, p_2, p_3) = \measuredangle((\mathrm{euc2cpx}(p_1 - p_2)), (\mathrm{euc2cpx}(p_3 - p_2)))$.

(49) $\measuredangle(c_1, c_2) + \measuredangle(c_2, c_3) = \measuredangle(c_1, c_3)$ or $\measuredangle(c_1, c_2) + \measuredangle(c_2, c_3) = \measuredangle(c_1, c_3) + 2 \cdot \pi$.

(50) Suppose $c_1 = \mathrm{euc2cpx}(p_1 - p_2)$ and $c_2 = \mathrm{euc2cpx}(p_3 - p_2)$. Then $\Re((c_1|c_2)) = ((p_1)_{\mathbf{1}} - (p_2)_{\mathbf{1}}) \cdot ((p_3)_{\mathbf{1}} - (p_2)_{\mathbf{1}}) + ((p_1)_{\mathbf{2}} - (p_2)_{\mathbf{2}}) \cdot ((p_3)_{\mathbf{2}} - (p_2)_{\mathbf{2}})$ and $\Im((c_1|c_2)) = -((p_1)_{\mathbf{1}} - (p_2)_{\mathbf{1}}) \cdot ((p_3)_{\mathbf{2}} - (p_2)_{\mathbf{2}}) + ((p_1)_{\mathbf{2}} - (p_2)_{\mathbf{2}}) \cdot ((p_3)_{\mathbf{1}} - (p_2)_{\mathbf{1}})$ and $|c_1| = \sqrt{((p_1)_{\mathbf{1}} - (p_2)_{\mathbf{1}})^{\mathbf{2}} + ((p_1)_{\mathbf{2}} - (p_2)_{\mathbf{2}})^{\mathbf{2}}}$ and $|p_1 - p_2| = |c_1|$.

(51) Let n be an element of $\mathbb{N}$, q_1 be a point of $\mathcal{E}^n_{\mathrm{T}}$, and f be a function from $\mathcal{E}^n_{\mathrm{T}}$ into $\mathbb{R}^{\mathbf{1}}$. If for every point q of $\mathcal{E}^n_{\mathrm{T}}$ holds $f(q) = |q - q_1|$, then f is continuous.

(52) Let n be an element of $\mathbb{N}$ and q_1 be a point of $\mathcal{E}^n_{\rm T}$. Then there exists a function f from $\mathcal{E}^n_{\rm T}$ into $\mathbb{R}^{\mathbf{1}}$ such that for every point q of $\mathcal{E}^n_{\rm T}$ holds $f(q) = |q - q_1|$ and f is continuous.

References

[1] Kanchun and Yatsuka Nakamura. The inner product of finite sequences and of points of n-dimensional topological space. *Formalized Mathematics*, 11(**2**):179–183, 2003.

[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[3] Leszek Borys. Paracompact and metrizable spaces. *Formalized Mathematics*, 2(**4**):481–485, 1991.

[4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

[5] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[6] Wenpai Chang, Yatsuka Nakamura, and Piotr Rudnicki. Inner products and angles of complex numbers. *Formalized Mathematics*, 11(**3**):275–280, 2003.

[7] Agata Darmochwał and Yatsuka Nakamura. Metric spaces as topological spaces – fundamental concepts. *Formalized Mathematics*, 2(**4**):605–608, 1991.

[8] Agata Darmochwał and Yatsuka Nakamura. The topological space $\mathcal{E}^2_{\rm T}$. Arcs, line segments and special polygonal arcs. *Formalized Mathematics*, 2(**5**):617–621, 1991.

[9] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[10] Stanisława Kanas, Adam Lecko, and Mariusz Startek. Metric spaces. *Formalized Mathematics*, 1(**3**):607–610, 1990.

[11] Akihiro Kubo and Yatsuka Nakamura. Angle and triangle in Euclidian topological space. *Formalized Mathematics*, 11(**3**):281–287, 2003.

[12] Yatsuka Nakamura. General Fashoda meet theorem for unit circle and square. *Formalized Mathematics*, 11(**3**):213–224, 2003.

[13] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.

[14] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[15] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[16] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[17] Freek Wiedijk. Formalizing 100 theorems. `http://www.cs.ru.nl/ freek/100/`.

[18] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

Received January 10, 2008

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 103–107, 2008

Uniqueness of Factoring an Integer and Multiplicative Group $\mathbb{Z}/p\mathbb{Z}^*$

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In the [20], it had been proven that the Integers modulo p, in this article we shall refer as $\mathbb{Z}/p\mathbb{Z}$, constitutes a field if and only if p is a prime. Then the prime modulo $\mathbb{Z}/p\mathbb{Z}$ is an additive cyclic group and $\mathbb{Z}/p\mathbb{Z}^* = \mathbb{Z}/p\mathbb{Z}\setminus\{0\}$ is a multiplicative cyclic group, too. The former has been proven in the [23]. However, the latter had not been proven yet. In this article, first, we prove a theorem concerning the LCM to prove the existence of primitive elements of $\mathbb{Z}/p^*$. Moreover we prove the uniqueness of factoring an integer. Next we define the multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$ and prove it is cyclic.

MML identifier: `INT_7`, version: `7.8.10 4.99.1005`

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

1. Uniqueness of Factoring an Integer

In this paper x, X denote sets.

Next we state four propositions:

(1) For every many sorted set p indexed by X such that $\operatorname{support} p = \{x\}$ holds $p = (X \longmapsto 0) +\cdot (x, p(x))$.

(2) Let X be a set and p, q, r be real-valued many sorted sets indexed by X. If $\operatorname{support} p \cap \operatorname{support} q = \emptyset$ and $\operatorname{support} p \cup \operatorname{support} q = \operatorname{support} r$ and $p \restriction \operatorname{support} p = r \restriction \operatorname{support} p$ and $q \restriction \operatorname{support} q = r \restriction \operatorname{support} q$, then $p + q = r$.

ISSN 1426–2630(p), 1898-9934(e)

(3) For every set X and for all many sorted sets p, q indexed by X such that $p\restriction \operatorname{support} p = q\restriction \operatorname{support} q$ holds $p = q$.

(4) For every set X and for all bags p, q of X such that $\operatorname{support} p = \emptyset$ and $\operatorname{support} q = \emptyset$ holds $p = q$.

Let p be a bag of Prime. We say that p is prime-factorization-like if and only if:

(Def. 1) For every prime number x such that $x \in \operatorname{support} p$ there exists a natural number n such that $0 < n$ and $p(x) = x^n$.

Let n be a non empty natural number. Note that $\mathrm{PPF}(n)$ is prime-factorization-like.

Next we state a number of propositions:

(5) For all prime numbers p, q and for all natural numbers n, m such that $p \mid m \cdot q^n$ and $p \neq q$ holds $p \mid m$.

(6) Let f be a finite sequence of elements of $\mathbb{N}$, b be a bag of Prime, and a be a prime number. Suppose b is prime-factorization-like and $\prod b \neq 1$ and $a \mid \prod b$ and $\prod b = \prod f$ and $f = b \cdot \mathrm{CFS}(\operatorname{support} b)$. Then $a \in \operatorname{support} b$.

(7) For all bags p, q of Prime such that $\operatorname{support} p \subseteq \operatorname{support} q$ and $p\restriction \operatorname{support} p = q\restriction \operatorname{support} p$ holds $\prod p \mid \prod q$.

(8) Let p be a bag of Prime and x be a prime number. If p is prime-factorization-like, then $x \mid \prod p$ iff $x \in \operatorname{support} p$.

(9) For all non empty natural numbers n, m, k such that $k = \operatorname{lcm}(n, m)$ holds $\operatorname{support} \mathrm{PPF}(k) = \operatorname{support} \mathrm{PPF}(n) \cup \operatorname{support} \mathrm{PPF}(m)$.

(10) For every set X and for all bags b_1, b_2 of X holds $\operatorname{support} \min(b_1, b_2) = \operatorname{support} b_1 \cap \operatorname{support} b_2$.

(11) For all non empty natural numbers n, m, k such that $k = n \gcd m$ holds $\operatorname{support} \mathrm{PPF}(k) = \operatorname{support} \mathrm{PPF}(n) \cap \operatorname{support} \mathrm{PPF}(m)$.

(12) Let p, q be bags of Prime. Suppose p is prime-factorization-like and q is prime-factorization-like and $\operatorname{support} p$ misses $\operatorname{support} q$. Then $\prod p$ and $\prod q$ are relative prime.

(13) For every bag p of Prime such that p is prime-factorization-like holds $\prod p \neq 0$.

(14) For every bag p of Prime such that p is prime-factorization-like holds $\prod p = 1$ iff $\operatorname{support} p = \emptyset$.

(15) Let p, q be bags of Prime. Suppose p is prime-factorization-like and q is prime-factorization-like and $\prod p = \prod q$. Then $p = q$.

(16) Let p be a bag of Prime and n be a non empty natural number. If p is prime-factorization-like and $n = \prod p$, then $\mathrm{PPF}(n) = p$.

(17) Let n, m be elements of $\mathbb{N}$. Suppose $1 \leq n$ and $1 \leq m$. Then there exist elements m_0, n_0 of $\mathbb{N}$ such that $\operatorname{lcm}(n, m) = n_0 \cdot m_0$ and $n_0 \gcd m_0 = 1$

and $n_0 \mid n$ and $m_0 \mid m$ and $n_0 \neq 0$ and $m_0 \neq 0$.

2. Multiplicative Group $\mathbb{Z}/p\mathbb{Z}^*$

Let n be a natural number. Let us assume that $1 < n$. The functor $\mathbb{Z}_n^*$ yields a non empty finite subset of $\mathbb{N}$ and is defined by:

(Def. 2) $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$.

We now state the proposition

(18) For every natural number n such that $1 < n$ holds $\overline{\overline{\mathbb{Z}_n^*}} = n - 1$.

Let n be a prime number. The functor $\cdot_{\mathbb{Z}_n^*}$ yielding a binary operation on $\mathbb{Z}_n^*$ is defined by:

(Def. 3) $\cdot_{\mathbb{Z}_n^*} = \cdot_{\mathbb{Z}_n} \restriction \mathbb{Z}_n^*$.

One can prove the following proposition

(19) For every prime number p holds $\langle \mathbb{Z}_p^*, \cdot_{\mathbb{Z}_p^*} \rangle$ is associative, commutative, and group-like.

Let p be a prime number. The functor $\mathbb{Z}/p\mathbb{Z}^*$ yielding a commutative group is defined by:

(Def. 4) $\mathbb{Z}/p\mathbb{Z}^* = \langle \mathbb{Z}_p^*, \cdot_{\mathbb{Z}_p^*} \rangle$.

The following three propositions are true:

(20) Let p be a prime number, x, y be elements of $\mathbb{Z}/p\mathbb{Z}^*$, and x_1, y_1 be elements of $\mathbb{Z}_p^{\mathrm{R}}$. If $x = x_1$ and $y = y_1$, then $x \cdot y = x_1 \cdot y_1$.

(21) For every prime number p holds $\mathbf{1}_{\mathbb{Z}/p\mathbb{Z}^*} = 1$ and $\mathbf{1}_{\mathbb{Z}/p\mathbb{Z}^*} = 1_{\mathbb{Z}_p^{\mathrm{R}}}$.

(22) For every prime number p and for every element x of $\mathbb{Z}/p\mathbb{Z}^*$ and for every element x_1 of $\mathbb{Z}_p^{\mathrm{R}}$ such that $x = x_1$ holds $x^{-1} = {x_1}^{-1}$.

Let p be a prime number. One can verify that $\mathbb{Z}/p\mathbb{Z}^*$ is finite.

We now state several propositions:

(23) For every prime number p holds $\mathrm{ord}(\mathbb{Z}/p\mathbb{Z}^*) = p - 1$.

(24) Let G be a group, a be an element of G, and i be an integer. Suppose a is not of order 0. Then there exist elements n, k of $\mathbb{N}$ such that $a^i = a^n$ and $n = k \cdot \mathrm{ord}(a) + i$.

(25) Let G be a commutative group, a, b be elements of G, and n, m be natural numbers. If G is finite and $\mathrm{ord}(a) = n$ and $\mathrm{ord}(b) = m$ and $n \gcd m = 1$, then $\mathrm{ord}(a \cdot b) = n \cdot m$.

(26) For every non empty zero structure L and for every polynomial p of L such that $0 \leq \deg p$ holds p is non-zero.

(27) For every field L and for every polynomial f of L such that $0 \leq \deg f$ holds $\mathrm{Roots}\, f$ is a finite set and $\overline{\overline{\mathrm{Roots}\, f}} \leq \deg f$.

(28) Let p be a prime number, z be an element of $\mathbb{Z}/p\mathbb{Z}^*$, and y be an element of $\mathbb{Z}_p^{\mathrm{R}}$. If $z = y$, then for every element n of $\mathbb{N}$ holds $\mathrm{power}_{\mathbb{Z}/p\mathbb{Z}^*}(z, n) = \mathrm{power}_{\mathbb{Z}_p^{\mathrm{R}}}(y, n)$.

(29) Let p be a prime number, a, b be elements of $\mathbb{Z}/p\mathbb{Z}^*$, and n be a natural number. If $0 < n$ and $\mathrm{ord}(a) = n$ and $b^n = 1$, then b is an element of $\mathrm{gr}(\{a\})$.

(30) Let G be a group, z be an element of G, and d, l be elements of $\mathbb{N}$. If G is finite and $\mathrm{ord}(z) = d \cdot l$, then $\mathrm{ord}(z^d) = l$.

(31) For every prime number p holds $\mathbb{Z}/p\mathbb{Z}^*$ is a cyclic group.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[5] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

[6] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

[7] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[9] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[10] Krzysztof Hryniewiecki. Recursive definitions. *Formalized Mathematics*, 1(**2**):321–328, 1990.

[11] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

[12] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.

[13] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[14] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[15] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[16] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.

[17] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.

[18] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**):49–58, 2004.

[19] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.

[20] Christoph Schwarzweller. The ring of integers, euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.

[21] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Schur's theorem on the stability of networks. *Formalized Mathematics*, 14(**4**):135–142, 2006.

[22] Christoph Schwarzweller and Andrzej Trybulec. The evaluation of multivariate polynomials. *Formalized Mathematics*, 9(**2**):331–338, 2001.

[23] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.

[24] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[25] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[26] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[27] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[28] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[29] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[30] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received January 31, 2008

FORMALIZED MATHEMATICS
Vol. **16**, No. **2**, Pages 109–114, **2008**

Ideals of BCI-algebras and their Properties

Chenglong Wu
Qingdao University of Science and Technology
China

Yuzhong Ding
Qingdao University of Science and Technology
China

Summary. In this article three classes of ideals are discussed: associative ideals, commutative ideals, implicative ideals and positive implicative ideals, and their elementary properties. Some of their properties and the relationships between them have not been proven yet, and will be completed in the following article.

MML identifier: `BCIIDEAL`, version: `7.8.10 4.99.1005`

The papers [4], [1], [2], and [3] provide the terminology and notation for this paper.

1. Preliminaries

For simplicity, we use the following convention: X denotes a BCI-algebra, X_1 denotes a non empty subset of X, A, I denote ideals of X, x, y, z denote elements of X, and a denotes an element of A.

The following four propositions are true:

(1) For all elements x, y, z, u of X such that $x \leq y$ holds $u \backslash (z \backslash x) \leq u \backslash (z \backslash y)$.

(2) For all elements x, y, z, u of X holds $x \setminus (y \setminus z) \setminus (x \setminus (y \setminus u)) \leq z \setminus u$.

(3) For all elements x, y, z, u, v of X holds $x \setminus (y \setminus (z \setminus u)) \setminus (x \setminus (y \setminus (z \setminus v))) \leq v \setminus u$.

(4) For all elements x, y of X holds $0_X \setminus (x \setminus y) \setminus (y \setminus x) = 0_X$.

Let us consider X and let a be an element of X. The initial section of a is defined by:

(Def. 1) The initial section of $a = \{x \in X \colon x \leq a\}$.

ISSN 1426–2630(p), 1898-9934(e)

The following propositions are true:

(5) If $x \leq a$, then $x \in A$.

(6) For all elements x, a, b of AtomSet X such that x is an element of BranchV b holds $a \setminus x = a \setminus b$.

(7) For every element a of X and for all elements x, b of AtomSet X such that x is an element of BranchV b holds $a \setminus x = a \setminus b$.

(8) The initial section of $a \subseteq A$.

(9) If AtomSet X is an ideal of X, then for every element x of BCK-part X and for every element a of AtomSet X such that $x \setminus a \in$ AtomSet X holds $x = 0_X$.

(10) If AtomSet X is an ideal of X, then AtomSet X is a closed ideal of X.

Let us consider X, I. We say that I is positive if and only if:

(Def. 2) Every element of I is positive.

Next we state three propositions:

(11) Let X be a BCK-algebra and A, I be ideals of X. Then $A \cap I = \{0_X\}$ if and only if for every element x of A and for every element y of I holds $x \setminus y = x$.

(12) For every associative BCI-algebra X holds every ideal of X is closed.

(13) For every BCI-algebra X and for every ideal A of X such that X is quasi-associative holds A is closed.

2. Definitions of Associative Ideals

Let X be a BCI-algebra and let I_1 be an ideal of X. We say that I_1 is associative if and only if:

(Def. 3) $0_X \in I_1$ and for all elements x, y, z of X such that $x \setminus (y \setminus z)$, $y \setminus z \in I_1$ holds $x \in I_1$.

Let X be a BCI-algebra. One can verify that there exists an ideal of X which is associative.

Let X be a BCI-algebra. A non empty subset of X is said to be an associative-ideal of X if:

(Def. 4) $0_X \in$ it and for all elements x, y, z of X such that $x \setminus y \setminus z$, $y \setminus z \in$ it holds $x \in$ it.

We now state four propositions:

(14) If X_1 is an associative-ideal of X, then X_1 is an ideal of X.

(15) I is an associative-ideal of X iff for all x, y, z such that $x \setminus y \setminus z \in I$ holds $x \setminus (y \setminus z) \in I$.

(16) If I is an associative-ideal of X, then for every element x of X holds $x \setminus (0_X \setminus x) \in I$.

(17) If for every element x of X holds $x \setminus (0_X \setminus x) \in I$, then I is a closed ideal of X.

Let X be a BCI-algebra. A non empty subset of X is said to be a p-ideal of X if:

(Def. 5) $0_X \in$ it and for all elements x, y, z of X such that $x \setminus z \setminus (y \setminus z)$, $y \in$ it holds $x \in$ it.

We now state several propositions:

(18) If X_1 is a p-ideal of X, then X_1 is an ideal of X.

(19) For all X, I such that I is a p-ideal of X holds BCK-part $X \subseteq I$.

(20) BCK-part X is a p-ideal of X.

(21) I is a p-ideal of X iff for all x, y such that $x \in I$ and $x \leq y$ holds $y \in I$.

(22) I is a p-ideal of X iff for all x, y, z such that $x \setminus z \setminus (y \setminus z) \in I$ holds $x \setminus y \in I$.

3. Definitions of Commutative Ideals

Let X be a BCK-algebra and let I_1 be an ideal of X. We say that I_1 is commutative if and only if:

(Def. 6) For all elements x, y, z of X such that $x \setminus y \setminus z$, $z \in I_1$ holds $x \setminus (y \setminus (y \setminus x)) \in I_1$.

Let X be a BCK-algebra. One can verify that there exists an ideal of X which is commutative.

Next we state two propositions:

(23) For every BCK-algebra X holds BCK-part X is a commutative ideal of X.

(24) Let X be a BCK-algebra. Suppose X is a p-semisimple BCI-algebra. Then $\{0_X\}$ is a commutative ideal of X.

In the sequel X denotes a BCK-algebra.

One can prove the following proposition

(25) BCK-part $X =$ the carrier of X.

In the sequel X denotes a BCI-algebra.

We now state several propositions:

(26) If for every BCI-algebra X and for all elements x, y of X holds $x \setminus y \setminus y = x \setminus y$, then the carrier of $X =$ BCK-part X.

(27) If for every BCI-algebra X and for all elements x, y of X holds $x \setminus (y \setminus x) = x$, then the carrier of $X =$ BCK-part X.

(28) If for every BCI-algebra X and for all elements x, y of X holds $x \setminus (x \setminus y) = y \setminus (y \setminus x)$, then the carrier of $X =$ BCK-part X.

(29) If for every BCI-algebra X and for all elements x, y, z of X holds $(x \setminus y) \setminus y = x \setminus z \setminus (y \setminus z)$, then the carrier of $X =$ BCK-part X.

(30) If for every BCI-algebra X and for all elements x, y of X holds $x \setminus y \setminus (y \setminus x) = x \setminus y$, then the carrier of $X =$ BCK-part X.

(31) If for every BCI-algebra X and for all elements x, y of X holds $x \setminus y \setminus (x \setminus y \setminus (y \setminus x)) = 0_X$, then the carrier of $X =$ BCK-part X.

(32) For every BCK-algebra X holds the carrier of X is a commutative ideal of X.

In the sequel X denotes a BCK-algebra and I denotes an ideal of X.

One can prove the following propositions:

(33) I is a commutative ideal of X iff for all elements x, y of X such that $x \setminus y \in I$ holds $x \setminus (y \setminus (y \setminus x)) \in I$.

(34) Let I, A be ideals of X. Suppose $I \subseteq A$ and I is a commutative ideal of X. Then A is a commutative ideal of X.

(35) Every ideal of X is a commutative ideal of X iff $\{0_X\}$ is a commutative ideal of X.

(36) $\{0_X\}$ is a commutative ideal of X iff X is a commutative BCK-algebra.

(37) X is a commutative BCK-algebra iff every ideal of X is a commutative ideal of X.

(38) $\{0_X\}$ is a commutative ideal of X iff every ideal of X is a commutative ideal of X.

In the sequel I denotes an ideal of X.

One can prove the following propositions:

(39) For all elements x, y of X such that $x \setminus (x \setminus y) \in I$ holds $x \setminus (x \setminus y \setminus (x \setminus y \setminus x))$, $y \setminus (y \setminus x) \setminus x$, $y \setminus (y \setminus x) \setminus (x \setminus y) \in I$.

(40) $\{0_X\}$ is a commutative ideal of X iff for all elements x, y of X holds $x \setminus (x \setminus y) \leq y \setminus (y \setminus x)$.

(41) $\{0_X\}$ is a commutative ideal of X iff for all elements x, y of X holds $x \setminus y = x \setminus (y \setminus (y \setminus x))$.

(42) $\{0_X\}$ is a commutative ideal of X iff for all elements x, y of X holds $x \setminus (x \setminus y) = y \setminus (y \setminus (x \setminus (x \setminus y)))$.

(43) $\{0_X\}$ is a commutative ideal of X iff for all elements x, y of X such that $x \leq y$ holds $x = y \setminus (y \setminus x)$.

(44) Suppose $\{0_X\}$ is a commutative ideal of X. Then

(i) for all elements x, y of X holds $x \setminus y = x$ iff $y \setminus (y \setminus x) = 0_X$,

(ii) for all elements x, y of X such that $x \setminus y = x$ holds $y \setminus x = y$,

(iii) for all elements x, y, a of X such that $y \leq a$ holds $a \setminus x \setminus (a \setminus y) = y \setminus x$,

(iv) for all elements x, y of X holds $x \setminus (y \setminus (y \setminus x)) = x \setminus y$ and $x \setminus y \setminus (x \setminus y \setminus x) = x \setminus y$, and

(v) for all elements x, y, a of X such that $x \leq a$ holds $(a \setminus y) \setminus (a \setminus y \setminus (a \setminus x)) = a \setminus y \setminus (x \setminus y)$.

(45) Every ideal of X is a commutative ideal of X iff for all elements x, y of X holds $x \setminus (x \setminus y) \leq y \setminus (y \setminus x)$.

(46) Every ideal of X is a commutative ideal of X iff for all elements x, y of X holds $x \setminus y = x \setminus (y \setminus (y \setminus x))$.

(47) Every ideal of X is a commutative ideal of X iff for all elements x, y of X holds $x \setminus (x \setminus y) = y \setminus (y \setminus (x \setminus (x \setminus y)))$.

(48) Every ideal of X is a commutative ideal of X iff for all elements x, y of X such that $x \leq y$ holds $x = y \setminus (y \setminus x)$.

(49) Suppose every ideal of X is a commutative ideal of X. Then

(i) for all elements x, y of X holds $x \setminus y = x$ iff $y \setminus (y \setminus x) = 0_X$,

(ii) for all elements x, y of X such that $x \setminus y = x$ holds $y \setminus x = y$,

(iii) for all elements x, y, a of X such that $y \leq a$ holds $a \setminus x \setminus (a \setminus y) = y \setminus x$,

(iv) for all elements x, y of X holds $x \setminus (y \setminus (y \setminus x)) = x \setminus y$ and $x \setminus y \setminus (x \setminus y \setminus x) = x \setminus y$, and

(v) for all elements x, y, a of X such that $x \leq a$ holds $(a \setminus y) \setminus (a \setminus y \setminus (a \setminus x)) = a \setminus y \setminus (x \setminus y)$.

4. Definitions of Implicative Ideals and Positive Implicative Ideals

Let X be a BCK-algebra. A non empty subset of X is said to be an implicative-ideal of X if:

(Def. 7) $0_X \in$ it and for all elements x, y, z of X such that $x \setminus (y \setminus x) \setminus z$, $z \in$ it holds $x \in$ it.

In the sequel X denotes a BCK-algebra and I denotes an ideal of X.

Next we state the proposition

(50) I is an implicative-ideal of X iff for all elements x, y of X such that $x \setminus (y \setminus x) \in I$ holds $x \in I$.

Let X be a BCK-algebra. A non empty subset of X is said to be a positive-implicative-ideal of X if:

(Def. 8) $0_X \in$ it and for all elements x, y, z of X such that $x \setminus y \setminus z$, $y \setminus z \in$ it holds $x \setminus z \in$ it.

We now state several propositions:

(51) I is a positive-implicative-ideal of X if and only if for all elements x, y of X such that $x \setminus y \setminus y \in I$ holds $x \setminus y \in I$.

(52) Suppose that for all elements x, y, z of X such that $x \setminus y \setminus z$, $y \setminus z \in I$ holds $x \setminus z \in I$. Let x, y, z be elements of X. If $x \setminus y \setminus z \in I$, then $x \setminus z \setminus (y \setminus z) \in I$.

(53) Suppose that for all elements x, y, z of X such that $x \setminus y \setminus z \in I$ holds $x \setminus z \setminus (y \setminus z) \in I$. Then I is a positive-implicative-ideal of X.

(54) I is a positive-implicative-ideal of X if and only if for all elements x, y, z of X such that $x \setminus y \setminus z$, $y \setminus z \in I$ holds $x \setminus z \in I$.

(55) I is a positive-implicative-ideal of X if and only if for all elements x, y, z of X such that $x \setminus y \setminus z \in I$ holds $x \setminus z \setminus (y \setminus z) \in I$.

(56) Let I, A be ideals of X. Suppose $I \subseteq A$ and I is a positive-implicative-ideal of X. Then A is a positive-implicative-ideal of X.

(57) Suppose I is an implicative-ideal of X. Then I is a commutative ideal of X and a positive-implicative-ideal of X.

References

[1] Yuzhong Ding. Several classes of BCI-algebras and their properties. *Formalized Mathematics*, 15(**1**):1–9, 2007.

[2] Yuzhong Ding and Zhiyong Pang. Congruences and quotient algebras of BCI-algebras. *Formalized Mathematics*, 15(**4**):175–180, 2007.

[3] Tao Sun, Dahai Hu, and Xiquan Liang. Several classes of BCK-algebras and their properties. *Formalized Mathematics*, 15(**4**):237–242, 2007.

[4] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received March 3, 2008

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 115–122, 2008

Banach Algebra of Bounded Functionals

Yasunari Shidama
Shinshu University
Nagano, Japan

Hikofumi Suzuki
Shinshu University
Nagano, Japan

Noboru Endou
Gifu National College of Technology
Japan

Summary. In this article, we describe some basic properties of the Banach algebra which is constructed from all bounded functionals.

MML identifier: `COSP1`, version: `7.8.10 4.99.1005`

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

1. Some Properties of Rings

Let V be a non empty additive loop structure and let V_1 be a subset of V. We say that V_1 has inverse if and only if:

(Def. 1) For every element v of V such that $v \in V_1$ holds $-v \in V_1$.

Let V be a non empty additive loop structure and let V_1 be a subset of V. We say that V_1 is additively-closed if and only if:

(Def. 2) V_1 is add closed and has inverse.

Let V be a non empty additive loop structure. One can verify that Ω_V is add closed and has inverse.

Let V be a non empty double loop structure. One can verify that every subset of V which is additively-closed is also add closed and has inverse and every subset of V which is add closed and has inverse is also additively-closed.

ISSN 1426–2630(p), 1898-9934(e)

Let V be a non empty additive loop structure. Observe that there exists a subset of V which is add closed and non empty and has inverse.

Let V be a ring. A ring is called a subring of V if it satisfies the conditions (Def. 3).

(Def. 3)(i) The carrier of it $\subseteq$ the carrier of V,

(ii) the addition of it = (the addition of V) $\restriction$ (the carrier of it),

(iii) the multiplication of it = (the multiplication of V) $\restriction$ (the carrier of it),

(iv) $1_{\rm it} = 1_V$, and

(v) $0_{\rm it} = 0_V$.

For simplicity, we follow the rules: X is a non empty set, x is an element of X, d_1, d_2 are elements of X, A is a binary operation on X, M is a function from $X \times X$ into X, V is a ring, and V_1 is a subset of V.

We now state the proposition

(1) Suppose $V_1 = X$ and $A =$ (the addition of V) $\restriction$ (V_1) and $M =$ (the multiplication of V) $\restriction$ (V_1) and $d_1 = 1_V$ and $d_2 = 0_V$ and V_1 has inverse. Then $\langle X, A, M, d_1, d_2 \rangle$ is a subring of V.

Let V be a ring. One can check that there exists a subring of V which is strict.

Let V be a non empty multiplicative loop with zero structure and let V_1 be a subset of V. We say that V_1 is multiplicatively-closed if and only if:

(Def. 4) $1_V \in V_1$ and for all elements v, u of V such that $v, u \in V_1$ holds $v \cdot u \in V_1$.

Let V be a non empty additive loop structure and let V_1 be a subset of V. Let us assume that V_1 is add closed and non empty. The functor $\mathrm{Add}(V_1, V)$ yielding a binary operation on V_1 is defined as follows:

(Def. 5) $\mathrm{Add}(V_1, V) =$ (the addition of V) $\restriction$ (V_1).

Let V be a non empty multiplicative loop with zero structure and let V_1 be a subset of V. Let us assume that V_1 is multiplicatively-closed and non empty. The functor $\mathrm{mult}(V_1, V)$ yields a binary operation on V_1 and is defined as follows:

(Def. 6) $\mathrm{mult}(V_1, V) =$ (the multiplication of V) $\restriction$ (V_1).

Let V be an add-associative right zeroed right complementable non empty double loop structure and let V_1 be a subset of V. Let us assume that V_1 is add closed and non empty and has inverse. The functor $\mathrm{Zero}(V_1, V)$ yields an element of V_1 and is defined by:

(Def. 7) $\mathrm{Zero}(V_1, V) = 0_V$.

Let V be a non empty multiplicative loop with zero structure and let V_1 be a subset of V. Let us assume that V_1 is multiplicatively-closed and non empty. The functor $\mathrm{One}(V_1, V)$ yields an element of V_1 and is defined as follows:

(Def. 8) $\mathrm{One}(V_1, V) = 1_V$.

We now state the proposition

(2) If V_1 is additively-closed, multiplicatively-closed, and non empty, then $\langle V_1, \mathrm{Add}(V_1, V), \mathrm{mult}(V_1, V), \mathrm{One}(V_1, V), \mathrm{Zero}(V_1, V)\rangle$ is a ring.

2. Some Properties of Algebras

In the sequel V is an algebra, V_1 is a subset of V, M_1 is a function from $\mathbb{R} \times X$ into X, and a is a real number.

Let V be an algebra. An algebra is called a subalgebra of V if it satisfies the conditions (Def. 9).

(Def. 9)(i) The carrier of it $\subseteq$ the carrier of V,

(ii) the addition of it $=$ (the addition of V) $\upharpoonright$ (the carrier of it),

(iii) the multiplication of it $=$ (the multiplication of V) $\upharpoonright$ (the carrier of it),

(iv) the external multiplication of it $=$ (the external multiplication of V)$\upharpoonright$($\mathbb{R} \times$ the carrier of it),

(v) $1_{\mathrm{it}} = 1_V$, and

(vi) $0_{\mathrm{it}} = 0_V$.

The following proposition is true

(3) Suppose that $V_1 = X$ and $d_1 = 0_V$ and $d_2 = 1_V$ and $A =$ (the addition of V) $\upharpoonright$ (V_1) and $M =$ (the multiplication of V) $\upharpoonright$ (V_1) and $M_1 =$ (the external multiplication of V)$\upharpoonright$($\mathbb{R} \times V_1$) and V_1 has inverse. Then $\langle X, M, A, M_1, d_2, d_1\rangle$ is a subalgebra of V.

Let V be an algebra. Observe that there exists a subalgebra of V which is strict.

Let V be an algebra and let V_1 be a subset of V. We say that V_1 is additively-linearly-closed if and only if:

(Def. 10) V_1 is add closed and has inverse and for every real number a and for every element v of V such that $v \in V_1$ holds $a \cdot v \in V_1$.

Let V be an algebra. One can check that every subset of V which is additively-linearly-closed is also additively-closed.

Let V be an algebra and let V_1 be a subset of V. Let us assume that V_1 is additively-linearly-closed and non empty. The functor $\mathrm{Mult}(V_1, V)$ yielding a function from $\mathbb{R} \times V_1$ into V_1 is defined by:

(Def. 11) $\mathrm{Mult}(V_1, V) =$ (the external multiplication of V)$\upharpoonright$($\mathbb{R} \times V_1$).

Let V be a non empty RLS structure. We say that V is scalar-multiplcation-cancelable if and only if:

(Def. 12) For every real number a and for every element v of V such that $a \cdot v = 0_V$ holds $a = 0$ or $v = 0_V$.

One can prove the following propositions:

(4) Let V be an add-associative right zeroed right complementable algebra-like non empty algebra structure and a be a real number. Then $a \cdot 0_V = 0_V$.

(5) Let V be an Abelian add-associative right zeroed right complementable algebra-like non empty algebra structure. Suppose V is scalar-multiplcation-cancelable. Then V is a real linear space.

(6) Suppose V_1 is additively-linearly-closed, multiplicatively-closed, and non empty.
Then $\langle V_1, \mathrm{mult}(V_1, V), \mathrm{Add}(V_1, V), \mathrm{Mult}(V_1, V), \mathrm{One}(V_1, V), \mathrm{Zero}(V_1, V)\rangle$ is a subalgebra of V.

Let X be a non empty set. Observe that RAlgebra X is Abelian, add-associative, right zeroed, right complementable, commutative, associative, right unital, right distributive, and algebra-like.

One can prove the following two propositions:

(7) RAlgebra X is a real linear space.

(8) Let V be an algebra and V_1 be a subalgebra of V. Then

(i) for all elements v_1, w_1 of V_1 and for all elements v, w of V such that $v_1 = v$ and $w_1 = w$ holds $v_1 + w_1 = v + w$,

(ii) for all elements v_1, w_1 of V_1 and for all elements v, w of V such that $v_1 = v$ and $w_1 = w$ holds $v_1 \cdot w_1 = v \cdot w$,

(iii) for every element v_1 of V_1 and for every element v of V and for every real number a such that $v_1 = v$ holds $a \cdot v_1 = a \cdot v$,

(iv) $\mathbf{1}_{(V_1)} = \mathbf{1}_V$, and

(v) $0_{(V_1)} = 0_V$.

3. Banach Algebra of Bounded Functionals

Let X be a non empty set. The functor BoundedFunctions X yielding a non empty subset of RAlgebra X is defined as follows:

(Def. 13) BoundedFunctions $X = \{f : X \to \mathbb{R}$: f is bounded on $X\}$.

We now state the proposition

(9) BoundedFunctions X is additively-linearly-closed and multiplicatively-closed.

Let us consider X. Note that BoundedFunctions X is additively-linearly-closed and multiplicatively-closed.

The following proposition is true

(10) $\langle$BoundedFunctions X, mult(BoundedFunctions X, RAlgebra X), Add(BoundedFunctions X, RAlgebra X), Mult(BoundedFunctions X, RAlgebra X), One(BoundedFunctions X, RAlgebra X), Zero(BoundedFunctions X, RAlgebra X)$\rangle$ is a subalgebra of RAlgebra X.

Let X be a non empty set. The $\mathbb{R}$-algebra of bounded functions on X yields an algebra and is defined by:

(Def. 14) The $\mathbb{R}$-algebra of bounded functions on $X = \langle \mathrm{BoundedFunctions}\, X, \mathrm{mult}(\mathrm{BoundedFunctions}\, X, \mathrm{RAlgebra}\, X), \mathrm{Add}(\mathrm{BoundedFunctions}\, X, \mathrm{RAlgebra}\, X), \mathrm{Mult}(\mathrm{BoundedFunctions}\, X, \mathrm{RAlgebra}\, X), \mathrm{One}(\mathrm{BoundedFunctions}\, X, \mathrm{RAlgebra}\, X), \mathrm{Zero}(\mathrm{BoundedFunctions}\, X, \mathrm{RAlgebra}\, X)\rangle$.

The following proposition is true

(11) The $\mathbb{R}$-algebra of bounded functions on X is a real linear space.

We adopt the following rules: F, G, H are vectors of the $\mathbb{R}$-algebra of bounded functions on X and f, g, h are functions from X into $\mathbb{R}$.

Next we state several propositions:

(12) If $f = F$ and $g = G$ and $h = H$, then $H = F + G$ iff for every element x of X holds $h(x) = f(x) + g(x)$.

(13) If $f = F$ and $g = G$, then $G = a \cdot F$ iff for every element x of X holds $g(x) = a \cdot f(x)$.

(14) If $f = F$ and $g = G$ and $h = H$, then $H = F \cdot G$ iff for every element x of X holds $h(x) = f(x) \cdot g(x)$.

(15) $0_{\text{the } \mathbb{R}\text{-algebra of bounded functions on } X} = X \longmapsto 0$.

(16) $\mathbf{1}_{\text{the } \mathbb{R}\text{-algebra of bounded functions on } X} = X \longmapsto 1$.

Let X be a non empty set and let F be a set. Let us assume that $F \in \mathrm{BoundedFunctions}\, X$. The functor $\mathrm{modetrans}(F, X)$ yielding a function from X into $\mathbb{R}$ is defined by:

(Def. 15) $\mathrm{modetrans}(F, X) = F$ and $\mathrm{modetrans}(F, X)$ is bounded on X.

Let X be a non empty set and let f be a function from X into $\mathbb{R}$. The functor $\mathrm{PreNorms}(f)$ yielding a non empty subset of $\mathbb{R}$ is defined as follows:

(Def. 16) $\mathrm{PreNorms}(f) = \{|f(x)| : x$ ranges over elements of $X\}$.

Next we state three propositions:

(17) If f is bounded on X, then $\mathrm{PreNorms}(f)$ is non empty and upper bounded.

(18) f is bounded on X iff $\mathrm{PreNorms}(f)$ is upper bounded.

(19) There exists a function N_1 from $\mathrm{BoundedFunctions}\, X$ into $\mathbb{R}$ such that for every set F such that $F \in \mathrm{BoundedFunctions}\, X$ holds $N_1(F) = \sup \mathrm{PreNorms}(\mathrm{modetrans}(F, X))$.

Let X be a non empty set. The functor $\mathrm{BoundedFunctionsNorm}\, X$ yields a function from $\mathrm{BoundedFunctions}\, X$ into $\mathbb{R}$ and is defined by:

(Def. 17) For every set x such that $x \in \mathrm{BoundedFunctions}\, X$ holds $(\mathrm{BoundedFunctionsNorm}\, X)(x) = \sup \mathrm{PreNorms}(\mathrm{modetrans}(x, X))$.

We now state two propositions:

(20) If f is bounded on X, then $\mathrm{modetrans}(f, X) = f$.

(21) If f is bounded on X, then $(\mathrm{BoundedFunctionsNorm}\, X)(f) = \sup \mathrm{PreNorms}(f)$.

Let X be a non empty set. The $\mathbb{R}$-normed algebra of bounded functions on X yielding a normed algebra structure is defined as follows:

(Def. 18) The $\mathbb{R}$-normed algebra of bounded functions on $X =$ $\langle \mathrm{BoundedFunctions}\, X, \mathrm{mult}(\mathrm{BoundedFunctions}\, X, \mathrm{RAlgebra}\, X),$ $\mathrm{Add}(\mathrm{BoundedFunctions}\, X, \mathrm{RAlgebra}\, X), \mathrm{Mult}(\mathrm{BoundedFunctions}\, X,$ $\mathrm{RAlgebra}\, X), \mathrm{One}(\mathrm{BoundedFunctions}\, X, \mathrm{RAlgebra}\, X),$ $\mathrm{Zero}(\mathrm{BoundedFunctions}\, X, \mathrm{RAlgebra}\, X), \mathrm{BoundedFunctionsNorm}\, X\rangle.$

Let X be a non empty set. Note that the $\mathbb{R}$-normed algebra of bounded functions on X is non empty.

Let X be a non empty set. Observe that the $\mathbb{R}$-normed algebra of bounded functions on X is unital.

We now state the proposition

(22) Let W be a normed algebra structure and V be an algebra. If the algebra structure of $W = V$ and $1_V = 1_W$, then W is an algebra.

In the sequel F, G, H denote points of the $\mathbb{R}$-normed algebra of bounded functions on X.

We now state a number of propositions:

(23) The $\mathbb{R}$-normed algebra of bounded functions on X is an algebra.

(24) $(\mathrm{Mult}(\mathrm{BoundedFunctions}\, X, \mathrm{RAlgebra}\, X))(1, F) = F.$

(25) The $\mathbb{R}$-normed algebra of bounded functions on X is a real linear space.

(26) $X \longmapsto 0 = 0_{\text{the } \mathbb{R}\text{-normed algebra of bounded functions on } X}.$

(27) If $f = F$ and f is bounded on X, then $|f(x)| \leq \|F\|$.

(28) $0 \leq \|F\|$.

(29) $0 = \|(0_{\text{the } \mathbb{R}\text{-normed algebra of bounded functions on } X})\|.$

(30) If $f = F$ and $g = G$ and $h = H$, then $H = F + G$ iff for every element x of X holds $h(x) = f(x) + g(x)$.

(31) If $f = F$ and $g = G$, then $G = a \cdot F$ iff for every element x of X holds $g(x) = a \cdot f(x)$.

(32) If $f = F$ and $g = G$ and $h = H$, then $H = F \cdot G$ iff for every element x of X holds $h(x) = f(x) \cdot g(x)$.

(33)(i) $\|F\| = 0$ iff $F = 0_{\text{the } \mathbb{R}\text{-normed algebra of bounded functions on } X}$,

(ii) $\|a \cdot F\| = |a| \cdot \|F\|$, and

(iii) $\|F + G\| \leq \|F\| + \|G\|$.

(34) The $\mathbb{R}$-normed algebra of bounded functions on X is real normed space-like.

Let X be a non empty set.

Note that the $\mathbb{R}$-normed algebra of bounded functions on X is real normed space-like, real linear space-like, Abelian, add-associative, right zeroed, and right complementable.

We now state three propositions:

(35) If $f = F$ and $g = G$ and $h = H$, then $H = F - G$ iff for every element x of X holds $h(x) = f(x) - g(x)$.

(36) Let X be a non empty set and s_1 be a sequence of the $\mathbb{R}$-normed algebra of bounded functions on X. If s_1 is Cauchy sequence by norm, then s_1 is convergent.

(37) The $\mathbb{R}$-normed algebra of bounded functions on X is a real Banach space.

Let X be a non empty set.

Observe that the $\mathbb{R}$-normed algebra of bounded functions on X is complete.

The following proposition is true

(38) The $\mathbb{R}$-normed algebra of bounded functions on X is a Banach algebra.

References

[1] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. *Formalized Mathematics*, 9(**3**):565–582, 2001.

[2] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

[3] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[8] Czesław Byliński and Piotr Rudnicki. Bounding boxes for compact sets in $\mathcal{E}^2$. *Formalized Mathematics*, 6(**3**):427–440, 1997.

[9] Jarosław Kotowicz. Convergent real sequences. Upper and lower bound of sets of real numbers. *Formalized Mathematics*, 1(**3**):477–481, 1990.

[10] Jarosław Kotowicz. Convergent sequences and the limit of sequences. *Formalized Mathematics*, 1(**2**):273–275, 1990.

[11] Jarosław Kotowicz. Partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 1(**4**):703–709, 1990.

[12] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[13] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[14] Yatsuka Nakamura, Piotr Rudnicki, Andrzej Trybulec, and Pauline N. Kawamoto. Preliminaries to circuits, I. *Formalized Mathematics*, 5(**2**):167–172, 1996.

[15] Henryk Oryszczyszyn and Krzysztof Prażmowski. Real functions spaces. *Formalized Mathematics*, 1(**3**):555–561, 1990.

[16] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.

[17] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.

[18] Yasunari Shidama. The Banach algebra of bounded linear operators. *Formalized Mathematics*, 12(**2**):103–108, 2004.

[19] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.

[20] Yasumasa Suzuki, Noboru Endou, and Yasunari Shidama. Banach space of absolute summable real sequences. *Formalized Mathematics*, 11(**4**):377–380, 2003.

[21] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

[22] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[23] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[24] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[25] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received March 3, 2008

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 123–133, 2008

Convex Sets and Convex Combinations on Complex Linear Spaces

Hidenori Matsuzaki
Shinshu University
Nagano, Japan

Noboru Endou
Gifu National College of Technology
Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, convex sets, convex combinations and convex hulls on complex linear spaces are introduced.

MML identifier: `CONVEX4`, version: `7.8.10 4.99.1005`

The articles [19], [18], [9], [23], [24], [6], [25], [7], [20], [3], [22], [17], [2], [11], [8], [1], [5], [10], [14], [15], [4], [16], [21], [12], and [13] provide the terminology and notation for this paper.

1. Complex Linear Combinations

Let V be a non empty zero structure. An element of $\mathbb{C}^{\text{the carrier of } V}$ is said to be a $\mathbb{C}$-linear combination of V if:

(Def. 1) There exists a finite subset T of V such that for every element v of V such that $v \notin T$ holds $\text{it}(v) = 0$.

Let V be a non empty additive loop structure and let L be an element of $\mathbb{C}^{\text{the carrier of } V}$. The support of L yielding a subset of V is defined by:

(Def. 2) The support of $L = \{v \in V\colon L(v) \neq 0_{\mathbb{C}}\}$.

Let V be a non empty additive loop structure and let L be a $\mathbb{C}$-linear combination of V. One can check that the support of L is finite.

The following proposition is true

(1) Let V be a non empty additive loop structure, L be a $\mathbb{C}$-linear combination of V, and v be an element of V. Then $L(v) = 0_{\mathbb{C}}$ if and only if $v \notin$ the support of L.

Let V be a non empty additive loop structure. The functor ZeroCLC V yields a $\mathbb{C}$-linear combination of V and is defined by:

(Def. 3) The support of ZeroCLC $V = \emptyset$.

Let V be a non empty additive loop structure. Note that the support of ZeroCLC V is empty.

We now state the proposition

(2) For every non empty additive loop structure V and for every element v of V holds $(\mathrm{ZeroCLC}\, V)(v) = 0_{\mathbb{C}}$.

Let V be a non empty additive loop structure and let A be a subset of V. A $\mathbb{C}$-linear combination of V is said to be a $\mathbb{C}$-linear combination of A if:

(Def. 4) The support of it $\subseteq A$.

Next we state three propositions:

(3) Let V be a non empty additive loop structure, A, B be subsets of V, and l be a $\mathbb{C}$-linear combination of A. If $A \subseteq B$, then l is a $\mathbb{C}$-linear combination of B.

(4) Let V be a non empty additive loop structure and A be a subset of V. Then ZeroCLC V is a $\mathbb{C}$-linear combination of A.

(5) Let V be a non empty additive loop structure and l be a $\mathbb{C}$-linear combination of $\emptyset_{\text{the carrier of } V}$. Then $l =$ ZeroCLC V.

In the sequel i is a natural number.

Let V be a non empty CLS structure, let F be a finite sequence of elements of the carrier of V, and let f be a function from the carrier of V into $\mathbb{C}$. The functor $f\,F$ yields a finite sequence of elements of the carrier of V and is defined as follows:

(Def. 5) $\mathrm{len}(f\,F) = \mathrm{len}\,F$ and for every i such that $i \in \mathrm{dom}(f\,F)$ holds $(f\,F)(i) = f(F_i) \cdot F_i$.

For simplicity, we follow the rules: V denotes a non empty CLS structure, v, v_1, v_2, v_3 denote vectors of V, A denotes a subset of V, l denotes a $\mathbb{C}$-linear combination of A, x denotes a set, a, b denote complex numbers, F denotes a finite sequence of elements of the carrier of V, and f denotes a function from the carrier of V into $\mathbb{C}$.

The following propositions are true:

(6) If $x \in \mathrm{dom}\,F$ and $v = F(x)$, then $(f\,F)(x) = f(v) \cdot v$.

(7) $f\,\varepsilon_{(\text{the carrier of } V)} = \varepsilon_{(\text{the carrier of } V)}$.

(8) $f\,\langle v \rangle = \langle f(v) \cdot v \rangle$.

(9) $f\,\langle v_1, v_2 \rangle = \langle f(v_1) \cdot v_1, f(v_2) \cdot v_2 \rangle$.

(10) $f\,\langle v_1, v_2, v_3\rangle = \langle f(v_1) \cdot v_1, f(v_2) \cdot v_2, f(v_3) \cdot v_3\rangle$.

In the sequel L, L_1, L_2, L_3 are $\mathbb{C}$-linear combinations of V.

Let V be an Abelian add-associative right zeroed right complementable non empty CLS structure and let L be a $\mathbb{C}$-linear combination of V. The functor $\sum L$ yields an element of V and is defined by the condition (Def. 6).

(Def. 6) There exists a finite sequence F of elements of the carrier of V such that F is one-to-one and $\operatorname{rng} F =$ the support of L and $\sum L = \sum L\,F$.

One can prove the following propositions:

(11) For every Abelian add-associative right zeroed right complementable non empty CLS structure V holds $\sum \operatorname{ZeroCLC} V = 0_V$.

(12) Let V be a complex linear space and A be a subset of V. Suppose $A \neq \emptyset$. Then A is linearly closed if and only if for every $\mathbb{C}$-linear combination l of A holds $\sum l \in A$.

(13) Let V be an Abelian add-associative right zeroed right complementable non empty CLS structure and l be a $\mathbb{C}$-linear combination of $\emptyset_{\text{the carrier of } V}$. Then $\sum l = 0_V$.

(14) Let V be a complex linear space, v be a vector of V, and l be a $\mathbb{C}$-linear combination of $\{v\}$. Then $\sum l = l(v) \cdot v$.

(15) Let V be a complex linear space and v_1, v_2 be vectors of V. Suppose $v_1 \neq v_2$. Let l be a $\mathbb{C}$-linear combination of $\{v_1, v_2\}$. Then $\sum l = l(v_1) \cdot v_1 + l(v_2) \cdot v_2$.

(16) Let V be an Abelian add-associative right zeroed right complementable non empty CLS structure and L be a $\mathbb{C}$-linear combination of V. If the support of $L = \emptyset$, then $\sum L = 0_V$.

(17) Let V be a complex linear space, L be a $\mathbb{C}$-linear combination of V, and v be a vector of V. If the support of $L = \{v\}$, then $\sum L = L(v) \cdot v$.

(18) Let V be a complex linear space, L be a $\mathbb{C}$-linear combination of V, and v_1, v_2 be vectors of V. If the support of $L = \{v_1, v_2\}$ and $v_1 \neq v_2$, then $\sum L = L(v_1) \cdot v_1 + L(v_2) \cdot v_2$.

Let V be a non empty additive loop structure and let L_1, L_2 be $\mathbb{C}$-linear combinations of V. Let us observe that $L_1 = L_2$ if and only if:

(Def. 7) For every element v of V holds $L_1(v) = L_2(v)$.

Let V be a non empty additive loop structure and let L_1, L_2 be $\mathbb{C}$-linear combinations of V. Then $L_1 + L_2$ is a $\mathbb{C}$-linear combination of V and it can be characterized by the condition:

(Def. 8) For every element v of V holds $(L_1 + L_2)(v) = L_1(v) + L_2(v)$.

One can prove the following propositions:

(19) The support of $L_1 + L_2 \subseteq$ (the support of L_1) $\cup$ (the support of L_2).

(20) Suppose L_1 is a $\mathbb{C}$-linear combination of A and L_2 is a $\mathbb{C}$-linear combination of A. Then $L_1 + L_2$ is a $\mathbb{C}$-linear combination of A.

Let us consider V, A and let L_1, L_2 be $\mathbb{C}$-linear combinations of A. Then $L_1 + L_2$ is a $\mathbb{C}$-linear combination of A.

The following three propositions are true:

(21) For every non empty additive loop structure V and for all $\mathbb{C}$-linear combinations L_1, L_2 of V holds $L_1 + L_2 = L_2 + L_1$.

(22) $L_1 + (L_2 + L_3) = (L_1 + L_2) + L_3$.

(23) $L + \mathrm{ZeroCLC}\, V = L$.

Let us consider V, a and let us consider L. The functor $a \cdot L$ yielding a $\mathbb{C}$-linear combination of V is defined as follows:

(Def. 9) For every v holds $(a \cdot L)(v) = a \cdot L(v)$.

One can prove the following propositions:

(24) If $a \neq 0_{\mathbb{C}}$, then the support of $a \cdot L =$ the support of L.

(25) $0_{\mathbb{C}} \cdot L = \mathrm{ZeroCLC}\, V$.

(26) If L is a $\mathbb{C}$-linear combination of A, then $a \cdot L$ is a $\mathbb{C}$-linear combination of A.

(27) $(a + b) \cdot L = a \cdot L + b \cdot L$.

(28) $a \cdot (L_1 + L_2) = a \cdot L_1 + a \cdot L_2$.

(29) $a \cdot (b \cdot L) = (a \cdot b) \cdot L$.

(30) $1_{\mathbb{C}} \cdot L = L$.

Let us consider V, L. The functor $-L$ yielding a $\mathbb{C}$-linear combination of V is defined as follows:

(Def. 10) $-L = (-1_{\mathbb{C}}) \cdot L$.

We now state three propositions:

(31) $(-L)(v) = -L(v)$.

(32) If $L_1 + L_2 = \mathrm{ZeroCLC}\, V$, then $L_2 = -L_1$.

(33) $--L = L$.

Let us consider V and let us consider L_1, L_2. The functor $L_1 - L_2$ yields a $\mathbb{C}$-linear combination of V and is defined by:

(Def. 11) $L_1 - L_2 = L_1 + -L_2$.

One can prove the following propositions:

(34) $(L_1 - L_2)(v) = L_1(v) - L_2(v)$.

(35) The support of $L_1 - L_2 \subseteq$ (the support of L_1) $\cup$ (the support of L_2).

(36) Suppose L_1 is a $\mathbb{C}$-linear combination of A and L_2 is a $\mathbb{C}$-linear combination of A. Then $L_1 - L_2$ is a $\mathbb{C}$-linear combination of A.

(37) $L - L = \mathrm{ZeroCLC}\, V$.

Let us consider V. The functor $\mathbb{C}$-LinComb V yields a set and is defined as follows:

(Def. 12) $x \in \mathbb{C}\text{-LinComb}\, V$ iff x is a $\mathbb{C}$-linear combination of V.

Let us consider V. One can verify that $\mathbb{C}$-LinComb V is non empty.

In the sequel e, e_1, e_2 denote elements of $\mathbb{C}$-LinComb V.

Let us consider V and let us consider e. The functor ${}^{@}e$ yields a $\mathbb{C}$-linear combination of V and is defined as follows:

(Def. 13) ${}^{@}e = e$.

Let us consider V and let us consider L. The functor ${}^{@}L$ yielding an element of $\mathbb{C}$-LinComb V is defined by:

(Def. 14) ${}^{@}L = L$.

Let us consider V. The functor $\mathbb{C}$-LCAdd V yields a binary operation on $\mathbb{C}$-LinComb V and is defined by:

(Def. 15) For all e_1, e_2 holds $(\mathbb{C}\text{-LCAdd}\, V)(e_1, e_2) = ({}^{@}e_1) + {}^{@}e_2$.

Let us consider V. The functor $\mathbb{C}$-LCMult V yields a function from $\mathbb{C} \times \mathbb{C}$-LinComb V into $\mathbb{C}$-LinComb V and is defined as follows:

(Def. 16) For all a, e holds $(\mathbb{C}\text{-LCMult}\, V)(\langle a, e\rangle) = a \cdot ({}^{@}e)$.

Let us consider V. The functor L$\mathbb{C}$-CLSpace V yielding a complex linear space is defined by:

(Def. 17) $\text{L}\mathbb{C}\text{-CLSpace}\, V = \langle \mathbb{C}\text{-LinComb}\, V, {}^{@}\text{ZeroCLC}\, V, \mathbb{C}\text{-LCAdd}\, V, \mathbb{C}\text{-LCMult}\, V \rangle$.

Let us consider V. Note that L$\mathbb{C}$-CLSpace V is strict and non empty.

We now state four propositions:

(38) ${L_1}^{\text{L}\mathbb{C}\text{-CLSpace}\, V} + {L_2}^{\text{L}\mathbb{C}\text{-CLSpace}\, V} = L_1 + L_2$.

(39) $a \cdot L^{\text{L}\mathbb{C}\text{-CLSpace}\, V} = a \cdot L$.

(40) $-L^{\text{L}\mathbb{C}\text{-CLSpace}\, V} = -L$.

(41) ${L_1}^{\text{L}\mathbb{C}\text{-CLSpace}\, V} - {L_2}^{\text{L}\mathbb{C}\text{-CLSpace}\, V} = L_1 - L_2$.

Let us consider V and let us consider A. The functor L$\mathbb{C}$-CLSpace A yielding a strict subspace of L$\mathbb{C}$-CLSpace V is defined as follows:

(Def. 18) The carrier of L$\mathbb{C}$-CLSpace $A = \{l\}$.

2. Preliminaries for Complex Convex Sets

Let V be a complex linear space and let W be a subspace of V. The functor $\text{Up}(W)$ yields a subset of V and is defined by:

(Def. 19) $\text{Up}(W) =$ the carrier of W.

Let V be a complex linear space and let W be a subspace of V. One can check that $\text{Up}(W)$ is non empty.

Let V be a non empty CLS structure and let S be a subset of V. We say that S is affine if and only if the condition (Def. 20) is satisfied.

(Def. 20) Let x, y be vectors of V and z be a complex number. If there exists a real number a such that $a = z$ and x, $y \in S$, then $(1_{\mathbb{C}} - z) \cdot x + z \cdot y \in S$.

Let V be a complex linear space. The functor Ω_V yields a strict subspace of V and is defined as follows:

(Def. 21) $\Omega_V =$ the CLS structure of V.

Let V be a non empty CLS structure. Observe that Ω_V is affine and $\emptyset_V$ is affine.

Let V be a non empty CLS structure. One can check that there exists a subset of V which is non empty and affine and there exists a subset of V which is empty and affine.

We now state three propositions:

(42) For every real number a and for every complex number z holds $\Re(a \cdot z) = a \cdot \Re(z)$.

(43) For every real number a and for every complex number z holds $\Im(a \cdot z) = a \cdot \Im(z)$.

(44) For every real number a and for every complex number z such that $0 \leq a \leq 1$ holds $|a \cdot z| = a \cdot |z|$ and $|(1_{\mathbb{C}} - a) \cdot z| = (1_{\mathbb{C}} - a) \cdot |z|$.

3. Complex Convex Sets

Let V be a non empty CLS structure, let M be a subset of V, and let r be an element of $\mathbb{C}$. The functor $r \cdot M$ yielding a subset of V is defined by:

(Def. 22) $r \cdot M = \{r \cdot v; v$ ranges over elements of V: $v \in M\}$.

Let V be a non empty CLS structure and let M be a subset of V. We say that M is convex if and only if the condition (Def. 23) is satisfied.

(Def. 23) Let u, v be vectors of V and z be a complex number. Suppose there exists a real number r such that $z = r$ and $0 < r < 1$ and u, $v \in M$. Then $z \cdot u + (1_{\mathbb{C}} - z) \cdot v \in M$.

One can prove the following propositions:

(45) Let V be a complex linear space-like non empty CLS structure, M be a subset of V, and z be a complex number. If M is convex, then $z \cdot M$ is convex.

(46) Let V be an Abelian add-associative complex linear space-like non empty CLS structure and M, N be subsets of V. If M is convex and N is convex, then $M + N$ is convex.

(47) Let V be a complex linear space and M, N be subsets of V. If M is convex and N is convex, then $M - N$ is convex.

(48) Let V be a non empty CLS structure and M be a subset of V. Then M is convex if and only if for every complex number z such that there exists a real number r such that $z = r$ and $0 < r < 1$ holds $z \cdot M + (1_{\mathbb{C}} - z) \cdot M \subseteq M$.

(49) Let V be an Abelian non empty CLS structure and M be a subset of V. Suppose M is convex. Let z be a complex number. If there exists a real number r such that $z = r$ and $0 < r < 1$, then $(1_{\mathbb{C}} - z) \cdot M + z \cdot M \subseteq M$.

(50) Let V be an Abelian add-associative complex linear space-like non empty CLS structure and M, N be subsets of V. Suppose M is convex and N is convex. Let z be a complex number. If there exists a real number r such that $z = r$, then $z \cdot M + (1_{\mathbb{C}} - z) \cdot N$ is convex.

(51) For every complex linear space-like non empty CLS structure V and for every subset M of V holds $1_{\mathbb{C}} \cdot M = M$.

(52) For every complex linear space V and for every non empty subset M of V holds $0_{\mathbb{C}} \cdot M = \{0_V\}$.

(53) For every add-associative non empty additive loop structure V and for all subsets M_1, M_2, M_3 of V holds $(M_1 + M_2) + M_3 = M_1 + (M_2 + M_3)$.

(54) Let V be a complex linear space-like non empty CLS structure, M be a subset of V, and z_1, z_2 be complex numbers. Then $z_1 \cdot (z_2 \cdot M) = (z_1 \cdot z_2) \cdot M$.

(55) Let V be a complex linear space-like non empty CLS structure, M_1, M_2 be subsets of V, and z be a complex number. Then $z \cdot (M_1 + M_2) = z \cdot M_1 + z \cdot M_2$.

(56) Let V be a complex linear space, M be a subset of V, and v be a vector of V. Then M is convex if and only if $v + M$ is convex.

(57) For every complex linear space V holds $\mathrm{Up}(\mathbf{0}_V)$ is convex.

(58) For every complex linear space V holds $\mathrm{Up}(\Omega_V)$ is convex.

(59) For every non empty CLS structure V and for every subset M of V such that $M = \emptyset$ holds M is convex.

(60) Let V be an Abelian add-associative complex linear space-like non empty CLS structure, M_1, M_2 be subsets of V, and z_1, z_2 be complex numbers. If M_1 is convex and M_2 is convex, then $z_1 \cdot M_1 + z_2 \cdot M_2$ is convex.

(61) Let V be a complex linear space-like non empty CLS structure, M be a subset of V, and z_1, z_2 be complex numbers. Then $(z_1 + z_2) \cdot M \subseteq z_1 \cdot M + z_2 \cdot M$.

(62) Let V be a non empty CLS structure, M, N be subsets of V, and z be a complex number. If $M \subseteq N$, then $z \cdot M \subseteq z \cdot N$.

(63) For every non empty CLS structure V and for every empty subset M of V and for every complex number z holds $z \cdot M = \emptyset$.

(64) Let V be a non empty additive loop structure, M be an empty subset of V, and N be a subset of V. Then $M + N = \emptyset$.

(65) For every right zeroed non empty additive loop structure V and for every subset M of V holds $M + \{0_V\} = M$.

(66) Let V be a complex linear space, M be a subset of V, and z_1, z_2 be complex numbers. Suppose there exist real numbers r_1, r_2 such that $z_1 = r_1$ and $z_2 = r_2$ and $r_1 \geq 0$ and $r_2 \geq 0$ and M is convex. Then $z_1 \cdot M + z_2 \cdot M = (z_1 + z_2) \cdot M$.

(67) Let V be an Abelian add-associative complex linear space-like non empty CLS structure, M_1, M_2, M_3 be subsets of V, and z_1, z_2, z_3 be complex numbers. If M_1 is convex and M_2 is convex and M_3 is convex, then $z_1 \cdot M_1 + z_2 \cdot M_2 + z_3 \cdot M_3$ is convex.

(68) Let V be a non empty CLS structure and F be a family of subsets of V. Suppose that for every subset M of V such that $M \in F$ holds M is convex. Then $\bigcap F$ is convex.

(69) For every non empty CLS structure V and for every subset M of V such that M is affine holds M is convex.

Let V be a non empty CLS structure. One can check that there exists a subset of V which is non empty and convex.

Let V be a non empty CLS structure. Observe that there exists a subset of V which is empty and convex.

One can prove the following propositions:

(70) Let V be a complex unitary space-like non empty complex unitary space structure, M be a subset of V, v be a vector of V, and r be a real number. If $M = \{u; u$ ranges over vectors of V: $\Re((u|v)) \geq r\}$, then M is convex.

(71) Let V be a complex unitary space-like non empty complex unitary space structure, M be a subset of V, v be a vector of V, and r be a real number. If $M = \{u; u$ ranges over vectors of V: $\Re((u|v)) > r\}$, then M is convex.

(72) Let V be a complex unitary space-like non empty complex unitary space structure, M be a subset of V, v be a vector of V, and r be a real number. If $M = \{u; u$ ranges over vectors of V: $\Re((u|v)) \leq r\}$, then M is convex.

(73) Let V be a complex unitary space-like non empty complex unitary space structure, M be a subset of V, v be a vector of V, and r be a real number. If $M = \{u; u$ ranges over vectors of V: $\Re((u|v)) < r\}$, then M is convex.

(74) Let V be a complex unitary space-like non empty complex unitary space structure, M be a subset of V, v be a vector of V, and r be a real number. If $M = \{u; u$ ranges over vectors of V: $\Im((u|v)) \geq r\}$, then M is convex.

(75) Let V be a complex unitary space-like non empty complex unitary space structure, M be a subset of V, v be a vector of V, and r be a real number. If $M = \{u; u$ ranges over vectors of V: $\Im((u|v)) > r\}$, then M is convex.

(76) Let V be a complex unitary space-like non empty complex unitary space structure, M be a subset of V, v be a vector of V, and r be a real number.

If $M = \{u; u$ ranges over vectors of V: $\Im((u|v)) \leq r\}$, then M is convex.

(77) Let V be a complex unitary space-like non empty complex unitary space structure, M be a subset of V, v be a vector of V, and r be a real number. If $M = \{u; u$ ranges over vectors of V: $\Im((u|v)) < r\}$, then M is convex.

(78) Let V be a complex unitary space-like non empty complex unitary space structure, M be a subset of V, v be a vector of V, and r be a real number. If $M = \{u; u$ ranges over vectors of V: $|(u|v)| \leq r\}$, then M is convex.

(79) Let V be a complex unitary space-like non empty complex unitary space structure, M be a subset of V, v be a vector of V, and r be a real number. If $M = \{u; u$ ranges over vectors of V: $|(u|v)| < r\}$, then M is convex.

4. Complex Convex Combinations

Let V be a complex linear space and let L be a $\mathbb{C}$-linear combination of V. We say that L is convex if and only if the condition (Def. 24) is satisfied.

(Def. 24) There exists a finite sequence F of elements of the carrier of V such that

(i) F is one-to-one,

(ii) $\operatorname{rng} F =$ the support of L, and

(iii) there exists a finite sequence f of elements of $\mathbb{R}$ such that $\operatorname{len} f = \operatorname{len} F$ and $\sum f = 1$ and for every natural number n such that $n \in \operatorname{dom} f$ holds $f(n) = L(F(n))$ and $f(n) \geq 0$.

We now state several propositions:

(80) Let V be a complex linear space and L be a $\mathbb{C}$-linear combination of V. If L is convex, then the support of $L \neq \emptyset$.

(81) Let V be a complex linear space, L be a $\mathbb{C}$-linear combination of V, and v be a vector of V. Suppose L is convex and there exists a real number r such that $r = L(v)$ and $r \leq 0$. Then $v \notin$ the support of L.

(82) For every complex linear space V and for every $\mathbb{C}$-linear combination L of V such that L is convex holds $L \neq \operatorname{ZeroCLC} V$.

(83) Let V be a complex linear space, v be a vector of V, and L be a $\mathbb{C}$-linear combination of V. Suppose L is convex and the support of $L = \{v\}$. Then there exists a real number r such that $r = L(v)$ and $r = 1$ and $\sum L = L(v) \cdot v$.

(84) Let V be a complex linear space, v_1, v_2 be vectors of V, and L be a $\mathbb{C}$-linear combination of V. Suppose L is convex and the support of $L = \{v_1, v_2\}$ and $v_1 \neq v_2$. Then there exist real numbers r_1, r_2 such that $r_1 = L(v_1)$ and $r_2 = L(v_2)$ and $r_1 + r_2 = 1$ and $r_1 \geq 0$ and $r_2 \geq 0$ and $\sum L = L(v_1) \cdot v_1 + L(v_2) \cdot v_2$.

(85) Let V be a complex linear space, v_1, v_2, v_3 be vectors of V, and L be a $\mathbb{C}$-linear combination of V. Suppose L is convex and the support of $L = \{v_1, v_2, v_3\}$ and $v_1 \neq v_2 \neq v_3 \neq v_1$. Then

(i) there exist real numbers r_1, r_2, r_3 such that $r_1 = L(v_1)$ and $r_2 = L(v_2)$ and $r_3 = L(v_3)$ and $r_1 + r_2 + r_3 = 1$ and $r_1 \geq 0$ and $r_2 \geq 0$ and $r_3 \geq 0$, and

(ii) $\sum L = L(v_1) \cdot v_1 + L(v_2) \cdot v_2 + L(v_3) \cdot v_3$.

(86) Let V be a complex linear space, v be a vector of V, and L be a $\mathbb{C}$-linear combination of $\{v\}$. Suppose L is convex. Then there exists a real number r such that $r = L(v)$ and $r = 1$ and $\sum L = L(v) \cdot v$.

(87) Let V be a complex linear space, v_1, v_2 be vectors of V, and L be a $\mathbb{C}$-linear combination of $\{v_1, v_2\}$. Suppose $v_1 \neq v_2$ and L is convex. Then there exist real numbers r_1, r_2 such that $r_1 = L(v_1)$ and $r_2 = L(v_2)$ and $r_1 \geq 0$ and $r_2 \geq 0$ and $\sum L = L(v_1) \cdot v_1 + L(v_2) \cdot v_2$.

(88) Let V be a complex linear space, v_1, v_2, v_3 be vectors of V, and L be a $\mathbb{C}$-linear combination of $\{v_1, v_2, v_3\}$. Suppose $v_1 \neq v_2 \neq v_3 \neq v_1$ and L is convex. Then

(i) there exist real numbers r_1, r_2, r_3 such that $r_1 = L(v_1)$ and $r_2 = L(v_2)$ and $r_3 = L(v_3)$ and $r_1 + r_2 + r_3 = 1$ and $r_1 \geq 0$ and $r_2 \geq 0$ and $r_3 \geq 0$, and

(ii) $\sum L = L(v_1) \cdot v_1 + L(v_2) \cdot v_2 + L(v_3) \cdot v_3$.

5. Complex Convex Hull

Let V be a non empty CLS structure and let M be a subset of V. The functor Convex-Family M yielding a family of subsets of V is defined by:

(Def. 25) For every subset N of V holds $N \in$ Convex-Family M iff N is convex and $M \subseteq N$.

Let V be a non empty CLS structure and let M be a subset of V. The functor conv M yielding a convex subset of V is defined as follows:

(Def. 26) conv $M = \bigcap$ Convex-Family M.

The following proposition is true

(89) Let V be a non empty CLS structure, M be a subset of V, and N be a convex subset of V. If $M \subseteq N$, then conv $M \subseteq N$.

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 and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[5] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[10] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[12] Noboru Endou. Complex linear space and complex normed space. *Formalized Mathematics*, 12(**2**):93–102, 2004.
[13] Noboru Endou. Complex linear space of complex sequences. *Formalized Mathematics*, 12(**2**):109–117, 2004.
[14] Noboru Endou, Takashi Mitsuishi, and Yasunari Shidama. Dimension of real unitary space. *Formalized Mathematics*, 11(**1**):23–28, 2003.
[15] Noboru Endou, Takashi Mitsuishi, and Yasunari Shidama. Topology of real unitary space. *Formalized Mathematics*, 11(**1**):33–38, 2003.
[16] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[17] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[18] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[19] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[20] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.
[21] Wojciech A. Trybulec. Linear combinations in real linear space. *Formalized Mathematics*, 1(**3**):581–588, 1990.
[22] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[23] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[24] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[25] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received March 3, 2008

FORMALIZED MATHEMATICS
Vol. **16**, No. **2**, Pages 135–139, **2008**

Inner Products, Group, Ring of Quaternion Numbers

Fuguo Ge
Qingdao University of Science
and Technology
China

Summary. In this article, we define the division of the quaternion numbers, we also give the definition of inner products, group, ring of the quaternion numbers, and we prove some of their properties.

MML identifier: `QUATERN2`, version: `7.8.10 4.100.1011`

The articles [9], [1], [3], [4], [6], [5], [2], [7], and [8] provide the notation and terminology for this paper.

We use the following convention: q, r, c, c_1, c_2, c_3 are quaternion numbers and x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 are elements of $\mathbb{R}$.

$0_{\mathbb{H}}$ is an element of $\mathbb{H}$.

$1_{\mathbb{H}}$ is an element of $\mathbb{H}$.

Next we state several propositions:

(1) For all real numbers x, y, z, w holds $\langle x, y, z, w\rangle_{\mathbb{H}} = x + y \cdot i + z \cdot j + w \cdot k$.

(2) $(c_1 + c_2) + c_3 = c_1 + (c_2 + c_3)$.

(3) $c + 0_{\mathbb{H}} = c$.

(4) $-\langle x_1, x_2, x_3, x_4\rangle_{\mathbb{H}} = \langle -x_1, -x_2, -x_3, -x_4\rangle_{\mathbb{H}}$.

(5) $\langle x_1, x_2, x_3, x_4\rangle_{\mathbb{H}} - \langle y_1, y_2, y_3, y_4\rangle_{\mathbb{H}} = \langle x_1 - y_1, x_2 - y_2, x_3 - y_3, x_4 - y_4\rangle_{\mathbb{H}}$.

(6) $(c_1 - c_2) + c_3 = (c_1 + c_3) - c_2$.

(7) $c_1 = (c_1 + c_2) - c_2$.

(8) $c_1 = (c_1 - c_2) + c_2$.

(9) $(-x_1) \cdot c = -x_1 \cdot c$.

ISSN 1426–2630(p), 1898-9934(e)

Let us consider q. Then $|q|$ is an element of $\mathbb{R}$.

i Is an element of $\mathbb{H}$.

We now state a number of propositions:

(10) If $r \neq 0$, then $|r| > 0$.

(11) $(0) \cdot c = 0$.

(12) $c \cdot (0) = 0$.

(13) $c \cdot 1_{\mathbb{H}} = c$.

(14) $1_{\mathbb{H}} \cdot c = c$.

(15) $(c_1 \cdot c_2) \cdot c_3 = c_1 \cdot (c_2 \cdot c_3)$.

(16) $c_1 \cdot (c_2 + c_3) = c_1 \cdot c_2 + c_1 \cdot c_3$.

(17) $(c_1 + c_2) \cdot c_3 = c_1 \cdot c_3 + c_2 \cdot c_3$.

(18) $-c = (-1_{\mathbb{H}}) \cdot c$.

(19) $(-c_1) \cdot c_2 = -c_1 \cdot c_2$.

(20) $c_1 \cdot -c_2 = -c_1 \cdot c_2$.

(21) $(-c_1) \cdot -c_2 = c_1 \cdot c_2$.

(22) $(c_1 - c_2) \cdot c_3 = c_1 \cdot c_3 - c_2 \cdot c_3$.

(23) $c_1 \cdot (c_2 - c_3) = c_1 \cdot c_2 - c_1 \cdot c_3$.

(24) $\overline{\langle x_1, x_2, x_3, x_4 \rangle_{\mathbb{H}}} = \langle x_1, -x_2, -x_3, -x_4 \rangle_{\mathbb{H}}$.

(25) $\overline{\overline{c}} = c$.

Let us consider q, r. The functor $\frac{q}{r}$ is defined by the condition (Def. 1).

(Def. 1) There exist elements q_0, q_1, q_2, q_3, r_0, r_1, r_2, r_3 of $\mathbb{R}$ such that

(i) $q = \langle q_0, q_1, q_2, q_3 \rangle_{\mathbb{H}}$,

(ii) $r = \langle r_0, r_1, r_2, r_3 \rangle_{\mathbb{H}}$, and

(iii) $\frac{q}{r} = \langle \frac{r_0 \cdot q_0 + r_1 \cdot q_1 + r_2 \cdot q_2 + r_3 \cdot q_3}{|r|^{\mathbf{2}}}, \frac{(r_0 \cdot q_1 - r_1 \cdot q_0 - r_2 \cdot q_3) + r_3 \cdot q_2}{|r|^{\mathbf{2}}}, \frac{(r_0 \cdot q_2 + r_1 \cdot q_3) - r_2 \cdot q_0 - r_3 \cdot q_1}{|r|^{\mathbf{2}}},$
$\frac{((r_0 \cdot q_3 - r_1 \cdot q_2) + r_2 \cdot q_1) - r_3 \cdot q_0}{|r|^{\mathbf{2}}} \rangle_{\mathbb{H}}$.

Let us consider q, r. One can check that $\frac{q}{r}$ is quaternion.

Let us consider q, r. Then $\frac{q}{r}$ is an element of $\mathbb{H}$ and it can be characterized by the condition:

(Def. 2) $\frac{q}{r} = \frac{\Re(r) \cdot \Re(q) + \Im_1(q) \cdot \Im_1(r) + \Im_2(r) \cdot \Im_2(q) + \Im_3(r) \cdot \Im_3(q)}{|r|^{\mathbf{2}}} +$
$\frac{(\Re(r) \cdot \Im_1(q) - \Im_1(r) \cdot \Re(q) - \Im_2(r) \cdot \Im_3(q)) + \Im_3(r) \cdot \Im_2(q)}{|r|^{\mathbf{2}}} \cdot i +$
$\frac{(\Re(r) \cdot \Im_2(q) + \Im_1(r) \cdot \Im_3(q)) - \Im_2(r) \cdot \Re(q) - \Im_3(r) \cdot \Im_1(q)}{|r|^{\mathbf{2}}} \cdot j +$
$\frac{((\Re(r) \cdot \Im_3(q) - \Im_1(r) \cdot \Im_2(q)) + \Im_2(r) \cdot \Im_1(q)) - \Im_3(r) \cdot \Re(q)}{|r|^{\mathbf{2}}} \cdot k$.

Let us consider c. The functor c^{-1} yielding a quaternion number is defined by:

(Def. 3) $c^{-1} = \frac{1_{\mathbb{H}}}{c}$.

Let us consider r. Then r^{-1} is an element of $\mathbb{H}$ and it can be characterized by the condition:

(Def. 4) $r^{-1} = \frac{\Re(r)}{|r|^{\mathbf{2}}} - \frac{\Im_1(r)}{|r|^{\mathbf{2}}} \cdot i - \frac{\Im_2(r)}{|r|^{\mathbf{2}}} \cdot j - \frac{\Im_3(r)}{|r|^{\mathbf{2}}} \cdot k$.

We now state several propositions:

(26) $\Re(r^{-1}) = \frac{\Re(r)}{|r|^{\mathbf{2}}}$ and $\Im_1(r^{-1}) = -\frac{\Im_1(r)}{|r|^{\mathbf{2}}}$ and $\Im_2(r^{-1}) = -\frac{\Im_2(r)}{|r|^{\mathbf{2}}}$ and $\Im_3(r^{-1}) = -\frac{\Im_3(r)}{|r|^{\mathbf{2}}}$.

(27)(i) $\Re(\frac{q}{r}) = \frac{\Re(r) \cdot \Re(q) + \Im_1(q) \cdot \Im_1(r) + \Im_2(r) \cdot \Im_2(q) + \Im_3(r) \cdot \Im_3(q)}{|r|^{\mathbf{2}}}$,

(ii) $\Im_1(\frac{q}{r}) = \frac{(\Re(r) \cdot \Im_1(q) - \Im_1(r) \cdot \Re(q) - \Im_2(r) \cdot \Im_3(q)) + \Im_3(r) \cdot \Im_2(q)}{|r|^{\mathbf{2}}}$,

(iii) $\Im_2(\frac{q}{r}) = \frac{(\Re(r) \cdot \Im_2(q) + \Im_1(r) \cdot \Im_3(q)) - \Im_2(r) \cdot \Re(q) - \Im_3(r) \cdot \Im_1(q)}{|r|^{\mathbf{2}}}$, and

(iv) $\Im_3(\frac{q}{r}) = \frac{((\Re(r) \cdot \Im_3(q) - \Im_1(r) \cdot \Im_2(q)) + \Im_2(r) \cdot \Im_1(q)) - \Im_3(r) \cdot \Re(q)}{|r|^{\mathbf{2}}}$.

(28) If $r \neq 0$, then $r \cdot r^{-1} = 1$.

(29) If $r \neq 0$, then $r^{-1} \cdot r = 1$.

(30) If $c \neq 0_{\mathbb{H}}$, then $\frac{c}{c} = 1_{\mathbb{H}}$.

(31) $(-c)^{-1} = -c^{-1}$.

The unary operation $\mathrm{compl}_{\mathbb{H}}$ on $\mathbb{H}$ is defined by:

(Def. 5) For every element c of $\mathbb{H}$ holds $\mathrm{compl}_{\mathbb{H}}(c) = -c$.

The binary operation $+_{\mathbb{H}}$ on $\mathbb{H}$ is defined as follows:

(Def. 6) For all elements c_1, c_2 of $\mathbb{H}$ holds $+_{\mathbb{H}}(c_1, c_2) = c_1 + c_2$.

The binary operation $-_{\mathbb{H}}$ on $\mathbb{H}$ is defined by:

(Def. 7) For all elements c_1, c_2 of $\mathbb{H}$ holds $-_{\mathbb{H}}(c_1, c_2) = c_1 - c_2$.

The binary operation $\cdot_{\mathbb{H}}$ on $\mathbb{H}$ is defined as follows:

(Def. 8) For all elements c_1, c_2 of $\mathbb{H}$ holds $\cdot_{\mathbb{H}}(c_1, c_2) = c_1 \cdot c_2$.

The binary operation $/_{\mathbb{H}}$ on $\mathbb{H}$ is defined as follows:

(Def. 9) For all elements c_1, c_2 of $\mathbb{H}$ holds $/_{\mathbb{H}}(c_1, c_2) = \frac{c_1}{c_2}$.

The unary operation $\overset{-1}{\mathbb{H}}$ on $\mathbb{H}$ is defined by:

(Def. 10) For every element c of $\mathbb{H}$ holds $(\overset{-1}{\mathbb{H}})(c) = c^{-1}$.

The strict additive loop structure $\mathbb{H}_{\mathrm{G}}$ is defined as follows:

(Def. 11) The carrier of $\mathbb{H}_{\mathrm{G}} = \mathbb{H}$ and the addition of $\mathbb{H}_{\mathrm{G}} = +_{\mathbb{H}}$ and $0_{\mathbb{H}_{\mathrm{G}}} = 0_{\mathbb{H}}$.

Let us mention that $\mathbb{H}_{\mathrm{G}}$ is non empty.

Let us note that every element of $\mathbb{H}_{\mathrm{G}}$ is quaternion.

Let x, y be elements of $\mathbb{H}_{\mathrm{G}}$ and let a, b be quaternion numbers. One can check that $x + y$ and $a + b$ can be identified when $x = a$ and $y = b$.

One can prove the following proposition

(32) $0_{\mathbb{H}_{\mathrm{G}}} = 0_{\mathbb{H}}$.

Let us observe that $\mathbb{H}_{\mathrm{G}}$ is Abelian, add-associative, right zeroed, and right complementable.

Let x be an element of $\mathbb{H}_{\mathrm{G}}$ and let a be a quaternion number. Note that $-x$ and $-a$ can be identified when $x = a$.

Let x, y be elements of $\mathbb{H}_{\mathrm{G}}$ and let a, b be quaternion numbers. One can verify that $x - y$ and $a - b$ can be identified when $x = a$ and $y = b$.

Next we state the proposition

(33) For all elements x, y, z of $\mathbb{H}_{\mathrm{G}}$ holds $x + y = y + x$ and $(x + y) + z = x + (y + z)$ and $x + 0_{\mathbb{H}_{\mathrm{G}}} = x$.

The strict double loop structure $\mathbb{H}_{\mathrm{R}}$ is defined as follows:

(Def. 12) The carrier of $\mathbb{H}_{\mathrm{R}} = \mathbb{H}$ and the addition of $\mathbb{H}_{\mathrm{R}} = +_{\mathbb{H}}$ and the multiplication of $\mathbb{H}_{\mathrm{R}} = \cdot_{\mathbb{H}}$ and $1_{\mathbb{H}_{\mathrm{R}}} = 1_{\mathbb{H}}$ and $0_{\mathbb{H}_{\mathrm{R}}} = 0_{\mathbb{H}}$.

Let us note that $\mathbb{H}_{\mathrm{R}}$ is non empty.

Let us observe that every element of $\mathbb{H}_{\mathrm{R}}$ is quaternion.

Let a, b be quaternion numbers and let x, y be elements of $\mathbb{H}_{\mathrm{R}}$. One can check the following observations: $x + y$ can be identified with $a + b$ and $x \cdot y$ can be identified with $a \cdot b$ when $x = a$ and $y = b$.

One can check that $\mathbb{H}_{\mathrm{R}}$ is well unital.

Next we state three propositions:

(34) $1_{\mathbb{H}_{\mathrm{R}}} = 1_{\mathbb{H}}$.

(35) $\mathbf{1}_{\mathbb{H}_{\mathrm{R}}} = 1_{\mathbb{H}}$.

(36) $0_{\mathbb{H}_{\mathrm{R}}} = 0_{\mathbb{H}}$.

Let us mention that $\mathbb{H}_{\mathrm{R}}$ is add-associative, right zeroed, right complementable, Abelian, associative, left unital, right unital, distributive, almost right invertible, and non degenerated.

Let x be an element of $\mathbb{H}_{\mathrm{R}}$ and let a be a quaternion number. Observe that $-x$ and $-a$ can be identified when $x = a$.

Let x, y be elements of $\mathbb{H}_{\mathrm{R}}$ and let a, b be quaternion numbers. Observe that $x - y$ and $a - b$ can be identified when $x = a$ and $y = b$.

Let z be an element of $\mathbb{H}_{\mathrm{R}}$. Then $\overline{z}$ is an element of $\mathbb{H}_{\mathrm{R}}$.

In the sequel z denotes an element of $\mathbb{H}_{\mathrm{R}}$.

The following propositions are true:

(37) $-z = (-\mathbf{1}_{\mathbb{H}_{\mathrm{R}}}) \cdot z$.

(38) $\overline{0_{\mathbb{H}_{\mathrm{R}}}} = 0_{\mathbb{H}_{\mathrm{R}}}$.

(39) If $\overline{z} = 0_{\mathbb{H}_{\mathrm{R}}}$, then $z = 0_{\mathbb{H}_{\mathrm{R}}}$.

(40) $\overline{1_{\mathbb{H}_{\mathrm{R}}}} = 1_{\mathbb{H}_{\mathrm{R}}}$.

(41) $|0_{\mathbb{H}_{\mathrm{R}}}| = 0$.

(42) If $|z| = 0$, then $z = 0_{\mathbb{H}_{\mathrm{R}}}$.

(43) $|1_{\mathbb{H}_{\mathrm{R}}}| = 1$.

(44) $(1_{\mathbb{H}_{\mathrm{R}}})^{-1} = 1_{\mathbb{H}_{\mathrm{R}}}$.

Let x, y be quaternion numbers. The functor $(x|y)$ yielding an element of $\mathbb{H}$ is defined as follows:

(Def. 13) $(x|y) = x \cdot \overline{y}$.

The following propositions are true:

(45) $(c_1|c_2) = \langle \Re(c_1) \cdot \Re(c_2) + \Im_1(c_1) \cdot \Im_1(c_2) + \Im_2(c_1) \cdot \Im_2(c_2) + \Im_3(c_1) \cdot \Im_3(c_2), ((\Re(c_1) \cdot -\Im_1(c_2) + \Im_1(c_1) \cdot \Re(c_2)) - \Im_2(c_1) \cdot \Im_3(c_2)) + \Im_3(c_1) \cdot \Im_2(c_2), ((\Re(c_1) \cdot -\Im_2(c_2) + \Re(c_2) \cdot \Im_2(c_1)) - \Im_1(c_2) \cdot \Im_3(c_1)) + \Im_3(c_2) \cdot \Im_1(c_1), ((\Re(c_1) \cdot -\Im_3(c_2) + \Im_3(c_1) \cdot \Re(c_2)) - \Im_1(c_1) \cdot \Im_2(c_2)) + \Im_2(c_1) \cdot \Im_1(c_2) \rangle_{\mathbb{H}}$.

(46) $(c|c) = |c|^{\mathbf{2}}$.

(47) $\Re((c|c)) = |c|^{\mathbf{2}}$ and $\Im_1((c|c)) = 0$ and $\Im_2((c|c)) = 0$ and $\Im_2((c|c)) = 0$.

(48) $|(c_1|c_2)| = |c_1| \cdot |c_2|$.

(49) If $(c|c) = 0$, then $c = 0$.

(50) $((c_1 + c_2)|c_3) = (c_1|c_3) + (c_2|c_3)$.

(51) $(c_1|(c_2 + c_3)) = (c_1|c_2) + (c_1|c_3)$.

(52) $((-c_1)|c_2) = -(c_1|c_2)$.

(53) $-(c_1|c_2) = (c_1|-c_2)$.

(54) $((-c_1)|-c_2) = (c_1|c_2)$.

(55) $((c_1 - c_2)|c_3) = (c_1|c_3) - (c_2|c_3)$.

(56) $(c_1|(c_2 - c_3)) = (c_1|c_2) - (c_1|c_3)$.

(57) $((c_1 + c_2)|(c_1 + c_2)) = (c_1|c_1) + (c_1|c_2) + (c_2|c_1) + (c_2|c_2)$.

(58) $((c_1 - c_2)|(c_1 - c_2)) = ((c_1|c_1) - (c_1|c_2) - (c_2|c_1)) + (c_2|c_2)$.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[2] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[4] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[5] Xiquan Liang and Fuguo Ge. The quaternion numbers. *Formalized Mathematics*, 14(**4**):161–169, 2006.

[6] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[7] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[8] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[9] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received March 18, 2008

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 141–145, 2008

Several Higher Differentiation Formulas of Special Functions

Junjie Zhao
Qingdao University of Science
and Technology
China

Xiquan Liang
Qingdao University of Science
and Technology
China

Li Yan
Qingdao University of Science
and Technology
China

Summary. In this paper, we proved some basic properties of higher differentiation, and higher differentiation formulas of special functions [4].

MML identifier: `HFDIFF_1`, version: `7.8.10 4.100.1011`

The notation and terminology used in this paper are introduced in the following articles: [16], [13], [2], [3], [5], [1], [7], [9], [12], [10], [8], [18], [14], [11], [6], [15], and [17].

For simplicity, we use the following convention: x, r, a, x_0, p are real numbers, n, i, m are elements of $\mathbb{N}$, Z is an open subset of $\mathbb{R}$, and f, f_1, f_2 are partial functions from $\mathbb{R}$ to $\mathbb{R}$.

Next we state a number of propositions:

(1) For every function f from $\mathbb{R}$ into $\mathbb{R}$ holds $\mathrm{dom}(f{\restriction}Z) = Z$.

(2) $(-f_1)\,-f_2 = f_1\,f_2$.

(3) If $n \geq 1$, then $\mathrm{dom}(\frac{1}{\square^n}) = \mathbb{R} \setminus \{0\}$ and $(\square^n)^{-1}(\{0\}) = \{0\}$.

(4) $(r \cdot p)\,\frac{1}{\square^n} = r\,(p\,\frac{1}{\square^n})$.

(5) For all elements n, m of $\mathbb{R}$ holds $n\,f + m\,f = (n+m)\,f$.

(6) If $f{\restriction}Z$ is differentiable on Z, then f is differentiable on Z.

ISSN 1426–2630(p), 1898-9934(e)

(7) If $n \geq 1$ and f is differentiable n times on Z, then f is differentiable on Z.

(8) $\square^n$ is differentiable on $\mathbb{R}$.

(9) If $x \in Z$, then (the function sin)$'(Z)(2)(x) = -\sin x$.

(10) If $x \in Z$, then (the function sin)$'(Z)(3)(x) = -\cos x$.

(11) If $x \in Z$, then (the function sin)$'(Z)(n)(x) = \sin(x + \frac{n \cdot \pi}{2})$.

(12) If $x \in Z$, then (the function cos)$'(Z)(2)(x) = -\cos x$.

(13) If $x \in Z$, then (the function cos)$'(Z)(3)(x) = \sin x$.

(14) If $x \in Z$, then (the function cos)$'(Z)(n)(x) = \cos(x + \frac{n \cdot \pi}{2})$.

(15) If f_1 is differentiable n times on Z and f_2 is differentiable n times on Z, then $(f_1 + f_2)'(Z)(n) = {f_1}'(Z)(n) + {f_2}'(Z)(n)$.

(16) If f_1 is differentiable n times on Z and f_2 is differentiable n times on Z, then $(f_1 - f_2)'(Z)(n) = {f_1}'(Z)(n) - {f_2}'(Z)(n)$.

(17) If f_1 is differentiable n times on Z and f_2 is differentiable n times on Z and $i \leq n$, then $(f_1 + f_2)'(Z)(i) = {f_1}'(Z)(i) + {f_2}'(Z)(i)$.

(18) If f_1 is differentiable n times on Z and f_2 is differentiable n times on Z and $i \leq n$, then $(f_1 - f_2)'(Z)(i) = {f_1}'(Z)(i) - {f_2}'(Z)(i)$.

(19) If f_1 is differentiable n times on Z and f_2 is differentiable n times on Z, then $f_1 + f_2$ is differentiable n times on Z.

(20) If f_1 is differentiable n times on Z and f_2 is differentiable n times on Z, then $f_1 - f_2$ is differentiable n times on Z.

(21) If f is differentiable n times on Z, then $(r\,f)'(Z)(n) = r\,f'(Z)(n)$.

(22) If f is differentiable n times on Z, then $r\,f$ is differentiable n times on Z.

(23) If f is differentiable on Z, then $f'(Z)(1) = f'_{\restriction Z}$.

(24) If $n \geq 1$ and f is differentiable n times on Z, then $f'(Z)(1) = f'_{\restriction Z}$.

(25) If $x \in Z$, then $(r\,$(the function sin)$)'(Z)(n)(x) = r \cdot \sin(x + \frac{n \cdot \pi}{2})$.

(26) If $x \in Z$, then $(r\,$(the function cos)$)'(Z)(n)(x) = r \cdot \cos(x + \frac{n \cdot \pi}{2})$.

(27) If $x \in Z$, then $(r\,$(the function exp)$)'(Z)(n)(x) = r \cdot \exp x$.

(28) $(\square^n)'_{\restriction Z} = (n\,(\square^{n-1}))\restriction Z$.

(29) If $x \neq 0$, then $\frac{1}{\square^n}$ is differentiable in x and $(\frac{1}{\square^n})'(x) = -\frac{n \cdot x^{n-1}}{(x^n)^{\mathbf{2}}}$.

(30) If $n \geq 1$, then $(\square^n)'(Z)(2) = ((n \cdot (n-1))\,(\square^{n-2}))\restriction Z$.

(31) If $n \geq 2$, then $(\square^n)'(Z)(3) = ((n \cdot (n-1) \cdot (n-2))\,(\square^{n-3}))\restriction Z$.

(32) If $n > m$, then $(\square^n)'(Z)(m) = ((\binom{n}{m} \cdot m!)\,(\square^{n-m}))\restriction Z$.

(33) If f is differentiable n times on Z, then $(-f)'(Z)(n) = -f'(Z)(n)$ and $-f$ is differentiable n times on Z.

(34) If $x_0 \in Z$, then (Taylor(the function sin$, Z, x_0, x$))$(n) =$

$\frac{\sin(x_0+\frac{n\cdot\pi}{2})\cdot(x-x_0)^n}{n!}$ and $(\mathrm{Taylor}(\text{the function cos}, Z, x_0, x))(n) = \frac{\cos(x_0+\frac{n\cdot\pi}{2})\cdot(x-x_0)^n}{n!}$.

(35) If $r > 0$, then $(\mathrm{Maclaurin}(\text{the function sin},]{-r}, r[, x))(n) = \frac{\sin(\frac{n\cdot\pi}{2})\cdot x^n}{n!}$ and $(\mathrm{Maclaurin}(\text{the function cos},]{-r}, r[, x))(n) = \frac{\cos(\frac{n\cdot\pi}{2})\cdot x^n}{n!}$.

(36) If $n > m$ and $x \in Z$, then $(\square^n)'(Z)(m)(x) = \binom{n}{m} \cdot m! \cdot x^{n-m}$.

(37) If $x \in Z$, then $(\square^m)'(Z)(m)(x) = m!$.

(38) $\square^n$ is differentiable n times on Z.

(39) If $x \in Z$ and $n > m$, then $(a\,(\square^n))'(Z)(m)(x) = a \cdot \binom{n}{m} \cdot m! \cdot x^{n-m}$.

(40) If $x \in Z$, then $(a\,(\square^n))'(Z)(n)(x) = a \cdot n!$.

(41) If $x_0 \in Z$ and $n > m$, then $(\mathrm{Taylor}(\square^n, Z, x_0, x))(m) = \binom{n}{m} \cdot {x_0}^{n-m} \cdot (x - x_0)^m$ and $(\mathrm{Taylor}(\square^n, Z, x_0, x))(n) = (x - x_0)^n$.

(42) Let n, m be elements of $\mathbb{N}$ and r, x be real numbers. If $n > m$ and $r > 0$, then $(\mathrm{Maclaurin}(\square^n,]{-r}, r[, x))(m) = 0$ and $(\mathrm{Maclaurin}(\square^n,]{-r}, r[, x))(n) = x^n$.

(43) $\frac{1}{\square^n}$ is differentiable on $]0, r[$.

(44) If $x_0 \in]0, r[$, then $(\frac{1}{\square^n})'_{\restriction]0,r[}(x_0) = -\frac{n}{(\square^{n+1})(x_0)}$.

(45) If $x \neq 0$, then $\frac{1}{\square^1}$ is differentiable in x and $(\frac{1}{\square^1})'(x) = -\frac{1}{(x^1)^{\mathbf{2}}}$.

(46) If $]0, r[\subseteq \mathrm{dom}(\frac{1}{\square^2})$, then $(\frac{1}{\square^1})'_{\restriction]0,r[} = ((-1)\,\frac{1}{\square^2}) \restriction]0, r[$.

(47) If $x \neq 0$, then $\frac{1}{\square^2}$ is differentiable in x and $(\frac{1}{\square^2})'(x) = -\frac{2\cdot x^1}{(x^2)^{\mathbf{2}}}$.

(48) If $]0, r[\subseteq \mathrm{dom}(\frac{1}{\square^3})$, then $(\frac{1}{\square^2})'_{\restriction]0,r[} = ((-2)\,\frac{1}{\square^3}) \restriction]0, r[$.

(49) If $n \geq 1$, then $(\frac{1}{\square^n})'_{\restriction]0,r[} = ((-n)\,\frac{1}{\square^{n+1}}) \restriction]0, r[$.

(50) Suppose f_1 is differentiable 2 times on Z and f_2 is differentiable 2 times on Z. Then $(f_1\,f_2)'(Z)(2) = {f_1}'(Z)(2)\,f_2 + 2\,((f_1)'_{\restriction Z}\,(f_2)'_{\restriction Z}) + f_1\,{f_2}'(Z)(2)$.

(51) If $Z \subseteq \mathrm{dom}\,(\text{the function ln})$ and $Z \subseteq \mathrm{dom}(\frac{1}{\square^1})$, then $(\text{the function ln})'_{\restriction Z} = \frac{1}{\square^1} \restriction Z$.

(52) If $n \geq 1$ and $x_0 \in]0, r[$, then $(\frac{1}{\square^n})'(]0, r[)(2)(x_0) = n\cdot(n+1)\cdot(\frac{1}{\square^{n+2}})(x_0)$.

(53) ((The function sin) (the function sin))$'(Z)(2) = 2\,(((\text{the function cos})\ (\text{the function cos})) \restriction Z) + (-2)\,(((\text{the function sin})\ (\text{the function sin})) \restriction Z)$.

(54) ((The function cos) (the function cos))$'(Z)(2) = 2\,(((\text{the function sin})\ (\text{the function sin})) \restriction Z) + (-2)\,(((\text{the function cos})\ (\text{the function cos})) \restriction Z)$.

(55) ((The function sin) (the function cos))$'(Z)(2) =$
$4\,(((-\text{the function sin})\,(\text{the function cos})) \restriction Z)$.

(56) Suppose $Z \subseteq \mathrm{dom}\,(\text{the function tan})$. Then the function tan is differentiable on Z and $(\text{the function tan})'_{\restriction Z} = (\frac{1}{\text{the function cos}}\ \frac{1}{\text{the function cos}}) \restriction Z$.

(57) Suppose $Z \subseteq \mathrm{dom}\,(\text{the function tan})$. Then $\frac{1}{\text{the function cos}}$ is differentiable on Z and $(\frac{1}{\text{the function cos}})'_{\restriction Z} = (\frac{1}{\text{the function cos}}\ (\text{the function tan})) \restriction Z$.

(58) Suppose $Z \subseteq \mathrm{dom}\,(\text{the function tan})$. Then $(\text{the function tan})'(Z)(2) = 2\,(((\text{the function tan})\ \frac{1}{\text{the function cos}}\ \frac{1}{\text{the function cos}}) \restriction Z)$.

(59) Suppose $Z \subseteq \mathrm{dom}\,(\text{the function cot})$. Then

(i) the function cot is differentiable on Z, and

(ii) $(\text{the function cot})'_{\restriction Z} = ((-1)\,(\frac{1}{\text{the function sin}}\ \frac{1}{\text{the function sin}})) \restriction Z$.

(60) Suppose $Z \subseteq \mathrm{dom}\,(\text{the function cot})$. Then

(i) $\frac{1}{\text{the function sin}}$ is differentiable on Z, and

(ii) $(\frac{1}{\text{the function sin}})'_{\restriction Z} = (-\frac{1}{\text{the function sin}}\ (\text{the function cot})) \restriction Z$.

(61) Suppose $Z \subseteq \mathrm{dom}\,(\text{the function cot})$. Then $(\text{the function cot})'(Z)(2) = 2\,(((\text{the function cot})\ \frac{1}{\text{the function sin}}\ \frac{1}{\text{the function sin}}) \restriction Z)$.

(62) $((\text{The function exp})\ (\text{the function sin}))'(Z)(2) = 2\,(((\text{the function exp})\ (\text{the function cos})) \restriction Z)$.

(63) $((\text{The function exp})\ (\text{the function cos}))'(Z)(2) = 2\,(((\text{the function exp})\ {-\text{the function sin}}) \restriction Z)$.

(64) Suppose f_1 is differentiable 3 times on Z and f_2 is differentiable 3 times on Z. Then $(f_1\,f_2)'(Z)(3) = f_1{}'(Z)(3)\,f_2 + (3\,(f_1{}'(Z)(2)\,(f_2)'_{\restriction Z}) + 3\,((f_1)'_{\restriction Z}\,f_2{}'(Z)(2))) + f_1\,f_2{}'(Z)(3)$.

(65) $((\text{The function sin})\ (\text{the function sin}))'(Z)(3) = (-8)\,(((\text{the function cos})\ (\text{the function sin})) \restriction Z)$.

(66) If f is differentiable 2 times on Z, then $(f\,f)'(Z)(2) = 2\,(f\,f'(Z)(2)) + 2\,(f'_{\restriction Z}\,f'_{\restriction Z})$.

(67) Suppose f is differentiable 2 times on Z and for every x_0 such that $x_0 \in Z$ holds $f(x_0) \neq 0$. Then $(\frac{1}{f})'(Z)(2) = \frac{2\,f'_{\restriction Z}\,f'_{\restriction Z} - f'(Z)(2)\,f}{f\,(f\,f)}$.

(68) $((\text{The function exp})\ (\text{the function sin}))'(Z)(3) = (2\,((\text{the function exp})\ (-\text{the function sin} + \text{the function cos}))) \restriction Z$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

[3] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[4] Chuanzhang Chen. *Mathematical Analysis.* Higher Education Press, Beijing, 1978.

[5] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[6] Jarosław Kotowicz. Partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 1(**4**):703–709, 1990.

[7] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[8] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[9] Akira Nishino and Yasunari Shidama. The Maclaurin expansions. *Formalized Mathematics*, 13(**3**):421–425, 2005.

[10] Beata Perkowska. Functional sequence from a domain to a domain. *Formalized Mathematics*, 3(**1**):17–21, 1992.

[11] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

[12] Konrad Raczkowski and Paweł Sadowski. Real function differentiability. *Formalized Mathematics*, 1(**4**):797–801, 1990.

[13] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.

[14] Yasunari Shidama. The Taylor expansions. *Formalized Mathematics*, 12(**2**):195–200, 2004.

[15] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[16] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[17] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[18] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

Received March 18, 2008

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 147–158, 2008

Inverse Trigonometric Functions Arctan and Arccot

Xiqcuan Liang
Qingdao University of Science and Technology
China

Bing Xie
Qingdao University of Science and Technology
China

Summary. This article describes definitions of inverse trigonometric functions arctan, arccot and their main properties, as well as several differentiation formulas of arctan and arccot.

MML identifier: `SIN_COS9`, version: `7.8.10 4.100.1011`

The articles [17], [1], [2], [18], [3], [13], [19], [7], [15], [5], [9], [12], [16], [4], [6], [8], [11], [14], and [10] provide the notation and terminology for this paper.

1. Function Arctan and Arccot

For simplicity, we adopt the following convention: x, r, s, h denote real numbers, n denotes an element of $\mathbb{N}$, Z denotes an open subset of $\mathbb{R}$, and f, f_1, f_2 denote partial functions from $\mathbb{R}$ to $\mathbb{R}$.

The following propositions are true:

(1) $]-\frac{\pi}{2}, \frac{\pi}{2}[\subseteq \mathrm{dom}$ (the function tan).

(2) $]0, \pi[\subseteq \mathrm{dom}$ (the function cot).

(3)(i) The function tan is differentiable on $]-\frac{\pi}{2}, \frac{\pi}{2}[$, and

(ii) for every x such that $x \in]-\frac{\pi}{2}, \frac{\pi}{2}[$ holds (the function tan)$'(x) = \frac{1}{(\cos x)^{\mathbf{2}}}$.

(4) The function cot is differentiable on $]0, \pi[$ and for every x such that $x \in]0, \pi[$ holds (the function cot)$'(x) = -\frac{1}{(\sin x)^{\mathbf{2}}}$.

(5) The function tan is continuous on $]-\frac{\pi}{2}, \frac{\pi}{2}[$.

(6) The function cot is continuous on $]0, \pi[$.

ISSN 1426–2630(p), 1898-9934(e)

(7) The function tan is increasing on $]-\frac{\pi}{2}, \frac{\pi}{2}[$.

(8) The function cot is decreasing on $]0, \pi[$.

(9) (The function tan)$\restriction]-\frac{\pi}{2}, \frac{\pi}{2}[$ is one-to-one.

(10) (The function cot)$\restriction]0, \pi[$ is one-to-one.

Let us mention that (the function tan)$\restriction]-\frac{\pi}{2}, \frac{\pi}{2}[$ is one-to-one and (the function cot)$\restriction]0, \pi[$ is one-to-one.

The partial function the function arctan from $\mathbb{R}$ to $\mathbb{R}$ is defined as follows:

(Def. 1) The function arctan $=$ ((the function tan)$\restriction]-\frac{\pi}{2}, \frac{\pi}{2}[)^{-1}$.

The partial function the function arccot from $\mathbb{R}$ to $\mathbb{R}$ is defined by:

(Def. 2) The function arccot $=$ ((the function cot)$\restriction]0, \pi[)^{-1}$.

Let r be a real number. The functor $\operatorname{arctan} r$ is defined by:

(Def. 3) $\operatorname{arctan} r =$ (the function arctan)(r).

The functor $\operatorname{arccot} r$ is defined by:

(Def. 4) $\operatorname{arccot} r =$ (the function arccot)(r).

Let r be a real number. Then $\operatorname{arctan} r$ is a real number. Then $\operatorname{arccot} r$ is a real number.

We now state two propositions:

(11) rng (the function arctan) $=]-\frac{\pi}{2}, \frac{\pi}{2}[$.

(12) rng (the function arccot) $=]0, \pi[$.

Let us mention that the function arctan is one-to-one and the function arccot is one-to-one.

Let r be a real number. Then $\tan r$ is a real number. Then $\cot r$ is a real number.

Next we state a number of propositions:

(13) For every real number x such that $x \in]-\frac{\pi}{2}, \frac{\pi}{2}[$ holds (the function tan)$(x) = \tan x$.

(14) For every real number x such that $x \in]0, \pi[$ holds (the function cot)$(x) = \cot x$.

(15) For every real number x such that $\cos x \neq 0$ holds (the function tan)$(x) = \tan x$.

(16) For every real number x such that (the function sin)$(x) \neq 0$ holds (the function cot)$(x) = \cot x$.

(17) $\tan(-\frac{\pi}{4}) = -1$.

(18) $\cot(\frac{\pi}{4}) = 1$ and $\cot(\frac{3}{4} \cdot \pi) = -1$.

(19) For every real number x such that $x \in [-\frac{\pi}{4}, \frac{\pi}{4}]$ holds $\tan x \in [-1, 1]$.

(20) For every real number x such that $x \in [\frac{\pi}{4}, \frac{3}{4} \cdot \pi]$ holds $\cot x \in [-1, 1]$.

(21) rng((the function tan)$\restriction[-\frac{\pi}{4}, \frac{\pi}{4}]) = [-1, 1]$.

(22) rng((the function cot)$\restriction[\frac{\pi}{4}, \frac{3}{4} \cdot \pi]) = [-1, 1]$.

(23) $[-1, 1] \subseteq \mathrm{dom}\,$(the function arctan).

(24) $[-1, 1] \subseteq \mathrm{dom}\,$(the function arccot).

Let us observe that (the function tan)$\upharpoonright[-\frac{\pi}{4}, \frac{\pi}{4}]$ is one-to-one and (the function cot)$\upharpoonright[\frac{\pi}{4}, \frac{3}{4} \cdot \pi]$ is one-to-one.

The following propositions are true:

(25) (The function arctan)$\upharpoonright[-1, 1] =$ ((the function tan)$\upharpoonright[-\frac{\pi}{4}, \frac{\pi}{4}])^{-1}$.

(26) (The function arccot)$\upharpoonright[-1, 1] =$ ((the function cot)$\upharpoonright[\frac{\pi}{4}, \frac{3}{4} \cdot \pi])^{-1}$.

(27) ((The function tan)$\upharpoonright[-\frac{\pi}{4}, \frac{\pi}{4}]$ **qua** function) $\cdot$((the function arctan)$\upharpoonright[-1, 1]) = \mathrm{id}_{[-1,1]}$.

(28) ((The function cot)$\upharpoonright[\frac{\pi}{4}, \frac{3}{4}{\cdot}\pi]$ **qua** function) $\cdot$((the function arccot)$\upharpoonright[-1, 1]) = \mathrm{id}_{[-1,1]}$.

(29) ((The function tan)$\upharpoonright[-\frac{\pi}{4}, \frac{\pi}{4}]) \cdot$ ((the function arctan)$\upharpoonright[-1, 1]) = \mathrm{id}_{[-1,1]}$.

(30) ((The function cot)$\upharpoonright[\frac{\pi}{4}, \frac{3}{4} \cdot \pi]) \cdot$ ((the function arccot)$\upharpoonright[-1, 1]) = \mathrm{id}_{[-1,1]}$.

(31) (The function arctan **qua** function) $\cdot$((the function tan)$\upharpoonright]-\frac{\pi}{2}, \frac{\pi}{2}[) = \mathrm{id}_{]-\frac{\pi}{2},\frac{\pi}{2}[}$.

(32) (The function arccot) $\cdot$((the function cot)$\upharpoonright]0, \pi[) = \mathrm{id}_{]0,\pi[}$.

(33) (The function arctan **qua** function) $\cdot$((the function tan)$\upharpoonright]-\frac{\pi}{2}, \frac{\pi}{2}[) = \mathrm{id}_{]-\frac{\pi}{2},\frac{\pi}{2}[}$.

(34) (The function arccot **qua** function) $\cdot$((the function cot)$\upharpoonright]0, \pi[) = \mathrm{id}_{]0,\pi[}$.

(35) If $-\frac{\pi}{2} < r < \frac{\pi}{2}$, then $\arctan \tan r = r$.

(36) If $0 < r < \pi$, then $\mathrm{arccot} \cot r = r$.

(37) $\arctan(-1) = -\frac{\pi}{4}$.

(38) $\mathrm{arccot}(-1) = \frac{3}{4} \cdot \pi$.

(39) $\arctan 1 = \frac{\pi}{4}$.

(40) $\mathrm{arccot}\, 1 = \frac{\pi}{4}$.

(41) $\tan 0 = 0$.

(42) $\cot(\frac{\pi}{2}) = 0$.

(43) $\arctan 0 = 0$.

(44) $\mathrm{arccot}\, 0 = \frac{\pi}{2}$.

(45) The function arctan is increasing on (the function tan) $^{\circ}]-\frac{\pi}{2}, \frac{\pi}{2}[$.

(46) The function arccot is decreasing on (the function cot) $^{\circ}]0, \pi[$.

(47) The function arctan is increasing on $[-1, 1]$.

(48) The function arccot is decreasing on $[-1, 1]$.

(49) For every real number x such that $x \in [-1, 1]$ holds $\arctan x \in [-\frac{\pi}{4}, \frac{\pi}{4}]$.

(50) For every real number x such that $x \in [-1, 1]$ holds $\mathrm{arccot}\, x \in [\frac{\pi}{4}, \frac{3}{4} \cdot \pi]$.

(51) If $-1 \leq r \leq 1$, then $\tan \arctan r = r$.

(52) If $-1 \leq r \leq 1$, then $\cot \mathrm{arccot}\, r = r$.

(53) The function arctan is continuous on $[-1,1]$.

(54) The function arccot is continuous on $[-1,1]$.

(55) $\mathrm{rng}((\text{the function arctan})\restriction[-1,1]) = [-\frac{\pi}{4},\frac{\pi}{4}]$.

(56) $\mathrm{rng}((\text{the function arccot})\restriction[-1,1]) = [\frac{\pi}{4},\frac{3}{4}\cdot\pi]$.

(57) If $-1 \leq r \leq 1$ and $\arctan r = -\frac{\pi}{4}$, then $r = -1$.

(58) If $-1 \leq r \leq 1$ and $\mathrm{arccot}\, r = \frac{3}{4}\cdot\pi$, then $r = -1$.

(59) If $-1 \leq r \leq 1$ and $\arctan r = 0$, then $r = 0$.

(60) If $-1 \leq r \leq 1$ and $\mathrm{arccot}\, r = \frac{\pi}{2}$, then $r = 0$.

(61) If $-1 \leq r \leq 1$ and $\arctan r = \frac{\pi}{4}$, then $r = 1$.

(62) If $-1 \leq r \leq 1$ and $\mathrm{arccot}\, r = \frac{\pi}{4}$, then $r = 1$.

(63) If $-1 \leq r \leq 1$, then $-\frac{\pi}{4} \leq \arctan r \leq \frac{\pi}{4}$.

(64) If $-1 \leq r \leq 1$, then $\frac{\pi}{4} \leq \mathrm{arccot}\, r \leq \frac{3}{4}\cdot\pi$.

(65) If $-1 < r < 1$, then $-\frac{\pi}{4} < \arctan r < \frac{\pi}{4}$.

(66) If $-1 < r < 1$, then $\frac{\pi}{4} < \mathrm{arccot}\, r < \frac{3}{4}\cdot\pi$.

(67) If $-1 \leq r \leq 1$, then $\arctan r = -\arctan(-r)$.

(68) If $-1 \leq r \leq 1$, then $\mathrm{arccot}\, r = \pi - \mathrm{arccot}(-r)$.

(69) If $-1 \leq r \leq 1$, then $\cot \arctan r = \frac{1}{r}$.

(70) If $-1 \leq r \leq 1$, then $\tan \mathrm{arccot}\, r = \frac{1}{r}$.

(71) The function arctan is differentiable on (the function tan) $^\circ]-\frac{\pi}{2},\frac{\pi}{2}[$.

(72) The function arccot is differentiable on (the function cot) $^\circ]0,\pi[$.

(73) The function arctan is differentiable on $]-1,1[$.

(74) The function arccot is differentiable on $]-1,1[$.

(75) If $-1 \leq r \leq 1$, then (the function arctan)$'(r) = \frac{1}{1+r^{\mathbf{2}}}$.

(76) If $-1 \leq r \leq 1$, then (the function arccot)$'(r) = -\frac{1}{1+r^{\mathbf{2}}}$.

(77) The function arctan is continuous on (the function tan) $^\circ]-\frac{\pi}{2},\frac{\pi}{2}[$.

(78) The function arccot is continuous on (the function cot) $^\circ]0,\pi[$.

(79) dom (the function arctan) is open.

(80) dom (the function arccot) is open.

2. Several Differentiation Formulas of Arctan and Arccot

We now state a number of propositions:

(81) Suppose $Z \subseteq]-1,1[$. Then the function arctan is differentiable on Z and for every x such that $x \in Z$ holds (the function arctan)$'_{\restriction Z}(x) = \frac{1}{1+x^{\mathbf{2}}}$.

(82) Suppose $Z \subseteq]-1,1[$. Then the function arccot is differentiable on Z and for every x such that $x \in Z$ holds (the function arccot)$'_{\restriction Z}(x) = -\frac{1}{1+x^{\mathbf{2}}}$.

(83) Suppose $Z \subseteq]-1,1[$. Then

(i) r the function arctan is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(r$ the function arctan$)'_{\restriction Z}(x) = \frac{r}{1+x^{\mathbf{2}}}$.

(84) Suppose $Z \subseteq]-1,1[$. Then

(i) r the function arccot is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(r$ the function arccot$)'_{\restriction Z}(x) = -\frac{r}{1+x^{\mathbf{2}}}$.

(85) Suppose f is differentiable in x and $-1 < f(x) < 1$. Then (the function arctan) $\cdot f$ is differentiable in x and ((the function arctan) $\cdot f)'(x) = \frac{f'(x)}{1+f(x)^{\mathbf{2}}}$.

(86) Suppose f is differentiable in x and $-1 < f(x) < 1$. Then (the function arccot) $\cdot f$ is differentiable in x and ((the function arccot) $\cdot f)'(x) = -\frac{f'(x)}{1+f(x)^{\mathbf{2}}}$.

(87) Suppose $Z \subseteq$ dom((the function arctan) $\cdot f$) and for every x such that $x \in Z$ holds $f(x) = r \cdot x + s$ and $-1 < f(x) < 1$. Then

(i) (the function arctan) $\cdot f$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function arctan) $\cdot f)'_{\restriction Z}(x) = \frac{r}{1+(r \cdot x+s)^{\mathbf{2}}}$.

(88) Suppose $Z \subseteq$ dom((the function arccot) $\cdot f$) and for every x such that $x \in Z$ holds $f(x) = r \cdot x + s$ and $-1 < f(x) < 1$. Then

(i) (the function arccot) $\cdot f$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function arccot) $\cdot f)'_{\restriction Z}(x) = -\frac{r}{1+(r \cdot x+s)^{\mathbf{2}}}$.

(89) Suppose $Z \subseteq$ dom((the function ln) $\cdot$(the function arctan)) and $Z \subseteq]-1,1[$ and for every x such that $x \in Z$ holds $\arctan x > 0$. Then

(i) (the function ln) $\cdot$(the function arctan) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function ln) $\cdot$(the function arctan))$'_{\restriction Z}(x) = \frac{1}{(1+x^{\mathbf{2}}) \cdot \arctan x}$.

(90) Suppose $Z \subseteq$ dom((the function ln) $\cdot$(the function arccot)) and $Z \subseteq]-1,1[$ and for every x such that $x \in Z$ holds $\operatorname{arccot} x > 0$. Then

(i) (the function ln) $\cdot$(the function arccot) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function ln) $\cdot$(the function arccot))$'_{\restriction Z}(x) = -\frac{1}{(1+x^{\mathbf{2}}) \cdot \operatorname{arccot} x}$.

(91) Suppose $Z \subseteq$ dom(($\square^n$) $\cdot$ the function arctan) and $Z \subseteq]-1,1[$. Then

(i) ($\square^n$) $\cdot$ the function arctan is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds (($\square^n$) $\cdot$ the function arctan)$'_{\restriction Z}(x) = \frac{n \cdot (\arctan x)^{n-1}}{1+x^{\mathbf{2}}}$.

(92) Suppose $Z \subseteq$ dom(($\square^n$) $\cdot$ the function arccot) and $Z \subseteq]-1,1[$. Then

(i) ($\square^n$) $\cdot$ the function arccot is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\square^{n}) \cdot \text{the function arccot})'_{\restriction Z}(x) = -\frac{n \cdot (\operatorname{arccot} x)^{n-1}}{1+x^{\mathbf{2}}}$.

(93) Suppose $Z \subseteq \operatorname{dom}(\frac{1}{2}\,((\square^{2}) \cdot \text{the function arctan}))$ and $Z \subseteq]-1,1[$. Then

(i) $\frac{1}{2}\,((\square^{2}) \cdot \text{the function arctan})$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{1}{2}\,((\square^{2}) \cdot \text{the function arctan}))'_{\restriction Z}(x) = \frac{\arctan x}{1+x^{\mathbf{2}}}$.

(94) Suppose $Z \subseteq \operatorname{dom}(\frac{1}{2}\,((\square^{2}) \cdot \text{the function arccot}))$ and $Z \subseteq]-1,1[$. Then

(i) $\frac{1}{2}\,((\square^{2}) \cdot \text{the function arccot})$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{1}{2}\,((\square^{2}) \cdot \text{the function arccot}))'_{\restriction Z}(x) = -\frac{\operatorname{arccot} x}{1+x^{\mathbf{2}}}$.

(95) Suppose $Z \subseteq]-1,1[$. Then

(i) id_{Z} the function arctan is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\mathrm{id}_{Z}\,\text{the function arctan})'_{\restriction Z}(x) = \arctan x + \frac{x}{1+x^{\mathbf{2}}}$.

(96) Suppose $Z \subseteq]-1,1[$. Then

(i) id_{Z} the function arccot is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\mathrm{id}_{Z}\,\text{the function arccot})'_{\restriction Z}(x) = \operatorname{arccot} x - \frac{x}{1+x^{\mathbf{2}}}$.

(97) Suppose $Z \subseteq \operatorname{dom}(f\,\text{the function arctan})$ and $Z \subseteq]-1,1[$ and for every x such that $x \in Z$ holds $f(x) = r \cdot x + s$. Then

(i) f the function arctan is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(f\,\text{the function arctan})'_{\restriction Z}(x) = r \cdot \arctan x + \frac{r \cdot x+s}{1+x^{\mathbf{2}}}$.

(98) Suppose $Z \subseteq \operatorname{dom}(f\,\text{the function arccot})$ and $Z \subseteq]-1,1[$ and for every x such that $x \in Z$ holds $f(x) = r \cdot x + s$. Then

(i) f the function arccot is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(f\,\text{the function arccot})'_{\restriction Z}(x) = r \cdot \operatorname{arccot} x - \frac{r \cdot x+s}{1+x^{\mathbf{2}}}$.

(99) Suppose $Z \subseteq \operatorname{dom}(\frac{1}{2}\,((\text{the function arctan}) \cdot f))$ and for every x such that $x \in Z$ holds $f(x) = 2 \cdot x$ and $-1 < f(x) < 1$. Then

(i) $\frac{1}{2}\,((\text{the function arctan}) \cdot f)$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{1}{2}\,((\text{the function arctan}) \cdot f))'_{\restriction Z}(x) = \frac{1}{1+(2 \cdot x)^{\mathbf{2}}}$.

(100) Suppose $Z \subseteq \operatorname{dom}(\frac{1}{2}\,((\text{the function arccot}) \cdot f))$ and for every x such that $x \in Z$ holds $f(x) = 2 \cdot x$ and $-1 < f(x) < 1$. Then

(i) $\frac{1}{2}\,((\text{the function arccot}) \cdot f)$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{1}{2}\,((\text{the function arccot}) \cdot f))'_{\restriction Z}(x) = -\frac{1}{1+(2 \cdot x)^{\mathbf{2}}}$.

(101) Suppose $Z \subseteq \operatorname{dom}(f_1 + f_2)$ and for every x such that $x \in Z$ holds $f_1(x) = 1$ and $f_2 = \square^{2}$. Then $f_1 + f_2$ is differentiable on Z and for every

x such that $x \in Z$ holds $(f_1 + f_2)'_{\restriction Z}(x) = 2 \cdot x$.

(102) Suppose $Z \subseteq \mathrm{dom}(\frac{1}{2}\,((\text{the function ln}) \cdot (f_1 + f_2)))$ and $f_2 = \square^2$ and for every x such that $x \in Z$ holds $f_1(x) = 1$. Then

(i) $\frac{1}{2}\,((\text{the function ln}) \cdot (f_1 + f_2))$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{1}{2}\,((\text{the function ln}) \cdot (f_1 + f_2)))'_{\restriction Z}(x) = \frac{x}{1+x^{\mathbf{2}}}$.

(103) Suppose that

(i) $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,\text{the function arctan}-\frac{1}{2}\,((\text{the function ln}) \cdot (f_1 + f_2)))$,

(ii) $Z \subseteq \,]-1, 1[$,

(iii) $f_2 = \square^2$, and

(iv) for every x such that $x \in Z$ holds $f_1(x) = 1$.

Then

(v) $\mathrm{id}_Z\,\text{the function arctan}-\frac{1}{2}\,((\text{the function ln}) \cdot (f_1 + f_2))$ is differentiable on Z, and

(vi) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,\text{the function arctan}-\frac{1}{2}\,((\text{the function ln}) \cdot (f_1 + f_2)))'_{\restriction Z}(x) = \arctan x$.

(104) Suppose that

(i) $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,\text{the function arccot}+\frac{1}{2}\,((\text{the function ln}) \cdot (f_1 + f_2)))$,

(ii) $Z \subseteq \,]-1, 1[$,

(iii) $f_2 = \square^2$, and

(iv) for every x such that $x \in Z$ holds $f_1(x) = 1$.

Then

(v) $\mathrm{id}_Z\,\text{the function arccot}+\frac{1}{2}\,((\text{the function ln}) \cdot (f_1 + f_2))$ is differentiable on Z, and

(vi) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,\text{the function arccot}+\frac{1}{2}\,((\text{the function ln}) \cdot (f_1 + f_2)))'_{\restriction Z}(x) = \mathrm{arccot}\, x$.

(105) Suppose $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,((\text{the function arctan}) \cdot f))$ and for every x such that $x \in Z$ holds $f(x) = \frac{x}{r}$ and $-1 < f(x) < 1$. Then

(i) $\mathrm{id}_Z\,((\text{the function arctan}) \cdot f)$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,((\text{the function arctan}) \cdot f))'_{\restriction Z}(x) = \arctan(\frac{x}{r}) + \frac{x}{r \cdot (1+(\frac{x}{r})^{\mathbf{2}})}$.

(106) Suppose $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,((\text{the function arccot}) \cdot f))$ and for every x such that $x \in Z$ holds $f(x) = \frac{x}{r}$ and $-1 < f(x) < 1$. Then

(i) $\mathrm{id}_Z\,((\text{the function arccot}) \cdot f)$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,((\text{the function arccot}) \cdot f))'_{\restriction Z}(x) = \mathrm{arccot}(\frac{x}{r}) - \frac{x}{r \cdot (1+(\frac{x}{r})^{\mathbf{2}})}$.

(107) Suppose $Z \subseteq \mathrm{dom}(f_1 + f_2)$ and for every x such that $x \in Z$ holds $f_1(x) = 1$ and $f_2 = (\square^2) \cdot f$ and for every x such that $x \in Z$ holds $f(x) = \frac{x}{r}$. Then $f_1 + f_2$ is differentiable on Z and for every x such that $x \in Z$ holds $(f_1 + f_2)'_{\restriction Z}(x) = \frac{2 \cdot x}{r^{\mathbf{2}}}$.

(108) Suppose that

(i) $Z \subseteq \mathrm{dom}(\frac{r}{2}\,((\text{the function ln})\cdot(f_1+f_2)))$,

(ii) for every x such that $x \in Z$ holds $f_1(x) = 1$,

(iii) $r \neq 0$,

(iv) $f_2 = (\square^2)\cdot f$, and

(v) for every x such that $x \in Z$ holds $f(x) = \frac{x}{r}$.

Then

(vi) $\frac{r}{2}\,((\text{the function ln})\cdot(f_1+f_2))$ is differentiable on Z, and

(vii) for every x such that $x \in Z$ holds $(\frac{r}{2}\,((\text{the function ln})\cdot(f_1+f_2)))'_{\restriction Z}(x) = \frac{x}{r\cdot(1+(\frac{x}{r})^{\mathbf{2}})}$.

(109) Suppose that

(i) $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,((\text{the function arctan})\cdot f) - \frac{r}{2}\,((\text{the function ln})\cdot(f_1+f_2)))$,

(ii) $r \neq 0$,

(iii) for every x such that $x \in Z$ holds $f(x) = \frac{x}{r}$ and $-1 < f(x) < 1$,

(iv) for every x such that $x \in Z$ holds $f_1(x) = 1$,

(v) $f_2 = (\square^2)\cdot f$, and

(vi) for every x such that $x \in Z$ holds $f(x) = \frac{x}{r}$.

Then

(vii) $\mathrm{id}_Z\,((\text{the function arctan})\cdot f) - \frac{r}{2}\,((\text{the function ln})\cdot(f_1+f_2))$ is differentiable on Z, and

(viii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,((\text{the function arctan})\cdot f) - \frac{r}{2}\,((\text{the function ln})\cdot(f_1+f_2)))'_{\restriction Z}(x) = \arctan(\frac{x}{r})$.

(110) Suppose that

(i) $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,((\text{the function arccot})\cdot f) + \frac{r}{2}\,((\text{the function ln})\cdot(f_1+f_2)))$,

(ii) $r \neq 0$,

(iii) for every x such that $x \in Z$ holds $f(x) = \frac{x}{r}$ and $-1 < f(x) < 1$,

(iv) for every x such that $x \in Z$ holds $f_1(x) = 1$,

(v) $f_2 = (\square^2)\cdot f$, and

(vi) for every x such that $x \in Z$ holds $f(x) = \frac{x}{r}$.

Then

(vii) $\mathrm{id}_Z\,((\text{the function arccot})\cdot f) + \frac{r}{2}\,((\text{the function ln})\cdot(f_1+f_2))$ is differentiable on Z, and

(viii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,((\text{the function arccot})\cdot f) + \frac{r}{2}\,((\text{the function ln})\cdot(f_1+f_2)))'_{\restriction Z}(x) = \mathrm{arccot}(\frac{x}{r})$.

(111) Suppose $Z \subseteq \mathrm{dom}((\text{the function arctan})\cdot\frac{1}{f})$ and for every x such that $x \in Z$ holds $f(x) = x$ and $-1 < (\frac{1}{f})(x) < 1$. Then

(i) $(\text{the function arctan})\cdot\frac{1}{f}$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\text{the function arctan})\cdot\frac{1}{f})'_{\restriction Z}(x) = -\frac{1}{1+x^{\mathbf{2}}}$.

(112) Suppose $Z \subseteq \mathrm{dom}((\text{the function arccot}) \cdot \frac{1}{f})$ and for every x such that $x \in Z$ holds $f(x) = x$ and $-1 < (\frac{1}{f})(x) < 1$. Then

(i) (the function arccot) $\cdot \frac{1}{f}$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\text{the function arccot}) \cdot \frac{1}{f})'_{\restriction Z}(x) = \frac{1}{1+x^{\mathbf{2}}}$.

(113) Suppose that

(i) $Z \subseteq \mathrm{dom}((\text{the function arctan}) \cdot f)$,

(ii) $f = f_1 + h\, f_2$,

(iii) for every x such that $x \in Z$ holds $-1 < f(x) < 1$,

(iv) for every x such that $x \in Z$ holds $f_1(x) = r + s \cdot x$, and

(v) $f_2 = \square^2$.

Then

(vi) (the function arctan) $\cdot(f_1 + h\, f_2)$ is differentiable on Z, and

(vii) for every x such that $x \in Z$ holds $((\text{the function arctan}) \cdot (f_1 + h\, f_2))'_{\restriction Z}(x) = \frac{s+2 \cdot h \cdot x}{1+(r+s \cdot x+h \cdot x^{\mathbf{2}})^{\mathbf{2}}}$.

(114) Suppose that

(i) $Z \subseteq \mathrm{dom}((\text{the function arccot}) \cdot f)$,

(ii) $f = f_1 + h\, f_2$,

(iii) for every x such that $x \in Z$ holds $-1 < f(x) < 1$,

(iv) for every x such that $x \in Z$ holds $f_1(x) = r + s \cdot x$, and

(v) $f_2 = \square^2$.

Then

(vi) (the function arccot) $\cdot(f_1 + h\, f_2)$ is differentiable on Z, and

(vii) for every x such that $x \in Z$ holds $((\text{the function arccot}) \cdot (f_1 + h\, f_2))'_{\restriction Z}(x) = -\frac{s+2 \cdot h \cdot x}{1+(r+s \cdot x+h \cdot x^{\mathbf{2}})^{\mathbf{2}}}$.

(115) Suppose $Z \subseteq \mathrm{dom}((\text{the function arctan}) \cdot (\text{the function exp}))$ and for every x such that $x \in Z$ holds $\exp x < 1$. Then

(i) (the function arctan) $\cdot$(the function exp) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\text{the function arctan}) \cdot (\text{the function exp}))'_{\restriction Z}(x) = \frac{\exp x}{1+(\exp x)^{\mathbf{2}}}$.

(116) Suppose $Z \subseteq \mathrm{dom}((\text{the function arccot}) \cdot (\text{the function exp}))$ and for every x such that $x \in Z$ holds $\exp x < 1$. Then

(i) (the function arccot) $\cdot$(the function exp) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\text{the function arccot}) \cdot (\text{the function exp}))'_{\restriction Z}(x) = -\frac{\exp x}{1+(\exp x)^{\mathbf{2}}}$.

(117) Suppose that

(i) $Z \subseteq \mathrm{dom}((\text{the function arctan}) \cdot (\text{the function ln}))$, and

(ii) for every x such that $x \in Z$ holds $-1 <$ (the function ln)(x) and (the function ln)$(x) < 1$.

Then

(iii) (the function arctan) $\cdot$(the function ln) is differentiable on Z, and

(iv) for every x such that $x \in Z$ holds ((the function arctan) $\cdot$(the function ln))$'_{\restriction Z}(x) = \frac{1}{x\cdot(1+(\text{the function ln})(x)^{\mathbf{2}})}$.

(118) Suppose that

(i) $Z \subseteq$ dom((the function arccot) $\cdot$(the function ln)), and

(ii) for every x such that $x \in Z$ holds $-1 <$ (the function ln)(x) and (the function ln)$(x) < 1$.

Then

(iii) (the function arccot) $\cdot$(the function ln) is differentiable on Z, and

(iv) for every x such that $x \in Z$ holds ((the function arccot) $\cdot$(the function ln))$'_{\restriction Z}(x) = -\frac{1}{x\cdot(1+(\text{the function ln})(x)^{\mathbf{2}})}$.

(119) Suppose $Z \subseteq$ dom((the function exp) $\cdot$(the function arctan)) and $Z \subseteq\,]-1, 1[$. Then

(i) (the function exp) $\cdot$(the function arctan) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function exp) $\cdot$(the function arctan))$'_{\restriction Z}(x) = \frac{\exp \arctan x}{1+x^{\mathbf{2}}}$.

(120) Suppose $Z \subseteq$ dom((the function exp) $\cdot$(the function arccot)) and $Z \subseteq\,]-1, 1[$. Then

(i) (the function exp) $\cdot$(the function arccot) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function exp) $\cdot$(the function arccot))$'_{\restriction Z}(x) = -\frac{\exp \operatorname{arccot} x}{1+x^{\mathbf{2}}}$.

(121) Suppose $Z \subseteq$ dom((the function arctan)$-\mathrm{id}_Z$) and $Z \subseteq\,]-1, 1[$. Then

(i) (the function arctan)$-\mathrm{id}_Z$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function arctan)$-\mathrm{id}_Z)'_{\restriction Z}(x) = -\frac{x^{\mathbf{2}}}{1+x^{\mathbf{2}}}$.

(122) Suppose $Z \subseteq$ dom($-$the function arccot $-$ id_Z) and $Z \subseteq\,]-1, 1[$. Then

(i) $-$the function arccot $-$ id_Z is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ($-$the function arccot $-$ $\mathrm{id}_Z)'_{\restriction Z}(x) = -\frac{x^{\mathbf{2}}}{1+x^{\mathbf{2}}}$.

(123) Suppose $Z \subseteq\,]-1, 1[$. Then

(i) (the function exp) (the function arctan) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function exp) (the function arctan))$'_{\restriction Z}(x) = \exp x \cdot \arctan x + \frac{\exp x}{1+x^{\mathbf{2}}}$.

(124) Suppose $Z \subseteq\,]-1, 1[$. Then

(i) (the function exp) (the function arccot) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function exp) (the function arccot))$'_{\restriction Z}(x) = \exp x \cdot \operatorname{arccot} x - \frac{\exp x}{1+x^{\mathbf{2}}}$.

(125) Suppose $Z \subseteq$ dom($\frac{1}{r}$ ((the function arctan) $\cdot f$) $-$ id_Z) and for every x such that $x \in Z$ holds $f(x) = r \cdot x$ and $r \neq 0$ and $-1 < f(x) < 1$. Then

(i) $\frac{1}{r}$ ((the function arctan) $\cdot f$) $-$ id_Z is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{1}{r}((\text{the function arctan}) \cdot f) - \mathrm{id}_Z)'_{\restriction Z}(x) = -\frac{(r\cdot x)^2}{1+(r\cdot x)^2}$.

(126) Suppose $Z \subseteq \mathrm{dom}((-\frac{1}{r})((\text{the function arccot}) \cdot f) - \mathrm{id}_Z)$ and for every x such that $x \in Z$ holds $f(x) = r \cdot x$ and $r \neq 0$ and $-1 < f(x) < 1$. Then

(i) $(-\frac{1}{r})((\text{the function arccot}) \cdot f) - \mathrm{id}_Z$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((-\frac{1}{r})((\text{the function arccot}) \cdot f) - \mathrm{id}_Z)'_{\restriction Z}(x) = -\frac{(r\cdot x)^2}{1+(r\cdot x)^2}$.

(127) Suppose $Z \subseteq \mathrm{dom}((\text{the function ln})\ (\text{the function arctan}))$ and $Z \subseteq]-1, 1[$. Then

(i) (the function ln) (the function arctan) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\text{the function ln})\ (\text{the function arctan}))'_{\restriction Z}(x) = \frac{\arctan x}{x} + \frac{(\text{the function ln})(x)}{1+x^2}$.

(128) Suppose $Z \subseteq \mathrm{dom}((\text{the function ln})\ (\text{the function arccot}))$ and $Z \subseteq]-1, 1[$. Then

(i) (the function ln) (the function arccot) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\text{the function ln})\ (\text{the function arccot}))'_{\restriction Z}(x) = \frac{\mathrm{arccot}\, x}{x} - \frac{(\text{the function ln})(x)}{1+x^2}$.

(129) Suppose $Z \subseteq \mathrm{dom}(\frac{1}{f}\ \text{the function arctan})$ and $Z \subseteq]-1, 1[$ and for every x such that $x \in Z$ holds $f(x) = x$. Then

(i) $\frac{1}{f}$ the function arctan is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{1}{f}\ \text{the function arctan})'_{\restriction Z}(x) = -\frac{\arctan x}{x^2} + \frac{1}{x\cdot(1+x^2)}$.

(130) Suppose $Z \subseteq \mathrm{dom}(\frac{1}{f}\ \text{the function arccot})$ and $Z \subseteq]-1, 1[$ and for every x such that $x \in Z$ holds $f(x) = x$. Then

(i) $\frac{1}{f}$ the function arccot is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{1}{f}\ \text{the function arccot})'_{\restriction Z}(x) = -\frac{\mathrm{arccot}\, x}{x^2} - \frac{1}{x\cdot(1+x^2)}$.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[2] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[3] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[4] Pacharapokin Chanapat, Kanchun, and Hiroshi Yamazaki. Formulas and identities of trigonometric functions. *Formalized Mathematics*, 12(**2**):139–141, 2004.

[5] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[6] Jarosław Kotowicz. Partial functions from a domain to a domain. *Formalized Mathematics*, 1(**4**):697–702, 1990.

[7] Jarosław Kotowicz. Partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 1(**4**):703–709, 1990.

[8] Jarosław Kotowicz. Properties of real functions. *Formalized Mathematics*, 1(**4**):781–786, 1990.

[9] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[10] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

[11] Konrad Raczkowski and Paweł Sadowski. Real function continuity. *Formalized Mathematics*, 1(**4**):787–791, 1990.

[12] Konrad Raczkowski and Paweł Sadowski. Real function differentiability. *Formalized Mathematics*, 1(**4**):797–801, 1990.

[13] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.

[14] Yasunari Shidama. The Taylor expansions. *Formalized Mathematics*, 12(**2**):195–200, 2004.

[15] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[16] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[17] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[18] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[19] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

Received March 18, 2008

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 159–165, 2008

Inverse Trigonometric Functions Arcsec and Arccosec

Bing Xie
Qingdao University of Science and Technology
China

Xiquan Liang
Qingdao University of Science and Technology
China

Fuguo Ge
Qingdao University of Science and Technology
China

Summary. This article describes definitions of inverse trigonometric functions arcsec and arccosec, as well as their main properties.

MML identifier: SINCOS10, version: 7.8.10 4.100.1011

The papers [1], [2], [16], [3], [12], [17], [13], [5], [8], [11], [14], [4], [6], [7], [10], [15], and [9] provide the notation and terminology for this paper.

In this paper x, r denote real numbers.

The following propositions are true:

(1) $[0, \frac{\pi}{2}[\subseteq \mathrm{dom}\,$(the function sec).

(2) $]\frac{\pi}{2}, \pi] \subseteq \mathrm{dom}\,$(the function sec).

(3) $[-\frac{\pi}{2}, 0[\subseteq \mathrm{dom}\,$(the function cosec).

(4) $]0, \frac{\pi}{2}] \subseteq \mathrm{dom}\,$(the function cosec).

(5) The function sec is differentiable on $]0, \frac{\pi}{2}[$ and for every x such that $x \in\,]0, \frac{\pi}{2}[$ holds (the function sec)$'(x) = \frac{\sin x}{(\cos x)^{\mathbf{2}}}$.

(6) The function sec is differentiable on $]\frac{\pi}{2}, \pi[$ and for every x such that $x \in\,]\frac{\pi}{2}, \pi[$ holds (the function sec)$'(x) = \frac{\sin x}{(\cos x)^{\mathbf{2}}}$.

(7)(i) The function cosec is differentiable on $]-\frac{\pi}{2}, 0[$, and

ISSN 1426–2630(p), 1898-9934(e)

(ii) for every x such that $x \in]-\frac{\pi}{2}, 0[$ holds (the function cosec)$'(x) = -\frac{\cos x}{(\sin x)^{\mathbf{2}}}$.

(8)(i) The function cosec is differentiable on $]0, \frac{\pi}{2}[$, and

(ii) for every x such that $x \in]0, \frac{\pi}{2}[$ holds (the function cosec)$'(x) = -\frac{\cos x}{(\sin x)^{\mathbf{2}}}$.

(9) The function sec is continuous on $]0, \frac{\pi}{2}[$.

(10) The function sec is continuous on $]\frac{\pi}{2}, \pi[$.

(11) The function cosec is continuous on $]-\frac{\pi}{2}, 0[$.

(12) The function cosec is continuous on $]0, \frac{\pi}{2}[$.

(13) The function sec is increasing on $]0, \frac{\pi}{2}[$.

(14) The function sec is increasing on $]\frac{\pi}{2}, \pi[$.

(15) The function cosec is decreasing on $]-\frac{\pi}{2}, 0[$.

(16) The function cosec is decreasing on $]0, \frac{\pi}{2}[$.

(17) The function sec is increasing on $[0, \frac{\pi}{2}[$.

(18) The function sec is increasing on $]\frac{\pi}{2}, \pi]$.

(19) The function cosec is decreasing on $[-\frac{\pi}{2}, 0[$.

(20) The function cosec is decreasing on $]0, \frac{\pi}{2}]$.

(21) (The function sec)$\restriction[0, \frac{\pi}{2}[$ is one-to-one.

(22) (The function sec)$\restriction]\frac{\pi}{2}, \pi]$ is one-to-one.

(23) (The function cosec)$\restriction[-\frac{\pi}{2}, 0[$ is one-to-one.

(24) (The function cosec)$\restriction]0, \frac{\pi}{2}]$ is one-to-one.

One can verify the following observations:

$*$ (the function sec)$\restriction[0, \frac{\pi}{2}[$ is one-to-one,

$*$ (the function sec)$\restriction]\frac{\pi}{2}, \pi]$ is one-to-one,

$*$ (the function cosec)$\restriction[-\frac{\pi}{2}, 0[$ is one-to-one, and

$*$ (the function cosec)$\restriction]0, \frac{\pi}{2}]$ is one-to-one.

The partial function the 1st part of arcsec from $\mathbb{R}$ to $\mathbb{R}$ is defined as follows:

(Def. 1) The 1st part of arcsec $=$ ((the function sec)$\restriction[0, \frac{\pi}{2}[)^{-1}$.

The partial function the 2nd part of arcsec from $\mathbb{R}$ to $\mathbb{R}$ is defined as follows:

(Def. 2) The 2nd part of arcsec $=$ ((the function sec)$\restriction]\frac{\pi}{2}, \pi])^{-1}$.

The partial function the 1st part of arccosec from $\mathbb{R}$ to $\mathbb{R}$ is defined by:

(Def. 3) The 1st part of arccosec $=$ ((the function cosec)$\restriction[-\frac{\pi}{2}, 0[)^{-1}$.

The partial function the 2nd part of arccosec from $\mathbb{R}$ to $\mathbb{R}$ is defined by:

(Def. 4) The 2nd part of arccosec $=$ ((the function cosec)$\restriction]0, \frac{\pi}{2}])^{-1}$.

Let r be a real number. The functor $\operatorname{arcsec}_1 r$ is defined by:

(Def. 5) $\operatorname{arcsec}_1 r =$ (the 1st part of arcsec)(r).

The functor $\operatorname{arcsec}_2 r$ is defined as follows:

(Def. 6) $\operatorname{arcsec}_2 r = (\text{the 2nd part of arcsec})(r)$.

The functor $\operatorname{arccosec}_1 r$ is defined as follows:

(Def. 7) $\operatorname{arccosec}_1 r = (\text{the 1st part of arccosec})(r)$.

The functor $\operatorname{arccosec}_2 r$ is defined by:

(Def. 8) $\operatorname{arccosec}_2 r = (\text{the 2nd part of arccosec})(r)$.

Let r be a real number. Then $\operatorname{arcsec}_1 r$ is a real number. Then $\operatorname{arcsec}_2 r$ is a real number. Then $\operatorname{arccosec}_1 r$ is a real number. Then $\operatorname{arccosec}_2 r$ is a real number.

We now state four propositions:

(25) $\operatorname{rng}(\text{the 1st part of arcsec}) = [0, \frac{\pi}{2}[$.

(26) $\operatorname{rng}(\text{the 2nd part of arcsec}) =]\frac{\pi}{2}, \pi]$.

(27) $\operatorname{rng}(\text{the 1st part of arccosec}) = [-\frac{\pi}{2}, 0[$.

(28) $\operatorname{rng}(\text{the 2nd part of arccosec}) =]0, \frac{\pi}{2}]$.

One can check the following observations:

* the 1st part of arcsec is one-to-one,
* the 2nd part of arcsec is one-to-one,
* the 1st part of arccosec is one-to-one, and
* the 2nd part of arccosec is one-to-one.

Let t_1 be a real number. Then $\sec t_1$ is a real number. Then $\operatorname{cosec} t_1$ is a real number.

We now state a number of propositions:

(29) $\sin(\frac{\pi}{4}) = \frac{1}{\sqrt{2}}$ and $\cos(\frac{\pi}{4}) = \frac{1}{\sqrt{2}}$.

(30) $\sin(-\frac{\pi}{4}) = -\frac{1}{\sqrt{2}}$ and $\cos(-\frac{\pi}{4}) = \frac{1}{\sqrt{2}}$ and $\sin(\frac{3}{4} \cdot \pi) = \frac{1}{\sqrt{2}}$ and $\cos(\frac{3}{4} \cdot \pi) = -\frac{1}{\sqrt{2}}$.

(31) $\sec 0 = 1$ and $\sec(\frac{\pi}{4}) = \sqrt{2}$ and $\sec(\frac{3}{4} \cdot \pi) = -\sqrt{2}$ and $\sec \pi = -1$.

(32) $\operatorname{cosec}(-\frac{\pi}{2}) = -1$ and $\operatorname{cosec}(-\frac{\pi}{4}) = -\sqrt{2}$ and $\operatorname{cosec}(\frac{\pi}{4}) = \sqrt{2}$ and $\operatorname{cosec}(\frac{\pi}{2}) = 1$.

(33) For every set x such that $x \in [0, \frac{\pi}{4}]$ holds $\sec x \in [1, \sqrt{2}]$.

(34) For every set x such that $x \in [\frac{3}{4} \cdot \pi, \pi]$ holds $\sec x \in [-\sqrt{2}, -1]$.

(35) For every set x such that $x \in [-\frac{\pi}{2}, -\frac{\pi}{4}]$ holds $\operatorname{cosec} x \in [-\sqrt{2}, -1]$.

(36) For every set x such that $x \in [\frac{\pi}{4}, \frac{\pi}{2}]$ holds $\operatorname{cosec} x \in [1, \sqrt{2}]$.

(37) The function sec is continuous on $[0, \frac{\pi}{2}[$.

(38) The function sec is continuous on $]\frac{\pi}{2}, \pi]$.

(39) The function cosec is continuous on $[-\frac{\pi}{2}, 0[$.

(40) The function cosec is continuous on $]0, \frac{\pi}{2}]$.

(41) $\operatorname{rng}((\text{the function sec}) \restriction [0, \frac{\pi}{4}]) = [1, \sqrt{2}]$.

(42) $\operatorname{rng}((\text{the function sec}) \restriction [\frac{3}{4} \cdot \pi, \pi]) = [-\sqrt{2}, -1]$.

(43) rng((the function cosec)$\restriction[-\frac{\pi}{2},-\frac{\pi}{4}]) = [-\sqrt{2},-1]$.

(44) rng((the function cosec)$\restriction[\frac{\pi}{4},\frac{\pi}{2}]) = [1,\sqrt{2}]$.

(45) $[1,\sqrt{2}] \subseteq$ dom (the 1st part of arcsec).

(46) $[-\sqrt{2},-1] \subseteq$ dom (the 2nd part of arcsec).

(47) $[-\sqrt{2},-1] \subseteq$ dom (the 1st part of arccosec).

(48) $[1,\sqrt{2}] \subseteq$ dom (the 2nd part of arccosec).

One can check the following observations:

* (the function sec)$\restriction[0,\frac{\pi}{4}]$ is one-to-one,
* (the function sec)$\restriction[\frac{3}{4}\cdot\pi,\pi]$ is one-to-one,
* (the function cosec)$\restriction[-\frac{\pi}{2},-\frac{\pi}{4}]$ is one-to-one, and
* (the function cosec)$\restriction[\frac{\pi}{4},\frac{\pi}{2}]$ is one-to-one.

One can prove the following propositions:

(49) (The 1st part of arcsec)$\restriction[1,\sqrt{2}] = ($(the function sec)$\restriction[0,\frac{\pi}{4}])^{-1}$.

(50) (The 2nd part of arcsec)$\restriction[-\sqrt{2},-1] = ($(the function sec)$\restriction[\frac{3}{4}\cdot\pi,\pi])^{-1}$.

(51) (The 1st part of arccosec)$\restriction[-\sqrt{2},-1] = ($(the function cosec)$\restriction[-\frac{\pi}{2},-\frac{\pi}{4}])^{-1}$.

(52) (The 2nd part of arccosec)$\restriction[1,\sqrt{2}] = ($(the function cosec)$\restriction[\frac{\pi}{4},\frac{\pi}{2}])^{-1}$.

(53) ((The function sec)$\restriction[0,\frac{\pi}{4}]$ **qua** function) $\cdot$((the 1st part of arcsec)$\restriction[1,\sqrt{2}]) = \mathrm{id}_{[1,\sqrt{2}]}$.

(54) ((The function sec)$\restriction[\frac{3}{4}\cdot\pi,\pi]$ **qua** function) $\cdot$((the 2nd part of arcsec)$\restriction[-\sqrt{2},-1]) = \mathrm{id}_{[-\sqrt{2},-1]}$.

(55) ((The function cosec)$\restriction[-\frac{\pi}{2},-\frac{\pi}{4}]$ **qua** function) $\cdot$((the 1st part of arccosec)$\restriction[-\sqrt{2},-1]) = \mathrm{id}_{[-\sqrt{2},-1]}$.

(56) ((The function cosec)$\restriction[\frac{\pi}{4},\frac{\pi}{2}]$ **qua** function) $\cdot$((the 2nd part of arccosec)$\restriction[1,\sqrt{2}]) = \mathrm{id}_{[1,\sqrt{2}]}$.

(57) ((The function sec)$\restriction[0,\frac{\pi}{4}]) \cdot$ ((the 1st part of arcsec)$\restriction[1,\sqrt{2}]) = \mathrm{id}_{[1,\sqrt{2}]}$.

(58) ((The function sec)$\restriction[\frac{3}{4}\cdot\pi,\pi]) \cdot$ ((the 2nd part of arcsec)$\restriction[-\sqrt{2},-1]) = \mathrm{id}_{[-\sqrt{2},-1]}$.

(59) ((The function cosec)$\restriction[-\frac{\pi}{2},-\frac{\pi}{4}])\cdot$((the 1st part of arccosec)$\restriction[-\sqrt{2},-1]) = \mathrm{id}_{[-\sqrt{2},-1]}$.

(60) ((The function cosec)$\restriction[\frac{\pi}{4},\frac{\pi}{2}]) \cdot$ ((the 2nd part of arccosec)$\restriction[1,\sqrt{2}]) = \mathrm{id}_{[1,\sqrt{2}]}$.

(61) (The 1st part of arcsec **qua** function) $\cdot$((the function sec)$\restriction[0,\frac{\pi}{2}[) = \mathrm{id}_{[0,\frac{\pi}{2}[}$.

(62) (The 2nd part of arcsec **qua** function) $\cdot$((the function sec)$\restriction]\frac{\pi}{2},\pi]) = \mathrm{id}_{]\frac{\pi}{2},\pi]}$.

(63) (The 1st part of arccosec **qua** function) $\cdot$((the function cosec)$\restriction[-\frac{\pi}{2},0[) = \mathrm{id}_{[-\frac{\pi}{2},0[}$.

(64) (The 2nd part of arccosec **qua** function) $\cdot$((the function cosec)$\restriction$$]0, \frac{\pi}{2}]$) $=$ $\mathrm{id}_{]0,\frac{\pi}{2}]}$.

(65) (The 1st part of arcsec) $\cdot$((the function sec)$\restriction$$[0, \frac{\pi}{2}[$) $= \mathrm{id}_{[0,\frac{\pi}{2}[}$.

(66) (The 2nd part of arcsec) $\cdot$((the function sec)$\restriction$$]\frac{\pi}{2}, \pi]$) $= \mathrm{id}_{]\frac{\pi}{2},\pi]}$.

(67) (The 1st part of arccosec) $\cdot$((the function cosec)$\restriction$$[-\frac{\pi}{2}, 0[$) $= \mathrm{id}_{[-\frac{\pi}{2},0[}$.

(68) (The 2nd part of arccosec) $\cdot$((the function cosec)$\restriction$$]0, \frac{\pi}{2}]$) $= \mathrm{id}_{]0,\frac{\pi}{2}]}$.

(69) If $0 \leq r < \frac{\pi}{2}$, then $\mathrm{arcsec}_1 \sec r = r$.

(70) If $\frac{\pi}{2} < r \leq \pi$, then $\mathrm{arcsec}_2 \sec r = r$.

(71) If $-\frac{\pi}{2} \leq r < 0$, then $\mathrm{arccosec}_1 \mathrm{cosec}\, r = r$.

(72) If $0 < r \leq \frac{\pi}{2}$, then $\mathrm{arccosec}_2 \mathrm{cosec}\, r = r$.

(73) $\mathrm{arcsec}_1 1 = 0$ and $\mathrm{arcsec}_1 \sqrt{2} = \frac{\pi}{4}$.

(74) $\mathrm{arcsec}_2(-\sqrt{2}) = \frac{3}{4} \cdot \pi$ and $\mathrm{arcsec}_2(-1) = \pi$.

(75) $\mathrm{arccosec}_1(-1) = -\frac{\pi}{2}$ and $\mathrm{arccosec}_1(-\sqrt{2}) = -\frac{\pi}{4}$.

(76) $\mathrm{arccosec}_2 \sqrt{2} = \frac{\pi}{4}$ and $\mathrm{arccosec}_2 1 = \frac{\pi}{2}$.

(77) The 1st part of arcsec is increasing on (the function sec) $^\circ[0, \frac{\pi}{2}[$.

(78) The 2nd part of arcsec is increasing on (the function sec) $^\circ]\frac{\pi}{2}, \pi]$.

(79) The 1st part of arccosec is decreasing on (the function cosec) $^\circ[-\frac{\pi}{2}, 0[$.

(80) The 2nd part of arccosec is decreasing on (the function cosec) $^\circ]0, \frac{\pi}{2}]$.

(81) The 1st part of arcsec is increasing on $[1, \sqrt{2}]$.

(82) The 2nd part of arcsec is increasing on $[-\sqrt{2}, -1]$.

(83) The 1st part of arccosec is decreasing on $[-\sqrt{2}, -1]$.

(84) The 2nd part of arccosec is decreasing on $[1, \sqrt{2}]$.

(85) For every set x such that $x \in [1, \sqrt{2}]$ holds $\mathrm{arcsec}_1 x \in [0, \frac{\pi}{4}]$.

(86) For every set x such that $x \in [-\sqrt{2}, -1]$ holds $\mathrm{arcsec}_2 x \in [\frac{3}{4} \cdot \pi, \pi]$.

(87) For every set x such that $x \in [-\sqrt{2}, -1]$ holds $\mathrm{arccosec}_1 x \in [-\frac{\pi}{2}, -\frac{\pi}{4}]$.

(88) For every set x such that $x \in [1, \sqrt{2}]$ holds $\mathrm{arccosec}_2 x \in [\frac{\pi}{4}, \frac{\pi}{2}]$.

(89) If $1 \leq r \leq \sqrt{2}$, then $\sec \mathrm{arcsec}_1 r = r$.

(90) If $-\sqrt{2} \leq r \leq -1$, then $\sec \mathrm{arcsec}_2 r = r$.

(91) If $-\sqrt{2} \leq r \leq -1$, then $\mathrm{cosec}\, \mathrm{arccosec}_1 r = r$.

(92) If $1 \leq r \leq \sqrt{2}$, then $\mathrm{cosec}\, \mathrm{arccosec}_2 r = r$.

(93) The 1st part of arcsec is continuous on $[1, \sqrt{2}]$.

(94) The 2nd part of arcsec is continuous on $[-\sqrt{2}, -1]$.

(95) The 1st part of arccosec is continuous on $[-\sqrt{2}, -1]$.

(96) The 2nd part of arccosec is continuous on $[1, \sqrt{2}]$.

(97) rng((the 1st part of arcsec)$\restriction$$[1, \sqrt{2}]$) $= [0, \frac{\pi}{4}]$.

(98) rng((the 2nd part of arcsec)$\restriction$$[-\sqrt{2}, -1]$) $= [\frac{3}{4} \cdot \pi, \pi]$.

(99) rng((the 1st part of arccosec)$\restriction$$[-\sqrt{2}, -1]$) $= [-\frac{\pi}{2}, -\frac{\pi}{4}]$.

(100) rng((the 2nd part of arccosec)$\restriction[1, \sqrt{2}]$) $= [\frac{\pi}{4}, \frac{\pi}{2}]$.

(101) If $1 \leq r \leq \sqrt{2}$ and $\operatorname{arcsec}_1 r = 0$, then $r = 1$ and if $1 \leq r \leq \sqrt{2}$ and $\operatorname{arcsec}_1 r = \frac{\pi}{4}$, then $r = \sqrt{2}$.

(102) If $-\sqrt{2} \leq r \leq -1$ and $\operatorname{arcsec}_2 r = \frac{3}{4} \cdot \pi$, then $r = -\sqrt{2}$ and if $-\sqrt{2} \leq r \leq -1$ and $\operatorname{arcsec}_2 r = \pi$, then $r = -1$.

(103) If $-\sqrt{2} \leq r \leq -1$ and $\operatorname{arccosec}_1 r = -\frac{\pi}{2}$, then $r = -1$ and if $-\sqrt{2} \leq r \leq -1$ and $\operatorname{arccosec}_1 r = -\frac{\pi}{4}$, then $r = -\sqrt{2}$.

(104) If $1 \leq r \leq \sqrt{2}$ and $\operatorname{arccosec}_2 r = \frac{\pi}{4}$, then $r = \sqrt{2}$ and if $1 \leq r \leq \sqrt{2}$ and $\operatorname{arccosec}_2 r = \frac{\pi}{2}$, then $r = 1$.

(105) If $1 \leq r \leq \sqrt{2}$, then $0 \leq \operatorname{arcsec}_1 r \leq \frac{\pi}{4}$.

(106) If $-\sqrt{2} \leq r \leq -1$, then $\frac{3}{4} \cdot \pi \leq \operatorname{arcsec}_2 r \leq \pi$.

(107) If $-\sqrt{2} \leq r \leq -1$, then $-\frac{\pi}{2} \leq \operatorname{arccosec}_1 r \leq -\frac{\pi}{4}$.

(108) If $1 \leq r \leq \sqrt{2}$, then $\frac{\pi}{4} \leq \operatorname{arccosec}_2 r \leq \frac{\pi}{2}$.

(109) If $1 < r < \sqrt{2}$, then $0 < \operatorname{arcsec}_1 r < \frac{\pi}{4}$.

(110) If $-\sqrt{2} < r < -1$, then $\frac{3}{4} \cdot \pi < \operatorname{arcsec}_2 r < \pi$.

(111) If $-\sqrt{2} < r < -1$, then $-\frac{\pi}{2} < \operatorname{arccosec}_1 r < -\frac{\pi}{4}$.

(112) If $1 < r < \sqrt{2}$, then $\frac{\pi}{4} < \operatorname{arccosec}_2 r < \frac{\pi}{2}$.

(113) If $1 \leq r \leq \sqrt{2}$, then $\sin \operatorname{arcsec}_1 r = \frac{\sqrt{r^2-1}}{r}$ and $\cos \operatorname{arcsec}_1 r = \frac{1}{r}$.

(114) If $-\sqrt{2} \leq r \leq -1$, then $\sin \operatorname{arcsec}_2 r = -\frac{\sqrt{r^2-1}}{r}$ and $\cos \operatorname{arcsec}_2 r = \frac{1}{r}$.

(115) If $-\sqrt{2} \leq r \leq -1$, then $\sin \operatorname{arccosec}_1 r = \frac{1}{r}$ and $\cos \operatorname{arccosec}_1 r = -\frac{\sqrt{r^2-1}}{r}$.

(116) If $1 \leq r \leq \sqrt{2}$, then $\sin \operatorname{arccosec}_2 r = \frac{1}{r}$ and $\cos \operatorname{arccosec}_2 r = \frac{\sqrt{r^2-1}}{r}$.

(117) If $1 < r < \sqrt{2}$, then $\operatorname{cosec} \operatorname{arcsec}_1 r = \frac{r}{\sqrt{r^2-1}}$.

(118) If $-\sqrt{2} < r < -1$, then $\operatorname{cosec} \operatorname{arcsec}_2 r = -\frac{r}{\sqrt{r^2-1}}$.

(119) If $-\sqrt{2} < r < -1$, then $\sec \operatorname{arccosec}_1 r = -\frac{r}{\sqrt{r^2-1}}$.

(120) If $1 < r < \sqrt{2}$, then $\sec \operatorname{arccosec}_2 r = \frac{r}{\sqrt{r^2-1}}$.

(121) The 1st part of arcsec is differentiable on (the function sec) $^\circ]0, \frac{\pi}{2}[$.

(122) The 2nd part of arcsec is differentiable on (the function sec) $^\circ]\frac{\pi}{2}, \pi[$.

(123) The 1st part of arccosec is differentiable on (the function cosec) $^\circ]-\frac{\pi}{2}, 0[$.

(124) The 2nd part of arccosec is differentiable on (the function cosec) $^\circ]0, \frac{\pi}{2}[$.

(125) (The function sec) $^\circ]0, \frac{\pi}{2}[$ is open.

(126) (The function sec) $^\circ]\frac{\pi}{2}, \pi[$ is open.

(127) (The function cosec) $^\circ]-\frac{\pi}{2}, 0[$ is open.

(128) (The function cosec) $^\circ]0, \frac{\pi}{2}[$ is open.

(129) The 1st part of arcsec is continuous on (the function sec) $^\circ]0, \frac{\pi}{2}[$.

(130) The 2nd part of arcsec is continuous on (the function sec) $^\circ]\frac{\pi}{2}, \pi[$.

(131) The 1st part of arccosec is continuous on (the function cosec) $^\circ]-\frac{\pi}{2}, 0[$.

(132) The 2nd part of arccosec is continuous on (the function cosec) $^\circ]0, \frac{\pi}{2}[$.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[2] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[3] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[4] Pacharapokin Chanapat, Kanchun, and Hiroshi Yamazaki. Formulas and identities of trigonometric functions. *Formalized Mathematics*, 12(**2**):139–141, 2004.

[5] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[6] Jarosław Kotowicz. Partial functions from a domain to a domain. *Formalized Mathematics*, 1(**4**):697–702, 1990.

[7] Jarosław Kotowicz. Properties of real functions. *Formalized Mathematics*, 1(**4**):781–786, 1990.

[8] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[9] Yatsuka Nakamura. Half open intervals in real numbers. *Formalized Mathematics*, 10(**1**):21–22, 2002.

[10] Konrad Raczkowski and Paweł Sadowski. Real function continuity. *Formalized Mathematics*, 1(**4**):787–791, 1990.

[11] Konrad Raczkowski and Paweł Sadowski. Real function differentiability. *Formalized Mathematics*, 1(**4**):797–801, 1990.

[12] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.

[13] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[14] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[15] Peng Wang and Bo Li. Several differentiation formulas of special functions. Part V. *Formalized Mathematics*, 15(**3**):73–79, 2007.

[16] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[17] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

Received March 18, 2008

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 167–175, 2008

The Lebesgue Monotone Convergence Theorem

Noboru Endou
Gifu National College of Technology
Japan

Keiko Narita
Hirosaki-city
Aomori, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article we prove the Monotone Convergence Theorem [16].

MML identifier: `MESFUNC9`, version: `7.8.10 4.100.1011`

The notation and terminology used in this paper have been introduced in the following articles: [10], [20], [2], [7], [21], [6], [8], [9], [1], [17], [18], [3], [4], [5], [13], [14], [15], [19], [11], [12], and [22].

1. Preliminaries

For simplicity, we adopt the following rules: X is a non empty set, S is a σ-field of subsets of X, M is a σ-measure on S, E is an element of S, F, G are sequences of partial functions from X into $\overline{\mathbb{R}}$, I is a sequence of extended reals, f, g are partial functions from X to $\overline{\mathbb{R}}$, s_1, s_2, s_3 are sequences of extended reals, p is an extended real number, n, m are natural numbers, x is an element of X, and z, D are sets.

Next we state a number of propositions:

(1) If f is without $+\infty$ and g is without $+\infty$, then $\mathrm{dom}(f+g) = \mathrm{dom}\, f \cap \mathrm{dom}\, g$.

(2) If f is without $+\infty$ and g is without $-\infty$, then $\mathrm{dom}(f-g) = \mathrm{dom}\, f \cap \mathrm{dom}\, g$.

(3) If f is without $-\infty$ and g is without $-\infty$, then $f+g$ is without $-\infty$.

(4) If f is without $+\infty$ and g is without $+\infty$, then $f+g$ is without $+\infty$.

(5) If f is without $-\infty$ and g is without $+\infty$, then $f-g$ is without $-\infty$.

(6) If f is without $+\infty$ and g is without $-\infty$, then $f-g$ is without $+\infty$.

(7)(i) If s_1 is convergent to finite number, then there exists a real number g such that $\lim s_1 = g$ and for every real number p such that $0 < p$ there exists a natural number n such that for every natural number m such that $n \leq m$ holds $|s_1(m) - \lim s_1| < p$,

(ii) if s_1 is convergent to $+\infty$, then $\lim s_1 = +\infty$, and

(iii) if s_1 is convergent to $-\infty$, then $\lim s_1 = -\infty$.

(8) If s_1 is non-negative, then s_1 is not convergent to $-\infty$.

(9) If s_1 is convergent and for every natural number k holds $s_1(k) \leq p$, then $\lim s_1 \leq p$.

(10) If s_1 is convergent and for every natural number k holds $p \leq s_1(k)$, then $p \leq \lim s_1$.

(11) Suppose that

(i) s_2 is convergent,

(ii) s_3 is convergent,

(iii) s_2 is non-negative,

(iv) s_3 is non-negative, and

(v) for every natural number k holds $s_1(k) = s_2(k) + s_3(k)$.

Then s_1 is non-negative and convergent and $\lim s_1 = \lim s_2 + \lim s_3$.

(12) Suppose for every natural number n holds $G(n) = F(n) \restriction D$ and $x \in D$. Then

(i) if $F\#x$ is convergent to $+\infty$, then $G\#x$ is convergent to $+\infty$,

(ii) if $F\#x$ is convergent to $-\infty$, then $G\#x$ is convergent to $-\infty$,

(iii) if $F\#x$ is convergent to finite number, then $G\#x$ is convergent to finite number, and

(iv) if $F\#x$ is convergent, then $G\#x$ is convergent.

(13) If $E = \operatorname{dom} f$ and f is measurable on E and f is non-negative and $M(E \cap \text{EQ-dom}(f, +\infty)) \neq 0$, then $\int f \, \mathrm{d}M = +\infty$.

(14) $\int \chi_{E,X} \, \mathrm{d}M = M(E)$ and $\int \chi_{E,X} \restriction E \, \mathrm{d}M = M(E)$.

(15) Suppose that

(i) $E \subseteq \operatorname{dom} f$,

(ii) $E \subseteq \operatorname{dom} g$,

(iii) f is measurable on E,

(iv) g is measurable on E,

(v) f is non-negative, and

(vi) for every element x of X such that $x \in E$ holds $f(x) \leq g(x)$.

Then $\int f \restriction E \, \mathrm{d}M \leq \int g \restriction E \, \mathrm{d}M$.

2. Selected Properties of Extended Real Sequence

Let f be an extended real-valued function and let x be a set. Then $f(x)$ is an element of $\overline{\mathbb{R}}$.

Let s be an extended real-valued function. The functor $(\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}$ yields a sequence of extended reals and is defined by:

(Def. 1) $(\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}(0) = s(0)$ and for every natural number n holds $(\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}(n+1) = (\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}(n) + s(n+1)$.

Let s be an extended real-valued function. We say that s is summable if and only if:

(Def. 2) $(\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}$ is convergent.

Let s be an extended real-valued function. The functor $\sum s$ yielding an extended real number is defined as follows:

(Def. 3) $\sum s = \lim((\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}})$.

Next we state several propositions:

(16) If s_1 is non-negative, then $(\sum_{\alpha=0}^{\kappa}(s_1)(\alpha))_{\kappa\in\mathbb{N}}$ is non-negative and $(\sum_{\alpha=0}^{\kappa}(s_1)(\alpha))_{\kappa\in\mathbb{N}}$ is non-decreasing.

(17) If for every natural number n holds $0 < s_1(n)$, then for every natural number m holds $0 < (\sum_{\alpha=0}^{\kappa}(s_1)(\alpha))_{\kappa\in\mathbb{N}}(m)$.

(18) If F has the same dom and for every natural number n holds $G(n) = F(n)\restriction D$, then G has the same dom.

(19) Suppose that

(i) $D \subseteq \operatorname{dom} F(0)$,

(ii) for every natural number n holds $G(n) = F(n)\restriction D$, and

(iii) for every element x of X such that $x \in D$ holds $F\#x$ is convergent.

Then $\lim F\restriction D = \lim G$.

(20) Suppose F has the same dom and $E \subseteq \operatorname{dom} F(0)$ and for every natural number m holds $F(m)$ is measurable on E and $G(m) = F(m)\restriction E$. Then $G(n)$ is measurable on E.

(21) Suppose that

(i) $E \subseteq \operatorname{dom} F(0)$,

(ii) G has the same dom,

(iii) for every element x of X such that $x \in E$ holds $F\#x$ is summable, and

(iv) for every natural number n holds $G(n) = F(n)\restriction E$.

Let x be an element of X. If $x \in E$, then $G\#x$ is summable.

3. Partial Sums of Functional Sequence and their Properties

Let X be a non empty set and let F be a sequence of partial functions from X into $\overline{\mathbb{R}}$. The functor $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}$ yields a sequence of partial functions from X into $\overline{\mathbb{R}}$ and is defined as follows:

(Def. 4) $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(0) = F(0)$ and for every natural number n holds $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n+1) = (\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n) + F(n+1)$.

Let X be a set and let F be a sequence of partial functions from X into $\overline{\mathbb{R}}$. We say that F is additive if and only if:

(Def. 5) For all natural numbers n, m such that $n \neq m$ and for every set x such that $x \in \operatorname{dom} F(n) \cap \operatorname{dom} F(m)$ holds $F(n)(x) \neq +\infty$ or $F(m)(x) \neq -\infty$.

Next we state a number of propositions:

(22) If $z \in \operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)$ and $m \leq n$, then $z \in \operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(m)$ and $z \in \operatorname{dom} F(m)$.

(23) If $z \in \operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)$ and $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)(z) = +\infty$, then there exists a natural number m such that $m \leq n$ and $F(m)(z) = +\infty$.

(24) If F is additive and $z \in \operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)$ and $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)(z) = +\infty$ and $m \leq n$, then $F(m)(z) \neq -\infty$.

(25) If $z \in \operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)$ and $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)(z) = -\infty$, then there exists a natural number m such that $m \leq n$ and $F(m)(z) = -\infty$.

(26) If F is additive and $z \in \operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)$ and $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)(z) = -\infty$ and $m \leq n$, then $F(m)(z) \neq +\infty$.

(27) If F is additive, then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)^{-1}(\{-\infty\}) \cap F(n+1)^{-1}(\{+\infty\}) = \emptyset$ and $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)^{-1}(\{+\infty\}) \cap F(n+1)^{-1}(\{-\infty\}) = \emptyset$.

(28) If F is additive, then $\operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n) = \bigcap\{\operatorname{dom} F(k); k$ ranges over elements of $\mathbb{N}$: $k \leq n\}$.

(29) If F is additive and has the same dom, then $\operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n) = \operatorname{dom} F(0)$.

(30) If for every natural number n holds $F(n)$ is non-negative, then F is additive.

(31) If F is additive and for every n holds $G(n) = F(n)\restriction D$, then G is additive.

(32) If F is additive and has the same dom and $D \subseteq \operatorname{dom} F(0)$ and $x \in D$, then $(\sum_{\alpha=0}^{\kappa}(F\#x)(\alpha))_{\kappa\in\mathbb{N}}(n) = ((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\#x)(n)$.

(33) Suppose F is additive and has the same dom and $D \subseteq \operatorname{dom} F(0)$ and $x \in D$. Then

(i) $(\sum_{\alpha=0}^{\kappa}(F\#x)(\alpha))_{\kappa\in\mathbb{N}}$ is convergent to finite number iff $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\#x$ is convergent to finite number,

(ii) $(\sum_{\alpha=0}^{\kappa}(F\#x)(\alpha))_{\kappa\in\mathbb{N}}$ is convergent to $+\infty$ iff $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\#x$ is convergent to $+\infty$,

(iii) $(\sum_{\alpha=0}^{\kappa}(F\#x)(\alpha))_{\kappa\in\mathbb{N}}$ is convergent to $-\infty$ iff $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}\#x$ is convergent to $-\infty$, and

(iv) $(\sum_{\alpha=0}^{\kappa}(F\#x)(\alpha))_{\kappa\in\mathbb{N}}$ is convergent iff $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}\#x$ is convergent.

(34) If F is additive and has the same dom and $\operatorname{dom} f \subseteq \operatorname{dom} F(0)$ and $x \in \operatorname{dom} f$ and $F\#x$ is summable and $f(x) = \sum F\#x$, then $f(x) = \lim((\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}\#x)$.

(35) Suppose that for every natural number m holds $F(m)$ is simple function in S. Then F is additive and $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}(n)$ is simple function in S.

(36) If for every natural number m holds $F(m)$ is non-negative, then $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}(n)$ is non-negative.

(37) If F has the same dom and $x \in \operatorname{dom} F(0)$ and for every natural number k holds $F(k)$ is non-negative and $n \leq m$, then $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}(n)(x) \leq (\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}(m)(x)$.

(38) Suppose F has the same dom and $x \in \operatorname{dom} F(0)$ and for every natural number m holds $F(m)$ is non-negative. Then $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}\#x$ is non-decreasing and $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}\#x$ is convergent.

(39) If for every natural number m holds $F(m)$ is without $-\infty$, then $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}(n)$ is without $-\infty$.

(40) If for every natural number m holds $F(m)$ is without $+\infty$, then $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}(n)$ is without $+\infty$.

(41) Suppose that for every natural number n holds $F(n)$ is measurable on E and $F(n)$ is without $-\infty$. Then $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}(m)$ is measurable on E.

(42) Suppose that

(i) F is additive and has the same dom,

(ii) G is additive and has the same dom,

(iii) $x \in \operatorname{dom} F(0) \cap \operatorname{dom} G(0)$, and

(iv) for every natural number k and for every element y of X such that $y \in \operatorname{dom} F(0) \cap \operatorname{dom} G(0)$ holds $F(k)(y) \leq G(k)(y)$.

Then $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}(n)(x) \leq (\sum_{\alpha=0}^{\kappa}G(\alpha))_{\kappa\in\mathbb{N}}(n)(x)$.

(43) Let X be a non empty set and F be a sequence of partial functions from X into $\overline{\mathbb{R}}$. If F is additive and has the same dom, then $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}$ has the same dom.

(44) Suppose that

(i) $\operatorname{dom} F(0) = E$,

(ii) F is additive and has the same dom,

(iii) for every natural number n holds $(\sum_{\alpha=0}^{\kappa}F(\alpha))_{\kappa\in\mathbb{N}}(n)$ is measurable on E, and

(iv) for every element x of X such that $x \in E$ holds $F\#x$ is summable.

Then $\lim((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}})$ is measurable on E.

(45) Suppose that for every natural number n holds $F(n)$ is integrable on M. Let m be a natural number. Then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(m)$ is integrable on M.

(46) Suppose that
(i) $E = \operatorname{dom} F(0)$,
(ii) F is additive and has the same dom, and
(iii) for every natural number n holds $F(n)$ is measurable on E and $F(n)$ is non-negative and $I(n) = \int F(n)\,\mathrm{d}M$.
Then $\int (\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(m)\,\mathrm{d}M = (\sum_{\alpha=0}^{\kappa} I(\alpha))_{\kappa\in\mathbb{N}}(m)$.

4. Sequence of Measurable Functions

Next we state two propositions:

(47) Suppose that
(i) $E \subseteq \operatorname{dom} f$,
(ii) f is non-negative,
(iii) f is measurable on E,
(iv) F is additive,
(v) for every n holds $F(n)$ is simple function in S and $F(n)$ is non-negative and $E \subseteq \operatorname{dom} F(n)$, and
(vi) for every x such that $x \in E$ holds $F\#x$ is summable and $f(x) = \sum F\#x$.
Then there exists a sequence I of extended reals such that for every n holds $I(n) = \int F(n){\restriction}E\,\mathrm{d}M$ and I is summable and $\int f{\restriction}E\,\mathrm{d}M = \sum I$.

(48) Suppose $E \subseteq \operatorname{dom} f$ and f is non-negative and f is measurable on E. Then there exists a sequence g of partial functions from X into $\overline{\mathbb{R}}$ such that
(i) g is additive,
(ii) for every natural number n holds $g(n)$ is simple function in S and $g(n)$ is non-negative and $g(n)$ is measurable on E,
(iii) for every element x of X such that $x \in E$ holds $g\#x$ is summable and $f(x) = \sum g\#x$, and
(iv) there exists a sequence I of extended reals such that for every natural number n holds $I(n) = \int g(n){\restriction}E\,\mathrm{d}M$ and I is summable and $\int f{\restriction}E\,\mathrm{d}M = \sum I$.

Let X be a non empty set. Observe that there exists a sequence of partial functions from X into $\overline{\mathbb{R}}$ which is additive and has the same dom.

Let C, D, X be non empty sets, let F be a function from $C \times D$ into $X \dot{\to} \overline{\mathbb{R}}$, let c be an element of C, and let d be an element of D. Then $F(c, d)$ is a partial function from X to $\overline{\mathbb{R}}$.

Let C, D, X be non empty sets, let F be a function from $C \times D$ into X, and let c be an element of C. The functor $\mathrm{curry}(F, c)$ yields a function from D into X and is defined as follows:

(Def. 6) For every element d of D holds $(\mathrm{curry}(F, c))(d) = F(c, d)$.

Let C, D, X be non empty sets, let F be a function from $C \times D$ into X, and let d be an element of D. The functor $\mathrm{curry}'(F, d)$ yields a function from C into X and is defined as follows:

(Def. 7) For every element c of C holds $(\mathrm{curry}'(F, d))(c) = F(c, d)$.

Let X, Y be sets, let F be a function from $\mathbb{N} \times \mathbb{N}$ into $X \dot{\rightarrow} Y$, and let n be a natural number. The functor $\mathrm{curry}(F, n)$ yielding a sequence of partial functions from X into Y is defined by:

(Def. 8) For every natural number m holds $(\mathrm{curry}(F, n))(m) = F(n, m)$.

The functor $\mathrm{curry}'(F, n)$ yields a sequence of partial functions from X into Y and is defined by:

(Def. 9) For every natural number m holds $(\mathrm{curry}'(F, n))(m) = F(m, n)$.

Let X be a non empty set, let F be a function from $\mathbb{N}$ into $(X \dot{\rightarrow} \overline{\mathbb{R}})^{\mathbb{N}}$, and let n be a natural number. Then $F(n)$ is a sequence of partial functions from X into $\overline{\mathbb{R}}$.

The following four propositions are true:

(49) Suppose $E = \mathrm{dom}\, F(0)$ and F has the same dom and for every natural number n holds $F(n)$ is non-negative and $F(n)$ is measurable on E. Then there exists a function F_1 from $\mathbb{N}$ into $(X \dot{\rightarrow} \overline{\mathbb{R}})^{\mathbb{N}}$ such that for every natural number n holds

(i) for every natural number m holds $F_1(n)(m)$ is simple function in S and $\mathrm{dom}\, F_1(n)(m) = \mathrm{dom}\, F(n)$,

(ii) for every natural number m holds $F_1(n)(m)$ is non-negative,

(iii) for all natural numbers j, k such that $j \leq k$ and for every element x of X such that $x \in \mathrm{dom}\, F(n)$ holds $F_1(n)(j)(x) \leq F_1(n)(k)(x)$, and

(iv) for every element x of X such that $x \in \mathrm{dom}\, F(n)$ holds $F_1(n)\#x$ is convergent and $\lim(F_1(n)\#x) = F(n)(x)$.

(50) Suppose that

(i) $E = \mathrm{dom}\, F(0)$,

(ii) F is additive and has the same dom, and

(iii) for every natural number n holds $F(n)$ is measurable on E and $F(n)$ is non-negative.

Then there exists a sequence I of extended reals such that for every natural number n holds

$I(n) = \int F(n)\, \mathrm{d}M$ and $\int (\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(n)\, \mathrm{d}M = (\sum_{\alpha=0}^{\kappa} I(\alpha))_{\kappa \in \mathbb{N}}(n)$.

(51) Suppose that

(i) $E \subseteq \mathrm{dom}\, F(0)$,

(ii) F is additive and has the same dom,

(iii) for every natural number n holds $F(n)$ is non-negative and $F(n)$ is measurable on E, and

(iv) for every element x of X such that $x \in E$ holds $F\#x$ is summable.

Then there exists a sequence I of extended reals such that for every natural number n holds $I(n) = \int F(n)\restriction E \, \mathrm{d}M$ and I is summable and $\int \lim((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}})\restriction E \, \mathrm{d}M = \sum I$.

(52) Suppose that

(i) $E = \operatorname{dom} F(0)$,

(ii) $F(0)$ is non-negative,

(iii) F has the same dom,

(iv) for every natural number n holds $F(n)$ is measurable on E,

(v) for all natural numbers n, m such that $n \leq m$ and for every element x of X such that $x \in E$ holds $F(n)(x) \leq F(m)(x)$, and

(vi) for every element x of X such that $x \in E$ holds $F\#x$ is convergent.

Then there exists a sequence I of extended reals such that for every natural number n holds $I(n) = \int F(n) \, \mathrm{d}M$ and I is convergent and $\int \lim F \, \mathrm{d}M = \lim I$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[3] Józef Białas. Infimum and supremum of the set of real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):163–171, 1991.

[4] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.

[5] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.

[6] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[11] Noboru Endou and Yasunari Shidama. Integral of measurable function. *Formalized Mathematics*, 14(**2**):53–70, 2006.

[12] Noboru Endou, Yasunari Shidama, and Keiko Narita. Egoroff's theorem. *Formalized Mathematics*, 16(**1**):57–63, 2008.

[13] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Basic properties of extended real numbers. *Formalized Mathematics*, 9(**3**):491–494, 2001.

[14] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definitions and basic properties of measurable functions. *Formalized Mathematics*, 9(**3**):495–500, 2001.

[15] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. The measurability of extended real valued functions. *Formalized Mathematics*, 9(**3**):525–529, 2001.

[16] P. R. Halmos. *Measure Theory*. Springer-Verlag, 1987.

[17] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.

[18] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[19] Beata Perkowska. Functional sequence from a domain to a domain. *Formalized Mathematics*, 3(**1**):17–21, 1992.

[20] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[21] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[22] Hiroshi Yamazaki, Noboru Endou, Yasunari Shidama, and Hiroyuki Okazaki. Inferior limit, superior limit and convergence of sequences of extended real numbers. *Formalized Mathematics*, 15(**4**):231–236, 2007.

Received March 18, 2008

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 177–194, 2008

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: $t_1 \div t_2$, $t_1 \bmod t_2$, $\mathrm{leq}(t_1, t_2)$, $\mathrm{gt}(t_1, t_2)$, 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 $(\mathrm{leq}(t_1, t_2))(s) = (t_1(s) > t_2(s) \rightarrow 0, 1)$.

(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 $(\mathrm{gt}(t_1, t_2))(s) = (t_1(s) > t_2(s) \rightarrow 1, 0)$.

(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 $(\mathrm{eq}(t_1, t_2))(s) = (t_1(s) = t_2(s) \rightarrow 1, 0)$.

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 $v\!:=\!t$ yielding an element of A is defined as follows:

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

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 $v\!:=\!t \in \mathrm{ElementaryInstructions}_A$.

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 $v\!:=\!t$ 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 $v\texttt{+=}t$ and $v\texttt{*=}t$ yielding absolutely-terminating elements of A are defined by:

(Def. 39) $v\texttt{+=}t = v\!:=\!(\dot{v} + t)$.

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

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 $x\!:=\!t$ yielding an absolutely-terminating element of A is defined as follows:

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

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

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

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 $x\!:=\!v$ yields an absolutely-terminating element of A and is defined by:

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

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

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

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

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

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 $\mathbb{Z}^X \upharpoonright^{b}_{\neq 0}$, 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) $t_1 \operatorname{eq} t_2 = b := \operatorname{eq}(t_1, t_2)$.

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 $f(s,$

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

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

(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 $g(s,\, x\,\mathrm{leq}\,i)(b) = 1$,

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

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

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

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

(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 $g(s,\, x\,\mathrm{leq}\,y)(b) = 1$ and if $s(x) > s(y)$, then $g(s,\, x\,\mathrm{leq}\,y)(b) = 0$ and for every z such that $z \neq b$ holds $g(s,\, x\,\mathrm{leq}\,y)(z) = s(z)$.

(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 $g(s,\, x\,\mathrm{leq}\,i) \in \mathbb{Z}^X{\restriction}^{b}_{\neq 0}$, and

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

(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 $g(s,\, x\,\mathrm{leq}\,y) \in \mathbb{Z}^X{\restriction}^{b}_{\neq 0}$, and

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

(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 $g(s,\, x\,\mathrm{gt}\,i)(b) = 1$,

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

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

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

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

(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 $g(s,\, x\,\mathrm{gt}\,y)(b) = 1$,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(ii) $s(x)$ is even iff $g(s,\, x$ 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:

- $\mathcal{E} = \texttt{for}\,\mathcal{G}\,\texttt{:=}\,\mathcal{J}\ \texttt{until}\ \mathcal{G}\,\mathrm{leq}\,\mathcal{H}\ \texttt{step}\ \mathcal{G}\texttt{+=}\,1\ \texttt{do}\ \mathcal{D}\ \texttt{done}$,
- $\mathcal{P}[\mathcal{F}(\mathcal{I},\, \mathcal{G}\,\texttt{:=}\,\mathcal{J})]$,
- 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 $\mathcal{P}[\mathcal{F}(s,\, \mathcal{G}\,\mathrm{leq}\,\mathcal{H})]$,
- 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:

- $\mathcal{E} = \texttt{for}\,\mathcal{G}\,\texttt{:=}\,\mathcal{J}\ \texttt{until}\ \dot{\mathcal{H}}\,\mathrm{leq}\,\dot{\mathcal{G}}\ \texttt{step}\ \mathcal{G}\texttt{+=}\,(-1)\ \texttt{do}\ \mathcal{D}\ \texttt{done}$,
- $\mathcal{P}[\mathcal{F}(\mathcal{I},\, \mathcal{G}\,\texttt{:=}\,\mathcal{J})]$,
- 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 $\mathcal{P}[\mathcal{F}(s,\, \mathcal{H}\,\mathrm{leq}\,\mathcal{G})]$,
- 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 $I; i \texttt{+=} 1; i \,\mathrm{leq}\, n$ terminates w.r.t. $g(s, i \,\mathrm{leq}\, n)$.

(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 $g(s, I)$, $g(s, i \,\mathrm{leq}\, n)$, $g(s, i \texttt{+=} 1) \in P$.

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

(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 $\texttt{for}\, i \texttt{:=} t \;\texttt{until}\; i \,\mathrm{leq}\, n \;\texttt{step}\; i \texttt{+=} 1 \;\texttt{do}\; I \;\texttt{done}$ 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. $i \,\mathrm{leq}\, n$ and g, and invariant w.r.t. $i \texttt{+=} 1$ and g.

Then $\texttt{for}\, i \texttt{:=} t \;\texttt{until}\; i \,\mathrm{leq}\, n \;\texttt{step}\; i \texttt{+=} 1 \;\texttt{do}\; I \;\texttt{done}$ 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 $g(s, \mathit{Fib})(x) = \mathrm{Fib}(N)$.

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 $g(s, \mathit{GCD}_1)(x) = \gcd(n, m)$.

Let GCD_2 denotes the program:

```
while $y$ gt $0$ do
  $z$ := $(\dot{x} - \dot{y})$;
  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

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 195–202, 2008

Invertibility of Matrices of Field Elements

Yatsuka Nakamura
Shinshu University
Nagano, Japan

Kunio Oniumi
Shinshu University
Nagano, Japan

Wenpai Chang
Nan Kai Institute of Technology
Nantou County, Taiwan

Summary. In this paper the theory of invertibility of matrices of field elements (see e.g. [5], [6]) is developed. The main purpose of this article is to prove that the left invertibility and the right invertibility are equivalent for a matrix of field elements. To prove this, we introduced a special transformation of matrix to some canonical forms. Other concepts as zero vector and base vectors of field elements are also introduced as a preparation.

MML identifier: `MATRIX14`, version: `7.9.01 4.101.1015`

The papers [14], [3], [7], [17], [4], [13], [15], [10], [1], [12], [18], [16], [9], [8], [2], and [11] provide the terminology and notation for this paper.

1. Preliminaries

We use the following convention: x, y denote sets, n, m, i, j denote elements of $\mathbb{N}$, and K denotes a field.

Let K be a non empty zero structure and let us consider n. The functor 0^n_K yields a finite sequence of elements of K and is defined by:

(Def. 1) $0^n_K = n \mapsto 0_K$.

Let K be a non empty zero structure and let us consider n. Then 0^n_K is an element of (the carrier of K)^n.

In the sequel L denotes a non empty additive loop structure.

The following three propositions are true:

ISSN 1426–2630(p), 1898-9934(e)

(1) Every finite sequence x of elements of L is an element of (the carrier of $L)^{\operatorname{len} x}$.

(2) For all finite sequences x_1, x_2 of elements of L such that $\operatorname{len} x_1 = \operatorname{len} x_2$ holds $\operatorname{len}(x_1 + x_2) = \operatorname{len} x_1$.

(3) For all finite sequences x_1, x_2 of elements of L such that $\operatorname{len} x_1 = \operatorname{len} x_2$ holds $\operatorname{len}(x_1 - x_2) = \operatorname{len} x_1$.

In the sequel G is a non empty multiplicative loop structure.

Next we state four propositions:

(4) Let x_1, x_2 be finite sequences of elements of G and given i. If $i \in \operatorname{dom}(x_1 \bullet x_2)$, then $(x_1 \bullet x_2)(i) = (x_1)_i \cdot (x_2)_i$ and $(x_1 \bullet x_2)_i = (x_1)_i \cdot (x_2)_i$.

(5) Let x_1, x_2 be finite sequences of elements of L and i be a natural number. If $\operatorname{len} x_1 = \operatorname{len} x_2$ and $1 \leq i \leq \operatorname{len} x_1$, then $(x_1 + x_2)(i) = (x_1)_i + (x_2)_i$ and $(x_1 - x_2)(i) = (x_1)_i - (x_2)_i$.

(6) For every element a of K and for every finite sequence x of elements of K holds $-a \cdot x = (-a) \cdot x$ and $-a \cdot x = a \cdot -x$.

(7) For all finite sequences x_1, x_2, y_1, y_2 of elements of G such that $\operatorname{len} x_1 = \operatorname{len} x_2$ and $\operatorname{len} y_1 = \operatorname{len} y_2$ holds $x_1 \frown y_1 \bullet x_2 \frown y_2 = (x_1 \bullet x_2) \frown (y_1 \bullet y_2)$.

Let us consider K and let e_1, e_2 be finite sequences of elements of K. We introduce $|(e_1, e_2)|$ as a synonym of $e_1 \cdot e_2$.

Next we state several propositions:

(8) Let x, y be finite sequences of elements of K and a be an element of K. If $\operatorname{len} x = \operatorname{len} y$, then $a \cdot x \bullet y = a \cdot (x \bullet y)$ and $x \bullet a \cdot y = a \cdot (x \bullet y)$.

(9) For all finite sequences x, y of elements of K and for every element a of K such that $\operatorname{len} x = \operatorname{len} y$ holds $|(a \cdot x, y)| = a \cdot |(x, y)|$.

(10) For all finite sequences x, y of elements of K and for every element a of K such that $\operatorname{len} x = \operatorname{len} y$ holds $|(x, a \cdot y)| = a \cdot |(x, y)|$.

(11) Let x, y_1, y_2 be finite sequences of elements of K and a be an element of K. If $\operatorname{len} x = \operatorname{len} y_1$ and $\operatorname{len} x = \operatorname{len} y_2$, then $|(x, y_1 + y_2)| = |(x, y_1)| + |(x, y_2)|$.

(12) For all finite sequences x_1, x_2, y_1, y_2 of elements of K such that $\operatorname{len} x_1 = \operatorname{len} x_2$ and $\operatorname{len} y_1 = \operatorname{len} y_2$ holds $|(x_1 \frown y_1, x_2 \frown y_2)| = |(x_1, x_2)| + |(y_1, y_2)|$.

(13) For every element p_1 of (the carrier of $K)^n$ holds $p_1 \bullet n \mapsto 0_K = n \mapsto 0_K$.

Let us consider n, let us consider K, and let A be a square matrix over K of dimension n. We introduce $\operatorname{Inv} A$ as a synonym of $A^{\smile}$.

2. Zero Vector and Base Vectors of Field Elements

Next we state several propositions:

(14) $I_K^{0 \times 0} = 0_K^{0 \times 0}$ and $I_K^{0 \times 0} = \emptyset$.

(15) For every square matrix A over K of dimension 0 holds $A = \emptyset$ and $A = I_K^{0\times 0}$ and $A = 0_K^{0\times 0}$.

(16) Every square matrix over K of dimension 0 is invertible.

(17) For all square matrices A, B, C over K of dimension n holds $(A\cdot B)\cdot C = A\cdot(B\cdot C)$.

(18) Let A, B be square matrices over K of dimension n. Then A is invertible and $B = A^{\smile}$ if and only if $B\cdot A = I_K^{n\times n}$ and $A\cdot B = I_K^{n\times n}$.

(19) Let A be a square matrix over K of dimension n. Then A is invertible if and only if there exists a square matrix B over K of dimension n such that $B\cdot A = I_K^{n\times n}$ and $A\cdot B = I_K^{n\times n}$.

(20) For every finite sequence x of elements of K holds $|(x, 0_K^{\mathrm{len}\,x})| = 0_K$.

(21) For every finite sequence x of elements of K holds $|(0_K^{\mathrm{len}\,x}, x)| = 0_K$.

(22) For every element a of K holds $|(\langle 0_K\rangle, \langle a\rangle)| = 0_K$.

Let K be a non empty set, let n be a natural number, and let a be an element of K. Then $n \mapsto a$ is a finite sequence of elements of K.

Let us consider K and let n, i be natural numbers. The i-versor in K^n yields a finite sequence of elements of K and is defined by:

(Def. 2) The i-versor in $K^n = \mathrm{Replace}(n \mapsto 0_K, i, 1_K)$.

Next we state several propositions:

(23) For all natural numbers n, i holds len (the i-versor in K^n) $= n$.

(24) For all natural numbers i, n such that $1 \leq i \leq n$ holds (the i-versor in $K^n)(i) = 1_K$.

(25) Let i, j, n be natural numbers. Suppose $1 \leq i \leq n$ and $1 \leq j \leq n$ and $i \neq j$. Then (the i-versor in $K^n)(j) = 0_K$.

(26) For all natural numbers i, n such that $1 \leq i \leq n$ holds $I_K^{n\times n}(i) =$ the i-versor in K^n.

(27) For all i, j such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds ${I_K^{n\times n}}_{i,j} =$ (the i-versor in $K^n)(j)$.

(28) Let A be a square matrix over K of dimension n. Then $A = 0_K^{n\times n}$ if and only if for all elements i, j of $\mathbb{N}$ such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds $A_{i,j} = 0_K$.

(29) Let A be a square matrix over K of dimension n. Then $A = I_K^{n\times n}$ if and only if for all elements i, j of $\mathbb{N}$ such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds $A_{i,j} = (i = j \rightarrow 1_K, 0_K)$.

3. Conditions of Invertibility

One can prove the following propositions:

(30) For all square matrices A, B over K of dimension n holds $(A \cdot B)^{\mathrm{T}} = B^{\mathrm{T}} \cdot A^{\mathrm{T}}$.

(31) For every square matrix A over K of dimension n such that A is invertible holds A^{T} is invertible and $(A^{\mathrm{T}})^{\smile} = (A^{\smile})^{\mathrm{T}}$.

(32) Let x be a finite sequence of elements of K and a be an element of K. Given i such that $1 \leq i \leq \mathrm{len}\, x$ and $x(i) = a$ and for every j such that $j \neq i$ and $1 \leq j \leq \mathrm{len}\, x$ holds $x(j) = 0_K$. Then $\sum x = a$.

(33) Let f_1, f_2 be finite sequences of elements of K. Then $\mathrm{dom}(f_1 \bullet f_2) = \mathrm{dom}\, f_1 \cap \mathrm{dom}\, f_2$ and for every i such that $i \in \mathrm{dom}(f_1 \bullet f_2)$ holds $(f_1 \bullet f_2)(i) = (f_1)_i \cdot (f_2)_i$.

(34) Let x, y be finite sequences of elements of K and given i. Suppose $\mathrm{len}\, x = m$ and $y = x \bullet$ the i-versor in K^m and $1 \leq i \leq m$. Then $y(i) = x(i)$ and for every j such that $j \neq i$ and $1 \leq j \leq m$ holds $y(j) = 0_K$.

(35) Let x be a finite sequence of elements of K. Suppose $\mathrm{len}\, x = m$ and $1 \leq i \leq m$. Then $|(x, \text{the } i\text{-versor in } K^m)| = x(i)$ and $|(x, \text{the } i\text{-versor in } K^m)| = x_i$.

(36) For all m, i such that $1 \leq i \leq m$ holds $|(\text{the } i\text{-versor in } K^m, \text{the } i\text{-versor in } K^m)| = 1_K$.

(37) Let a be an element of K and P, Q be square matrices over K of dimension n. Suppose that $n > 0$ and $a \neq 0_K$ and $P_{1,1} = a^{-1}$ and for every i such that $1 < i \leq n$ holds $P(i) =$ the i-versor in K^n and $Q_{1,1} = a$ and for every j such that $1 < j \leq n$ holds $Q_{1,j} = -a \cdot P_{1,j}$ and for every i such that $1 < i \leq n$ holds $Q(i) =$ the i-versor in K^n. Then P is invertible and $Q = P^{\smile}$.

(38) Let a be an element of K and P be a square matrix over K of dimension n. Suppose $n > 0$ and $a \neq 0_K$ and $P_{1,1} = a^{-1}$ and for every i such that $1 < i \leq n$ holds $P(i) =$ the i-versor in K^n. Then P is invertible.

(39) Let A be a square matrix over K of dimension n. Suppose $n > 0$ and $A_{1,1} \neq 0_K$. Then there exists a square matrix P over K of dimension n such that

(i) P is invertible,

(ii) $(A \cdot P)_{1,1} = 1_K$,

(iii) for every j such that $1 < j \leq n$ holds $(A \cdot P)_{1,j} = 0_K$, and

(iv) for every i such that $1 < i \leq n$ and $A_{i,1} = 0_K$ holds $(A \cdot P)_{i,1} = 0_K$.

(40) Let A be a square matrix over K of dimension n. Suppose $n > 0$ and $A_{1,1} \neq 0_K$. Then there exists a square matrix P over K of dimension n such that

(i) P is invertible,

(ii) $(P \cdot A)_{1,1} = 1_K$,

(iii) for every i such that $1 < i \leq n$ holds $(P \cdot A)_{i,1} = 0_K$, and

(iv) for every j such that $1 < j \leq n$ and $A_{1,j} = 0_K$ holds $(P \cdot A)_{1,j} = 0_K$.

(41) Let A be a square matrix over K of dimension n. Suppose $n > 0$ and $A_{1,1} \neq 0_K$. Then there exist square matrices P, Q over K of dimension n such that

(i) P is invertible,

(ii) Q is invertible,

(iii) $(P \cdot A \cdot Q)_{1,1} = 1_K$,

(iv) for every i such that $1 < i \leq n$ holds $(P \cdot A \cdot Q)_{i,1} = 0_K$, and

(v) for every j such that $1 < j \leq n$ holds $(P \cdot A \cdot Q)_{1,j} = 0_K$.

4. A Transformation of Matrix to Some Canonical Form

We now state the proposition

(42) Let D be a non empty set, m, n, i, j be elements of $\mathbb{N}$, and A be a matrix over D of dimension $m \times n$. Then $\mathrm{Swap}(A, i, j)$ is a matrix over D of dimension $m \times n$.

Let us consider K, let n be an element of $\mathbb{N}$, and let i_0 be a natural number. The functor $\mathrm{SwapDiagonal}(K, n, i_0)$ yields a square matrix over K of dimension n and is defined as follows:

(Def. 3) $\mathrm{SwapDiagonal}(K, n, i_0) = \mathrm{Swap}(I_K^{n \times n}, 1, i_0)$.

Next we state a number of propositions:

(43) Let n be an element of $\mathbb{N}$, i_0 be a natural number, and A be a square matrix over K of dimension n. Suppose $1 \leq i_0 \leq n$ and $A = \mathrm{SwapDiagonal}(K, n, i_0)$. Let i, j be natural numbers. Suppose $1 \leq i \leq n$ and $1 \leq j \leq n$. Suppose $i_0 \neq 1$. Then

(i) if $i = 1$ and $j = i_0$, then $A_{i,j} = 1_K$,

(ii) if $i = i_0$ and $j = 1$, then $A_{i,j} = 1_K$,

(iii) if $i = 1$ and $j = 1$, then $A_{i,j} = 0_K$,

(iv) if $i = i_0$ and $j = i_0$, then $A_{i,j} = 0_K$, and

(v) if $i \neq 1$ and $i \neq i_0$ or $j \neq 1$ and $j \neq i_0$, then if $i = j$, then $A_{i,j} = 1_K$ and if $i \neq j$, then $A_{i,j} = 0_K$.

(44) Let n be an element of $\mathbb{N}$, A be a square matrix over K of dimension n, and i be a natural number. If $1 \leq i \leq n$, then $(\mathrm{SwapDiagonal}(K, n, 1))_{i,i} = 1_K$.

(45) Let n be an element of $\mathbb{N}$, A be a square matrix over K of dimension n, and i, j be natural numbers. If $1 \leq i \leq n$ and $1 \leq j \leq n$, then if $i \neq j$, then $(\mathrm{SwapDiagonal}(K, n, 1))_{i,j} = 0_K$.

(46) Let given K, n, i_0 be elements of $\mathbb{N}$, and A be a square matrix over K of dimension n. Suppose that

(i) $1 \leq i_0$,

(ii) $i_0 \leq n$,

(iii) $i_0 = 1$, and

(iv) for all natural numbers i, j such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds if $i = j$, then $A_{i,j} = 1_K$ and if $i \neq j$, then $A_{i,j} = 0_K$.

Then $A = \mathrm{SwapDiagonal}(K, n, i_0)$.

(47) Let given K, n, i_0 be elements of $\mathbb{N}$, and A be a square matrix over K of dimension n. Suppose that

(i) $1 \leq i_0$,

(ii) $i_0 \leq n$,

(iii) $i_0 \neq 1$, and

(iv) for all natural numbers i, j such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds if $i = 1$ and $j = i_0$, then $A_{i,j} = 1_K$ and if $i = i_0$ and $j = 1$, then $A_{i,j} = 1_K$ and if $i = 1$ and $j = 1$, then $A_{i,j} = 0_K$ and if $i = i_0$ and $j = i_0$, then $A_{i,j} = 0_K$ and if $i \neq 1$ and $i \neq i_0$ or $j \neq 1$ and $j \neq i_0$, then if $i = j$, then $A_{i,j} = 1_K$ and if $i \neq j$, then $A_{i,j} = 0_K$.

Then $A = \mathrm{SwapDiagonal}(K, n, i_0)$.

(48) Let A be a square matrix over K of dimension n and i_0 be an element of $\mathbb{N}$. Suppose $1 \leq i_0 \leq n$. Then

(i) for every j such that $1 \leq j \leq n$ holds $(\mathrm{SwapDiagonal}(K, n, i_0) \cdot A)_{i_0,j} = A_{1,j}$ and $(\mathrm{SwapDiagonal}(K, n, i_0) \cdot A)_{1,j} = A_{i_0,j}$, and

(ii) for all i, j such that $i \neq 1$ and $i \neq i_0$ and $1 \leq i \leq n$ and $1 \leq j \leq n$ holds $(\mathrm{SwapDiagonal}(K, n, i_0) \cdot A)_{i,j} = A_{i,j}$.

(49) For every element i_0 of $\mathbb{N}$ such that $1 \leq i_0 \leq n$ holds $\mathrm{SwapDiagonal}(K, n, i_0)$ is invertible and $(\mathrm{SwapDiagonal}(K, n, i_0))^{\smile} = \mathrm{SwapDiagonal}(K, n, i_0)$.

(50) For every element i_0 of $\mathbb{N}$ such that $1 \leq i_0 \leq n$ holds $(\mathrm{SwapDiagonal}(K, n, i_0))^{\mathrm{T}} = \mathrm{SwapDiagonal}(K, n, i_0)$.

(51) Let A be a square matrix over K of dimension n and j_0 be an element of $\mathbb{N}$. Suppose $1 \leq j_0 \leq n$. Then

(i) for every i such that $1 \leq i \leq n$ holds $(A \cdot \mathrm{SwapDiagonal}(K, n, j_0))_{i,j_0} = A_{i,1}$ and $(A \cdot \mathrm{SwapDiagonal}(K, n, j_0))_{i,1} = A_{i,j_0}$, and

(ii) for all i, j such that $j \neq 1$ and $j \neq j_0$ and $1 \leq i \leq n$ and $1 \leq j \leq n$ holds $(A \cdot \mathrm{SwapDiagonal}(K, n, j_0))_{i,j} = A_{i,j}$.

(52) Let A be a square matrix over K of dimension n. Then $A = 0_K^{n \times n}$ if and only if for all i, j such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds $A_{i,j} = 0_K$.

5. Left/Right Invertibility and Invertibility

The following four propositions are true:

(53) Let A be a square matrix over K of dimension n. Suppose $A \neq 0_K^{n \times n}$. Then there exist square matrices B, C over K of dimension n such that

(i) B is invertible,

(ii) C is invertible,

(iii) $(B \cdot A \cdot C)_{1,1} = 1_K$,

(iv) for every i such that $1 < i \leq n$ holds $(B \cdot A \cdot C)_{i,1} = 0_K$, and

(v) for every j such that $1 < j \leq n$ holds $(B \cdot A \cdot C)_{1,j} = 0_K$.

(54) Let A, B be square matrices over K of dimension n. Suppose $B \cdot A = I_K^{n \times n}$. Then there exists a square matrix B_2 over K of dimension n such that $A \cdot B_2 = I_K^{n \times n}$.

(55) Let A be a square matrix over K of dimension n. Then the following statements are equivalent

(i) there exists a square matrix B_1 over K of dimension n such that $B_1 \cdot A = I_K^{n \times n}$,

(ii) there exists a square matrix B_2 over K of dimension n such that $A \cdot B_2 = I_K^{n \times n}$.

(56) For all square matrices A, B over K of dimension n such that $A \cdot B = I_K^{n \times n}$ holds A is invertible and B is invertible.

References

[1] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[2] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[4] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[5] Shigeru Furuya. *Matrix and Determinant.* Baifuukan (in Japanese), 1957.

[6] Felix R. Gantmacher. *The Theory of Matrices.* AMS Chelsea Publishing, 1959.

[7] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.

[8] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[9] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[10] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[11] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.

[12] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[13] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[14] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[15] Hiroshi Yamazaki, Yoshinori Fujisawa, and Yatsuka Nakamura. On replace function and swap function for finite sequences. *Formalized Mathematics*, 9(**3**):471–474, 2001.

[16] Xiaopeng Yue, Xiquan Liang, and Zhongpin Sun. Some properties of some special matrices. *Formalized Mathematics*, 13(**4**):541–547, 2005.

[17] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.

[18] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

Received April 2, 2008

FORMALIZED MATHEMATICS
Vol. 16, No. 2, Pages 203–205, 2008

Ramsey's Theorem

Marco Riccardi
Casella Postale 49
54038 Montignoso, Italy

Summary. The goal of this article is to formalize two versions of Ramsey's theorem. The theorems are not phrased in the usually pictorial representation of a coloured graph but use a set-theoretic terminology. After some useful lemma, the second section presents a generalization of Ramsey's theorem on infinite set closely following the book [9]. The last section includes the formalization of the theorem in a more known version (see [1]).

MML identifier: `RAMSEY_1`, version: `7.9.01 4.101.1015`

The notation and terminology used here are introduced in the following papers: [15], [16], [17], [4], [3], [6], [12], [7], [2], [5], [8], [14], [13], [10], and [11].

1. Preliminaries

For simplicity, we adopt the following convention: n, m, k are natural numbers, X, Y, Z are sets, f is a function from X into Y, and H is a subset of X.

Let us consider X, Y, H and let P be a partition of $[X]^Y$. We say that H is homogeneous for P if and only if:

(Def. 1) There exists an element p of P such that $[H]^Y \subseteq p$.

Let us consider n and let X be an infinite set. One can check that $[X]^n$ is non empty.

Let us consider n, X, Y, f. Let us assume that f is one-to-one and $\overline{\overline{n}} \subseteq \overline{\overline{X}}$ and X is non empty and Y is non empty. The functor $f||^n$ yields a function from $[X]^n$ into $[Y]^n$ and is defined by:

(Def. 2) For every element x of $[X]^n$ holds $(f||^n)(x) = f^\circ x$.

Next we state four propositions:

ISSN 1426–2630(p), 1898-9934(e)

(1) If f is one-to-one and $\overline{\overline{n}} \subseteq \overline{\overline{X}}$ and X is non empty and Y is non empty, then $[f^{\circ}H]^{n} = (f||^{n})^{\circ}([H]^{n})$.

(2) If X is infinite and $X \subseteq \omega$, then $\overline{\overline{X}} = \omega$.

(3) If X is infinite, then $X \cup Y$ is infinite.

(4) If X is infinite and Y is finite, then $X \setminus Y$ is infinite.

Let X be an infinite set and let Y be a set. Note that $X \cup Y$ is infinite.

Let X be an infinite set and let Y be a finite set. One can verify that $X \setminus Y$ is infinite.

The following propositions are true:

(5) $[X]^{0} = \{0\}$.

(6) For every finite set X such that $\operatorname{card} X < n$ holds $[X]^{n}$ is empty.

(7) If $X \subseteq Y$, then $[X]^{Z} \subseteq [Y]^{Z}$.

(8) If X is finite and Y is finite and $\overline{\overline{Y}} = X$, then $[Y]^{X} = \{Y\}$.

(9) If X is non empty and Y is non empty, then f is constant iff there exists an element y of Y such that $\operatorname{rng} f = \{y\}$.

(10) For every finite set X such that $k \leq \operatorname{card} X$ there exists a subset Y of X such that $\operatorname{card} Y = k$.

(11) If $m \geq 1$, then $n + 1 \leq \binom{n+m}{m}$.

(12) If $m \geq 1$ and $n \geq 1$, then $m + 1 \leq \binom{n+m}{m}$.

(13) Let X be a non empty set, p_1, p_2 be elements of X, P be a partition of X, and A be an element of P. Suppose $p_1 \in A$ and (the projection onto P)(p_1) = (the projection onto P)(p_2). Then $p_2 \in A$.

2. Infinite Ramsey Theorem

We now state two propositions:

(14) Let F be a function from $[X]^{n}$ into k. Suppose $k \neq 0$ and X is infinite. Then there exists H such that H is infinite and $F{\restriction}[H]^{n}$ is constant.

(15) Let X be an infinite set and P be a partition of $[X]^{n}$. If $\overline{\overline{P}} = k$, then there exists a subset of X which is infinite and homogeneous for P.

3. Ramsey's Theorem

The scheme *BinInd2* concerns a binary predicate $\mathcal{P}$, and states that:

$\mathcal{P}[m, n]$

provided the following conditions are satisfied:

- $\mathcal{P}[0, n]$ and $\mathcal{P}[n, 0]$, and
- If $\mathcal{P}[m + 1, n]$ and $\mathcal{P}[m, n + 1]$, then $\mathcal{P}[m + 1, n + 1]$.

We now state two propositions:

(16) Suppose $m \geq 2$ and $n \geq 2$. Then there exists a natural number r such that

(i) $r \leq \binom{(m+n)-'2}{m-'1}$,

(ii) $r \geq 2$, and

(iii) for every finite set X and for every function F from $[X]^2$ into $\mathrm{Seg}\,2$ such that $\mathrm{card}\,X \geq r$ there exists a subset S of X such that $\mathrm{card}\,S \geq m$ and $\mathrm{rng}(F{\restriction}[S]^2) = \{1\}$ or $\mathrm{card}\,S \geq n$ and $\mathrm{rng}(F{\restriction}[S]^2) = \{2\}$.

(17) Let m be a natural number. Then there exists a natural number r such that for every finite set X and for every partition P of $[X]^2$ if $\mathrm{card}\,X \geq r$ and $\overline{\overline{P}} = 2$, then there exists a subset S of X such that $\mathrm{card}\,S \geq m$ and S is homogeneous for P.

References

[1] M. Aigner and G. M. Ziegler. *Proofs from THE BOOK.* Springer-Verlag, Berlin Heidelberg New York, 2004.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[7] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[8] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[9] T. J. Jech. *Set Theory.* Springer-Verlag, Berlin Heidelberg New York, 2002.

[10] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[11] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[12] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.

[13] Marco Riccardi. The sylow theorems. *Formalized Mathematics*, 15(**3**):159–165, 2007.

[14] Andrzej Trybulec. A Borsuk theorem on homotopy types. *Formalized Mathematics*, 2(**4**):535–545, 1991.

[15] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[16] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[17] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received April 18, 2008

FORMALIZED MATHEMATICS
Vol. **16**, No. **2**, Pages 207–230, **2008**

Towards the Construction of a Model of Mizar Concepts[1]

Grzegorz Bancerek
Białystok Technical University
Poland

Summary. The aim of this paper is to develop a formal theory of Mizar linguistic concepts following the ideas from [14] and [13]. The theory here presented is an abstract of the existing implementation of the Mizar system and is devoted to the formalization of Mizar expressions. The base idea behind the formalization is dependence on variables which is determined by variable-dependence (variables may depend on other variables). The dependence constitutes a Galois connection between opposite poset of dependence-closed set of variables and the sup-semilattice of widening of Mizar types (smooth type widening).

In the paper the concepts strictly connected with Mizar expressions are formalized. Among them are quasi-loci, quasi-terms, quasi-adjectives, and quasi-types. The structural induction and operation of substitution are also introduced. The prefix *quasi* is used to indicate that some rules of construction of Mizar expressions may not be fulfilled. For example, variables, quasi-loci, and quasi-terms have no assigned types and, in result, there is no possibility to conduct type-checking of arguments. The other gaps concern inconsistent and out-of-context clusters of adjectives in types. Those rules are required in the Mizar *identification* process. However, the expression appearing in later processes of Mizar checker may not satisfy the rules. So, introduced apparatus is enough and adequate to describe data structures and algorithms from the Mizar checker (like *equational classes*).

MML identifier: `ABCMIZ_1`, version: `7.9.01 4.101.1015`

The notation and terminology used in this paper are introduced in the following papers: [24], [41], [33], [30], [42], [20], [43], [39], [23], [17], [34], [21], [22], [32], [2],

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

ISSN 1426–2630(p), 1898-9934(e)

[38], [35], [26], [1], [4], [15], [19], [28], [3], [7], [8], [9], [36], [25], [5], [40], [6], [11], [12], [27], [18], [37], [29], [31], [10], and [16].

1. Variables

We adopt the following convention: i is a natural number, j is an element of $\mathbb{N}$, and X, Y, x, y, z are sets.

One can prove the following propositions:

(1) For every function f holds $f(x) \subseteq \bigcup f$.

(2) For every function f such that $\bigcup f = \emptyset$ holds $f(x) = \emptyset$.

(3) For every function f and for all sets x, y such that $f = \langle x, y\rangle$ holds $x = y$.

(4) $(\mathrm{id}_X)^\circ Y \subseteq Y$.

(5) Let Σ be a non void signature and X be a non-empty many sorted set indexed by the carrier of Σ. Then every term of Σ over X is non pair.

Let Σ be a non void signature and let X be a non empty yielding many sorted set indexed by the carrier of Σ. Observe that every element of $\mathrm{Free}_\Sigma(X)$ is non pair.

We now state the proposition

(6) For all sets x, y, z such that $x, y \in \{z\}^*$ and $\overline{\overline{x}} = \overline{\overline{y}}$ holds $x = y$.

Let us note that $\emptyset$ is decorated tree yielding.

Let Σ be a non void signature and let $\mathfrak{A}$ be an algebra over Σ. A subset of $\mathfrak{A}$ is a subset of $\bigcup$(the sorts of $\mathfrak{A}$). A finite sequence of elements of $\mathfrak{A}$ is a finite sequence of elements of $\bigcup$(the sorts of $\mathfrak{A}$).

Let Σ be a non void signature and let X be a non empty yielding many sorted set indexed by Σ. Note that every finite sequence of elements of $\mathrm{Free}_\Sigma(X)$ is decorated tree yielding.

Next we state the proposition

(7) Let Σ be a non void signature, X be a non empty yielding many sorted set indexed by the carrier of Σ, and τ be an element of $\mathrm{Free}_\Sigma(X)$. Then

(i) there exists a sort symbol s of Σ and there exists a set v such that $\tau =$ the root tree of $\langle v, s\rangle$ and $v \in X(s)$, or

(ii) there exists an operation symbol o of Σ and there exists a finite sequence p of elements of $\mathrm{Free}_\Sigma(X)$ such that $\tau = \langle o,$ the carrier of $\Sigma\rangle$-tree(p) and $\mathrm{len}\, p = \mathrm{len}\,\mathrm{Arity}(o)$ and p is decorated tree yielding and an argument sequence of $\mathrm{Sym}(o, X \cup ((\text{the carrier of } \Sigma) \longmapsto \{0\}))$.

Let A be a set. The functor $\mathrm{varcl}\, A$ is defined by the conditions (Def. 1).

(Def. 1)(i) $A \subseteq \mathrm{varcl}\, A$,

(ii) for all x, y such that $\langle x, y\rangle \in \mathrm{varcl}\, A$ holds $x \subseteq \mathrm{varcl}\, A$, and

(iii) for every set B such that $A \subseteq B$ and for all x, y such that $\langle x, y\rangle \in B$ holds $x \subseteq B$ holds $\operatorname{varcl} A \subseteq B$.

Let us observe that the functor $\operatorname{varcl} A$ is projective.

We now state three propositions:

(8) $\operatorname{varcl} \emptyset = \emptyset$.

(9) For all sets Y, Z such that $Y \subseteq Z$ holds $\operatorname{varcl} Y \subseteq \operatorname{varcl} Z$.

(10) For every set Z holds $\operatorname{varcl} \bigcup Z = \bigcup\{\operatorname{varcl} z : z$ ranges over elements of $Z\}$.

The scheme *Sch14* deals with a set $\mathcal{A}$, a unary functor $\mathcal{F}$ yielding a set, and a unary predicate $\mathcal{P}$, and states that:

$\operatorname{varcl} \bigcup\{\mathcal{F}(z); z$ ranges over elements of $\mathcal{A} : \mathcal{P}[z]\} = \bigcup\{\operatorname{varcl} \mathcal{F}(z); z$ ranges over elements of $\mathcal{A} : \mathcal{P}[z]\}$

for all values of the parameters.

Next we state three propositions:

(11) $\operatorname{varcl}(X \cup Y) = \operatorname{varcl} X \cup \operatorname{varcl} Y$.

(12) For every non empty set Z such that for every element z of Z holds $\operatorname{varcl} z = z$ holds $\operatorname{varcl} \bigcap Z = \bigcap Z$.

(13) $\operatorname{varcl}(\operatorname{varcl} X \cap \operatorname{varcl} Y) = \operatorname{varcl} X \cap \operatorname{varcl} Y$.

Let Z be an empty set. Observe that $\operatorname{varcl} Z$ is empty.

The functor Vars is defined by the condition (Def. 2).

(Def. 2) There exists a many sorted set V indexed by $\mathbb{N}$ such that

(i) $\mathrm{Vars} = \bigcup V$,

(ii) $V(0) = \{\langle \emptyset, i\rangle : i$ ranges over elements of $\mathbb{N}\}$, and

(iii) for every natural number n holds $V(n+1) = \{\langle \operatorname{varcl} Z, j\rangle; Z$ ranges over subsets of $V(n)$, j ranges over elements of $\mathbb{N}$: Z is finite$\}$.

Next we state a number of propositions:

(14) Let V be a many sorted set indexed by $\mathbb{N}$. Suppose that

(i) $V(0) = \{\langle \emptyset, i\rangle : i$ ranges over elements of $\mathbb{N}\}$, and

(ii) for every natural number n holds $V(n+1) = \{\langle \operatorname{varcl} Z, j\rangle; Z$ ranges over subsets of $V(n)$, j ranges over elements of $\mathbb{N}$: Z is finite$\}$.

Let i, j be elements of $\mathbb{N}$. If $i \leq j$, then $V(i) \subseteq V(j)$.

(15) Let V be a many sorted set indexed by $\mathbb{N}$. Suppose that

(i) $V(0) = \{\langle \emptyset, i\rangle : i$ ranges over elements of $\mathbb{N}\}$, and

(ii) for every natural number n holds $V(n+1) = \{\langle \operatorname{varcl} Z, j\rangle; Z$ ranges over subsets of $V(n)$, j ranges over elements of $\mathbb{N}$: Z is finite$\}$.

Let Z be a finite subset of Vars. Then there exists an element i of $\mathbb{N}$ such that $Z \subseteq V(i)$.

(16) $\{\langle \emptyset, i\rangle : i$ ranges over elements of $\mathbb{N}\} \subseteq \mathrm{Vars}$.

(17) For every finite subset Z of Vars and for every natural number i holds $\langle \operatorname{varcl} Z, i\rangle \in \mathrm{Vars}$.

(18) $\mathrm{Vars} = \{\langle \mathrm{varcl}\, Z, j\rangle; Z$ ranges over subsets of Vars, j ranges over elements of $\mathbb{N}$: Z is finite$\}$.

(19) $\mathrm{varcl}\,\mathrm{Vars} = \mathrm{Vars}$.

(20) For every X such that $\mathrm{rk}(X)$ is finite holds X is finite.

(21) $\mathrm{rk}(\mathrm{varcl}\, X) = \mathrm{rk}(X)$.

(22) For every finite subset X of $\mathbf{R}_\omega$ holds $X \in \mathbf{R}_\omega$.

(23) $\mathrm{Vars} \subseteq \mathbf{R}_\omega$.

(24) For every finite subset Z of Vars holds $\mathrm{varcl}\, Z$ is a finite subset of Vars.

One can verify that Vars is non empty.

A variable is an element of Vars.

Let x be a variable. Observe that $x_{\mathbf{1}}$ is finite.

Let x be a variable. We introduce $\mathrm{vars}(x)$ as a synonym of $x_{\mathbf{1}}$.

Let x be a variable. Then $\mathrm{vars}(x)$ is a subset of Vars.

The following propositions are true:

(25) $\langle \emptyset, i\rangle \in \mathrm{Vars}$.

(26) For every subset Z of Vars holds $\mathrm{varcl}\{\langle \mathrm{varcl}\, Z, j\rangle\} = \mathrm{varcl}\, Z \cup \{\langle \mathrm{varcl}\, Z, j\rangle\}$.

(27) For every variable x holds $\mathrm{varcl}\{x\} = \mathrm{vars}(x) \cup \{x\}$.

(28) For every variable x holds $\langle \mathrm{vars}(x) \cup \{x\}, i\rangle \in \mathrm{Vars}$.

2. Quasi-loci

Let R be a binary relation and let X be a set. We introduce $R\, \mathrm{dom}\, X$ as a synonym of $R{\restriction}X$.

The set QuasiLoci of finite sequences of Vars is defined by the condition (Def. 3).

(Def. 3) Let p be a finite sequence of elements of Vars. Then $p \in \mathrm{QuasiLoci}$ if and only if the following conditions are satisfied:

(i) p is one-to-one, and

(ii) for every i such that $i \in \mathrm{dom}\, p$ holds $p(i)_{\mathbf{1}} \subseteq \mathrm{rng}(p\, \mathrm{dom}\, i)$.

One can prove the following proposition

(29) $\varepsilon_{\mathrm{Vars}} \in \mathrm{QuasiLoci}$.

Let us observe that QuasiLoci is non empty.

A quasi-locus sequence is an element of QuasiLoci.

One can verify that every quasi-locus sequence is one-to-one.

Next we state several propositions:

(30) Let l be an one-to-one finite sequence of elements of Vars. Then l is a quasi-locus sequence if and only if for every natural number i and for every variable x such that $i \in \mathrm{dom}\, l$ and $x = l(i)$ and for every variable y such

that $y \in \mathrm{vars}(x)$ there exists a natural number j such that $j \in \mathrm{dom}\, l$ and $j < i$ and $y = l(j)$.

(31) Let l be a quasi-locus sequence and x be a variable. Then $l \mathbin{^\frown} \langle x \rangle$ is a quasi-locus sequence if and only if $x \notin \mathrm{rng}\, l$ and $\mathrm{vars}(x) \subseteq \mathrm{rng}\, l$.

(32) Let p_1, p_2 be finite sequences. Suppose $p_1 \mathbin{^\frown} p_2$ is a quasi-locus sequence. Then p_1 is a quasi-locus sequence and p_2 is a finite sequence of elements of Vars.

(33) For every quasi-locus sequence l holds $\mathrm{varcl}\, \mathrm{rng}\, l = \mathrm{rng}\, l$.

(34) For every variable x holds $\langle x \rangle$ is a quasi-locus sequence iff $\mathrm{vars}(x) = \emptyset$.

(35) For all variables x, y holds $\langle x, y \rangle$ is a quasi-locus sequence iff $\mathrm{vars}(x) = \emptyset$ and $x \neq y$ and $\mathrm{vars}(y) \subseteq \{x\}$.

(36) Let x, y, z be variables. Then $\langle x, y, z \rangle$ is a quasi-locus sequence if and only if $\mathrm{vars}(x) = \emptyset$ and $x \neq y$ and $\mathrm{vars}(y) \subseteq \{x\}$ and $x \neq z$ and $y \neq z$ and $\mathrm{vars}(z) \subseteq \{x, y\}$.

Let l be a quasi-locus sequence. Then l^{-1} is a partial function from Vars to $\mathbb{N}$.

3. Mizar Constructor Signature

The functor **type** is defined by:

(Def. 4) $\mathbf{type} = 0$.

The functor **adj** is defined by:

(Def. 5) $\mathbf{adj} = 1$.

The functor **term** is defined as follows:

(Def. 6) $\mathbf{term} = 2$.

The functor $*$ is defined by:

(Def. 7) $* = 0$.

The functor **non** is defined as follows:

(Def. 8) $\mathbf{non} = 1$.

Let $\mathfrak{C}$ be a signature. We say that $\mathfrak{C}$ is constructor if and only if the conditions (Def. 9) are satisfied.

(Def. 9) The carrier of $\mathfrak{C} = \{\mathbf{type}, \mathbf{adj}, \mathbf{term}\}$ and $\{*, \mathbf{non}\} \subseteq$ the operation symbols of $\mathfrak{C}$ and (the arity of $\mathfrak{C})(*) = \langle \mathbf{adj}, \mathbf{type} \rangle$ and (the arity of $\mathfrak{C})(\mathbf{non}) = \langle \mathbf{adj} \rangle$ and (the result sort of $\mathfrak{C})(*) = \mathbf{type}$ and (the result sort of $\mathfrak{C})(\mathbf{non}) = \mathbf{adj}$ and for every element o of the operation symbols of $\mathfrak{C}$ such that $o \neq *$ and $o \neq \mathbf{non}$ holds (the arity of $\mathfrak{C})(o) \in \{\mathbf{term}\}^*$.

Let us note that every signature which is constructor is also non empty and non void.

The strict signature MinConstrSign is defined by:

(Def. 10) MinConstrSign is constructor and the operation symbols of MinConstrSign $=$ $\{*, \mathbf{non}\}$.

Let us observe that MinConstrSign is constructor.

Let us observe that there exists a signature which is constructor and strict.

Let $\mathfrak{C}$ be a constructor signature and let o be an operation symbol of $\mathfrak{C}$. We say that o is constructor if and only if:

(Def. 11) $o \neq *$ and $o \neq \mathbf{non}$.

We now state the proposition

(37) Let Σ be a constructor signature and o be an operation symbol of Σ. If o is constructor, then $\mathrm{Arity}(o) = \mathrm{len}\,\mathrm{Arity}(o) \mapsto \mathbf{term}$.

Let $\mathfrak{C}$ be a non empty non void signature. We say that $\mathfrak{C}$ is initialized if and only if the condition (Def. 12) is satisfied.

(Def. 12) There exist operation symbols m, α of $\mathfrak{C}$ such that the result sort of $m =$ $\mathbf{type}$ and $\mathrm{Arity}(m) = \emptyset$ and the result sort of $\alpha = \mathbf{adj}$ and $\mathrm{Arity}(\alpha) = \emptyset$.

Let $\mathfrak{C}$ be a constructor signature. The functor $\mathbf{type}_{\mathfrak{C}}$ is a sort symbol of $\mathfrak{C}$ and is defined by:

(Def. 13) $\mathbf{type}_{\mathfrak{C}} = \mathbf{type}$.

The functor $\mathbf{adj}_{\mathfrak{C}}$ is a sort symbol of $\mathfrak{C}$ and is defined as follows:

(Def. 14) $\mathbf{adj}_{\mathfrak{C}} = \mathbf{adj}$.

The functor $\mathbf{term}_{\mathfrak{C}}$ is a sort symbol of $\mathfrak{C}$ and is defined by:

(Def. 15) $\mathbf{term}_{\mathfrak{C}} = \mathbf{term}$.

The functor $\mathbf{non}_{\mathfrak{C}}$ yielding an operation symbol of $\mathfrak{C}$ is defined as follows:

(Def. 16) $\mathbf{non}_{\mathfrak{C}} = \mathbf{non}$.

The functor $*_{\mathfrak{C}}$ yielding an operation symbol of $\mathfrak{C}$ is defined as follows:

(Def. 17) $*_{\mathfrak{C}} = *$.

We now state the proposition

(38) Let $\mathfrak{C}$ be a constructor signature. Then $\mathrm{Arity}(\mathbf{non}_{\mathfrak{C}}) = \langle \mathbf{adj}_{\mathfrak{C}} \rangle$ and the result sort of $\mathbf{non}_{\mathfrak{C}} = \mathbf{adj}_{\mathfrak{C}}$ and $\mathrm{Arity}(*_{\mathfrak{C}}) = \langle \mathbf{adj}_{\mathfrak{C}}, \mathbf{type}_{\mathfrak{C}} \rangle$ and the result sort of $*_{\mathfrak{C}} = \mathbf{type}_{\mathfrak{C}}$.

The functor Modes is defined as follows:

(Def. 18) $\mathrm{Modes} = \{\mathbf{type}\} \times (\mathrm{QuasiLoci} \times \mathbb{N})$.

The functor Attrs is defined as follows:

(Def. 19) $\mathrm{Attrs} = \{\mathbf{adj}\} \times (\mathrm{QuasiLoci} \times \mathbb{N})$.

The functor Funcs is defined by:

(Def. 20) $\mathrm{Funcs} = \{\mathbf{term}\} \times (\mathrm{QuasiLoci} \times \mathbb{N})$.

One can verify the following observations:

- $*$ Modes is non empty,
- $*$ Attrs is non empty, and

$*$ Funcs is non empty.

The non empty set Constructors is defined by:

(Def. 21) Constructors $=$ Modes $\cup$ Attrs $\cup$ Funcs.

Next we state the proposition

(39) $\{*, \mathbf{non}\}$ misses Constructors.

Let x be an element of QuasiLoci $\times \mathbb{N}$. Then $x_{\mathbf{1}}$ is a quasi-locus sequence. Then $x_{\mathbf{2}}$ is an element of $\mathbb{N}$.

Let c be an element of Constructors. We introduce the kind of c as a synonym of $c_{\mathbf{1}}$.

Let c be an element of Constructors. Then the kind of c is an element of $\{\mathbf{type}, \mathbf{adj}, \mathbf{term}\}$. Then $c_{\mathbf{2}}$ is an element of QuasiLoci $\times \mathbb{N}$.

Let c be an element of Constructors. The loci of c yields a quasi-locus sequence and is defined as follows:

(Def. 22) The loci of $c = (c_{\mathbf{2}})_{\mathbf{1}}$.

The index of c yielding a natural number is defined as follows:

(Def. 23) The index of $c = (c_{\mathbf{2}})_{\mathbf{2}}$.

We now state the proposition

(40) Let c be an element of Constructors. Then

(i) the kind of $c = \mathbf{type}$ iff $c \in$ Modes,

(ii) the kind of $c = \mathbf{adj}$ iff $c \in$ Attrs, and

(iii) the kind of $c = \mathbf{term}$ iff $c \in$ Funcs.

The strict constructor signature MaxConstrSign is defined by the conditions (Def. 24).

(Def. 24)(i) The operation symbols of MaxConstrSign $= \{*, \mathbf{non}\} \cup$ Constructors, and

(ii) for every operation symbol o of MaxConstrSign such that o is constructor holds (the result sort of MaxConstrSign)(o) $= o_{\mathbf{1}}$ and (the arity of MaxConstrSign)(o) $= (o_{\mathbf{2}})_{\mathbf{1}}$.

Let us note that MinConstrSign is non initialized and MaxConstrSign is initialized.

Let us observe that there exists a constructor signature which is initialized and strict.

Let $\mathfrak{C}$ be an initialized constructor signature. One can check that there exists an operation symbol of $\mathfrak{C}$ which is constructor.

4. Mizar Expressions

Let $\mathfrak{C}$ be a constructor signature. The functor Vars $\mathfrak{C}$ yielding a many sorted set indexed by the carrier of $\mathfrak{C}$ is defined as follows:

(Def. 25) $(\mathrm{Vars}\,\mathfrak{C})(\mathbf{type}) = \emptyset$ and $(\mathrm{Vars}\,\mathfrak{C})(\mathbf{adj}) = \emptyset$ and $(\mathrm{Vars}\,\mathfrak{C})(\mathbf{term}) = \mathrm{Vars}$.

Let $\mathfrak{C}$ be a constructor signature. Note that $\mathrm{Vars}\,\mathfrak{C}$ is non empty yielding.

Let $\mathfrak{C}$ be an initialized constructor signature. Observe that $\mathrm{Free}_{\mathfrak{C}}(\mathrm{Vars}\,\mathfrak{C})$ is non-empty.

Let Σ be a non void signature, let X be a non empty yielding many sorted set indexed by the carrier of Σ, and let τ be an element of $\mathrm{Free}_{\Sigma}(X)$. We say that τ is ground if and only if:

(Def. 26) $\bigcup \mathrm{Var}_{\Sigma}\,\tau = \emptyset$.

We say that τ is compound if and only if:

(Def. 27) $\tau(\emptyset) \in$ (the operation symbols of Σ) $\times$ {the carrier of Σ}.

In the sequel $\mathfrak{C}$ denotes an initialized constructor signature, s denotes a sort symbol of $\mathfrak{C}$, o denotes an operation symbol of $\mathfrak{C}$, and c denotes a constructor operation symbol of $\mathfrak{C}$.

Let us consider $\mathfrak{C}$. An expression of $\mathfrak{C}$ is an element of $\mathrm{Free}_{\mathfrak{C}}(\mathrm{Vars}\,\mathfrak{C})$.

Let us consider $\mathfrak{C}$, s. An expression of $\mathfrak{C}$ is called an expression of $\mathfrak{C}$ from s if:

(Def. 28) It $\in$ (the sorts of $\mathrm{Free}_{\mathfrak{C}}(\mathrm{Vars}\,\mathfrak{C})$)$(s)$.

Next we state the proposition

(41) z is an expression of $\mathfrak{C}$ from s iff $z \in$ (the sorts of $\mathrm{Free}_{\mathfrak{C}}(\mathrm{Vars}\,\mathfrak{C})$)$(s)$.

Let us consider $\mathfrak{C}$ and let us consider c. Let us assume that $\mathrm{len}\,\mathrm{Arity}(c) = 0$. The functor c_{t} yielding an expression of $\mathfrak{C}$ is defined by:

(Def. 29) $c_{\mathrm{t}} = \langle c$, the carrier of $\mathfrak{C}\rangle$-tree$(\emptyset)$.

The following proposition is true

(42) Let given o. Suppose $\mathrm{len}\,\mathrm{Arity}(o) = 1$. Let α be an expression of $\mathfrak{C}$. Given s such that $s = \mathrm{Arity}(o)(1)$ and α is an expression of $\mathfrak{C}$ from s. Then $\langle o$, the carrier of $\mathfrak{C}\rangle$-tree$(\langle\alpha\rangle)$ is an expression of $\mathfrak{C}$ from the result sort of o.

Let us consider $\mathfrak{C}$, o. Let us assume that $\mathrm{len}\,\mathrm{Arity}(o) = 1$. Let η be an expression of $\mathfrak{C}$. Let us assume that there exists a sort symbol s of $\mathfrak{C}$ such that $s = \mathrm{Arity}(o)(1)$ and η is an expression of $\mathfrak{C}$ from s. The functor $o(\eta)$ yielding an expression of $\mathfrak{C}$ is defined by:

(Def. 30) $o(\eta) = \langle o$, the carrier of $\mathfrak{C}\rangle$-tree$(\langle\eta\rangle)$.

In the sequel α, β are expressions of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$.

One can prove the following two propositions:

(43) $\mathbf{non}_{\mathfrak{C}}(\alpha)$ is an expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ and $\mathbf{non}_{\mathfrak{C}}(\alpha) = \langle\,\mathbf{non}$, the carrier of $\mathfrak{C}\rangle$-tree$(\langle\alpha\rangle)$.

(44) If $\mathbf{non}_{\mathfrak{C}}(\alpha) = \mathbf{non}_{\mathfrak{C}}(\beta)$, then $\alpha = \beta$.

Let us consider $\mathfrak{C}$, α. Observe that $\mathbf{non}_{\mathfrak{C}}(\alpha)$ is compound.

Let us consider $\mathfrak{C}$. Note that there exists an expression of $\mathfrak{C}$ which is compound.

Next we state the proposition

(45) Let given o. Suppose len Arity$(o) = 2$. Let α, β be expressions of $\mathfrak{C}$. Given sort symbols s_1, s_2 of $\mathfrak{C}$ such that $s_1 = \mathrm{Arity}(o)(1)$ and $s_2 = \mathrm{Arity}(o)(2)$ and α is an expression of $\mathfrak{C}$ from s_1 and β is an expression of $\mathfrak{C}$ from s_2. Then $\langle o$, the carrier of $\mathfrak{C}\rangle$-tree$(\langle\alpha, \beta\rangle)$ is an expression of $\mathfrak{C}$ from the result sort of o.

Let us consider $\mathfrak{C}$, o. Let us assume that len Arity$(o) = 2$. Let η_1, η_2 be expressions of $\mathfrak{C}$. Let us assume that there exist sort symbols s_1, s_2 of $\mathfrak{C}$ such that $s_1 = \mathrm{Arity}(o)(1)$ and $s_2 = \mathrm{Arity}(o)(2)$ and η_1 is an expression of $\mathfrak{C}$ from s_1 and η_2 is an expression of $\mathfrak{C}$ from s_2. The functor $o(\eta_1, \eta_2)$ yielding an expression of $\mathfrak{C}$ is defined as follows:

(Def. 31) $o(\eta_1, \eta_2) = \langle o$, the carrier of $\mathfrak{C}\rangle$-tree$(\langle\eta_1, \eta_2\rangle)$.

In the sequel τ, τ_1, τ_2 are expressions of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$.

We now state two propositions:

(46) $*_{\mathfrak{C}}(\alpha, \tau)$ is an expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$ and $*_{\mathfrak{C}}(\alpha, \tau) = \langle *$, the carrier of $\mathfrak{C}\rangle$-tree$(\langle\alpha, \tau\rangle)$.

(47) If $*_{\mathfrak{C}}(\alpha, \tau_1) = *_{\mathfrak{C}}(\beta, \tau_2)$, then $\alpha = \beta$ and $\tau_1 = \tau_2$.

Let us consider $\mathfrak{C}$, α, τ. One can check that $*_{\mathfrak{C}}(\alpha, \tau)$ is compound.

Let Σ be a non void signature and let s be a sort symbol of Σ. Let us assume that there exists an operation symbol o of Σ such that the result sort of $o = s$. An operation symbol of Σ is said to be an operation symbol of s if:

(Def. 32) The result sort of it $= s$.

Let $\mathfrak{C}$ be a constructor signature. Then $\mathbf{non}_{\mathfrak{C}}$ is an operation symbol of $\mathbf{adj}_{\mathfrak{C}}$. Then $*_{\mathfrak{C}}$ is an operation symbol of $\mathbf{type}_{\mathfrak{C}}$.

The following proposition is true

(48) Let s_1, s_2 be sort symbols of $\mathfrak{C}$. Suppose $s_1 \neq s_2$. Let τ_1 be an expression of $\mathfrak{C}$ from s_1 and τ_2 be an expression of $\mathfrak{C}$ from s_2. Then $\tau_1 \neq \tau_2$.

5. Quasi-terms

Let us consider $\mathfrak{C}$. The functor QuasiTerms $\mathfrak{C}$ yields a subset of $\mathrm{Free}_{\mathfrak{C}}(\mathrm{Vars}\,\mathfrak{C})$ and is defined as follows:

(Def. 33) QuasiTerms $\mathfrak{C}$ = (the sorts of $\mathrm{Free}_{\mathfrak{C}}(\mathrm{Vars}\,\mathfrak{C}))(\mathbf{term}_{\mathfrak{C}})$.

Let us consider $\mathfrak{C}$. One can check that QuasiTerms $\mathfrak{C}$ is non empty and constituted of decorated trees.

Let us consider $\mathfrak{C}$. A quasi-term of $\mathfrak{C}$ is an expression of $\mathfrak{C}$ from $\mathbf{term}_{\mathfrak{C}}$.

We now state the proposition

(49) z is a quasi-term of $\mathfrak{C}$ iff $z \in$ QuasiTerms $\mathfrak{C}$.

Let x be a variable and let us consider $\mathfrak{C}$. The functor $x_{\mathfrak{C}}$ yields a quasi-term of $\mathfrak{C}$ and is defined by:

(Def. 34) $x_{\mathfrak{C}} =$ the root tree of $\langle x,$ **term** $\rangle$.

One can prove the following proposition

(50) For all variables x_1, x_2 and for all initialized constructor signatures $\mathfrak{C}_1$, $\mathfrak{C}_2$ such that $(x_1)_{\mathfrak{C}_1} = (x_2)_{\mathfrak{C}_2}$ holds $x_1 = x_2$.

Let x be a variable and let us consider $\mathfrak{C}$. One can check that $x_{\mathfrak{C}}$ is non compound.

We now state the proposition

(51) Let p be a decorated tree yielding finite sequence. Then $\langle c$, the carrier of $\mathfrak{C}\rangle$-tree(p) is an expression of $\mathfrak{C}$ if and only if $\operatorname{len} p = \operatorname{len}\operatorname{Arity}(c)$ and $p \in (\operatorname{QuasiTerms}\mathfrak{C})^*$.

In the sequel p is a finite sequence of elements of QuasiTerms $\mathfrak{C}$.

Let us consider $\mathfrak{C}$, c and let us consider p. Let us assume that $\operatorname{len} p = \operatorname{len}\operatorname{Arity}(c)$. The functor $c^{\neg}(p)$ yields a compound expression of $\mathfrak{C}$ and is defined as follows:

(Def. 35) $c^{\neg}(p) = \langle c$, the carrier of $\mathfrak{C}\rangle$-tree(p).

Next we state several propositions:

(52) If $\operatorname{len} p = \operatorname{len}\operatorname{Arity}(c)$, then $c^{\neg}(p)$ is an expression of $\mathfrak{C}$ from the result sort of c.

(53) Let η be an expression of $\mathfrak{C}$. Then

(i) there exists a variable x such that $\eta = x_{\mathfrak{C}}$, or

(ii) there exists a constructor operation symbol c of $\mathfrak{C}$ and there exists a finite sequence p of elements of QuasiTerms $\mathfrak{C}$ such that $\operatorname{len} p = \operatorname{len}\operatorname{Arity}(c)$ and $\eta = c^{\neg}(p)$, or

(iii) there exists an expression α of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ such that $\eta = \mathbf{non}_{\mathfrak{C}}(\alpha)$, or

(iv) there exists an expression α of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ and there exists an expression τ of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$ such that $\eta = *_{\mathfrak{C}}(\alpha, \tau)$.

(54) If $\operatorname{len} p = \operatorname{len}\operatorname{Arity}(c)$, then $c^{\neg}(p) \neq \mathbf{non}_{\mathfrak{C}}(\alpha)$.

(55) If $\operatorname{len} p = \operatorname{len}\operatorname{Arity}(c)$, then $c^{\neg}(p) \neq *_{\mathfrak{C}}(\alpha, \tau)$.

(56) $\mathbf{non}_{\mathfrak{C}}(\alpha) \neq *_{\mathfrak{C}}(\beta, \tau)$.

In the sequel η is an expression of $\mathfrak{C}$.

Next we state two propositions:

(57) If $\eta(\emptyset) = \langle$ **non**, the carrier of $\mathfrak{C}\rangle$, then there exists α such that $\eta = \mathbf{non}_{\mathfrak{C}}(\alpha)$.

(58) If $\eta(\emptyset) = \langle *$, the carrier of $\mathfrak{C}\rangle$, then there exist α, τ such that $\eta = *_{\mathfrak{C}}(\alpha, \tau)$.

6. Quasi-adjectives

In the sequel α, α' denote expressions of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$.

Let us consider $\mathfrak{C}$, α. The functor $\mathrm{non}\,\alpha$ yields an expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ and is defined by:

(Def. 36) $\mathrm{non}\,\alpha = \begin{cases} \alpha{\restriction}\langle 0\rangle, & \text{if there exists } \alpha' \text{ such that } \alpha = \mathbf{non}_{\mathfrak{C}}(\alpha'), \\ \mathbf{non}_{\mathfrak{C}}(\alpha), & \text{otherwise.} \end{cases}$

Let us consider $\mathfrak{C}$, α. We say that α is positive if and only if:

(Def. 37) It is not true that there exists α' such that $\alpha = \mathbf{non}_{\mathfrak{C}}(\alpha')$.

Let us consider $\mathfrak{C}$. Note that there exists an expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ which is positive.

Next we state the proposition

(59) For every positive expression α of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ holds $\mathrm{non}\,\alpha = \mathbf{non}_{\mathfrak{C}}(\alpha)$.

Let us consider $\mathfrak{C}$, α. We say that α is negative if and only if:

(Def. 38) There exists α' such that α' is positive and $\alpha = \mathbf{non}_{\mathfrak{C}}(\alpha')$.

Let us consider $\mathfrak{C}$ and let α be a positive expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$. Note that $\mathrm{non}\,\alpha$ is negative and non positive.

Let us consider $\mathfrak{C}$. One can check that there exists an expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ which is negative and non positive.

Next we state three propositions:

(60) For every non positive expression α of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ there exists an expression α' of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ such that $\alpha = \mathbf{non}_{\mathfrak{C}}(\alpha')$ and $\mathrm{non}\,\alpha = \alpha'$.

(61) Let α be a negative expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$. Then there exists a positive expression α' of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ such that $\alpha = \mathbf{non}_{\mathfrak{C}}(\alpha')$ and $\mathrm{non}\,\alpha = \alpha'$.

(62) For every non positive expression α of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ holds $\mathbf{non}_{\mathfrak{C}}(\mathrm{non}\,\alpha) = \alpha$.

Let us consider $\mathfrak{C}$ and let α be a negative expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$. Note that $\mathrm{non}\,\alpha$ is positive.

Let us consider $\mathfrak{C}$, α. We say that α is regular if and only if:

(Def. 39) α is positive or negative.

Let us consider $\mathfrak{C}$. Observe that every expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ which is positive is also regular and non negative and every expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ which is negative is also regular and non positive.

Let us consider $\mathfrak{C}$. Note that there exists an expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ which is regular.

Let us consider $\mathfrak{C}$. The functor $\mathrm{QuasiAdjs}\,\mathfrak{C}$ yields a subset of $\mathrm{Free}_{\mathfrak{C}}(\mathrm{Vars}\,\mathfrak{C})$ and is defined as follows:

(Def. 40) $\mathrm{QuasiAdjs}\,\mathfrak{C} = \{\alpha : \alpha \text{ is regular}\}$.

Let us consider $\mathfrak{C}$. Note that QuasiAdjs $\mathfrak{C}$ is non empty and constituted of decorated trees.

Let us consider $\mathfrak{C}$. A quasi-adjective of $\mathfrak{C}$ is a regular expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$.

Next we state two propositions:

(63) z is a quasi-adjective of $\mathfrak{C}$ iff $z \in$ QuasiAdjs $\mathfrak{C}$.

(64) z is a quasi-adjective of $\mathfrak{C}$ if and only if z is a positive expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ or a negative expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$.

Let us consider $\mathfrak{C}$. Note that every quasi-adjective of $\mathfrak{C}$ which is non positive is also negative and every quasi-adjective of $\mathfrak{C}$ which is non negative is also positive.

Let us consider $\mathfrak{C}$. Note that there exists a quasi-adjective of $\mathfrak{C}$ which is positive and there exists a quasi-adjective of $\mathfrak{C}$ which is negative.

The following propositions are true:

(65) Let α be a positive quasi-adjective of $\mathfrak{C}$. Then there exists a constructor operation symbol v of $\mathfrak{C}$ such that the result sort of $v = \mathbf{adj}_{\mathfrak{C}}$ and there exists p such that $\operatorname{len} p = \operatorname{len} \operatorname{Arity}(v)$ and $\alpha = v^{\urcorner}(p)$.

(66) Let v be a constructor operation symbol of $\mathfrak{C}$. Suppose the result sort of $v = \mathbf{adj}_{\mathfrak{C}}$ and $\operatorname{len} p = \operatorname{len} \operatorname{Arity}(v)$. Then $v^{\urcorner}(p)$ is a positive quasi-adjective of $\mathfrak{C}$.

Let us consider $\mathfrak{C}$ and let α be a quasi-adjective of $\mathfrak{C}$. One can check that $\operatorname{non} \alpha$ is regular.

We now state three propositions:

(67) For every quasi-adjective α of $\mathfrak{C}$ holds $\operatorname{non} \operatorname{non} \alpha = \alpha$.

(68) For all quasi-adjectives α_1, α_2 of $\mathfrak{C}$ such that $\operatorname{non} \alpha_1 = \operatorname{non} \alpha_2$ holds $\alpha_1 = \alpha_2$.

(69) For every quasi-adjective α of $\mathfrak{C}$ holds $\operatorname{non} \alpha \neq \alpha$.

7. Quasi-types

Let us consider $\mathfrak{C}$ and let ϑ be an expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$. We say that ϑ is pure if and only if:

(Def. 41) It is not true that there exist α, τ such that $\vartheta = *_{\mathfrak{C}}(\alpha, \tau)$.

The following propositions are true:

(70) Let m be an operation symbol of $\mathfrak{C}$. Suppose the result sort of $m = \mathbf{type}$ and $\operatorname{Arity}(m) = \emptyset$. Then there exists τ such that $\tau =$ the root tree of $\langle m$, the carrier of $\mathfrak{C}\rangle$ and τ is pure.

(71) Let v be an operation symbol of $\mathfrak{C}$. Suppose the result sort of $v = \mathbf{adj}$ and $\operatorname{Arity}(v) = \emptyset$. Then there exists α such that $\alpha =$ the root tree of $\langle v$, the carrier of $\mathfrak{C}\rangle$ and α is positive.

Let us consider $\mathfrak{C}$. Note that there exists an expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$ which is pure.

In the sequel ϑ denotes a pure expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$ and A denotes a finite subset of QuasiAdjs $\mathfrak{C}$.

Let us consider $\mathfrak{C}$. The functor QuasiTypes $\mathfrak{C}$ is defined as follows:

(Def. 42) QuasiTypes $\mathfrak{C} = \{\langle A, \tau\rangle : \tau$ is pure$\}$.

Let us consider $\mathfrak{C}$. Note that QuasiTypes $\mathfrak{C}$ is non empty.

Let us consider $\mathfrak{C}$. Quasi-type of $\mathfrak{C}$ is defined by:

(Def. 43) It $\in$ QuasiTypes $\mathfrak{C}$.

The following two propositions are true:

(72) z is a quasi-type of $\mathfrak{C}$ iff there exist A, ϑ such that $z = \langle A, \vartheta\rangle$.

(73) $\langle x, y\rangle$ is a quasi-type of $\mathfrak{C}$ if and only if x is a finite subset of QuasiAdjs $\mathfrak{C}$ and y is a pure expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$.

In the sequel θ is a quasi-type of $\mathfrak{C}$.

Let us consider $\mathfrak{C}$. Observe that every quasi-type of $\mathfrak{C}$ is pair.

Next we state four propositions:

(74) There exists a constructor operation symbol m of $\mathfrak{C}$ such that the result sort of $m = \mathbf{type}_{\mathfrak{C}}$ and there exists p such that $\operatorname{len} p = \operatorname{len} \operatorname{Arity}(m)$ and $\vartheta = m^{\urcorner}(p)$.

(75) Let m be a constructor operation symbol of $\mathfrak{C}$. Suppose the result sort of $m = \mathbf{type}_{\mathfrak{C}}$ and $\operatorname{len} p = \operatorname{len} \operatorname{Arity}(m)$. Then $m^{\urcorner}(p)$ is a pure expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$.

(76) QuasiTerms $\mathfrak{C}$ misses QuasiAdjs $\mathfrak{C}$ and QuasiTerms $\mathfrak{C}$ misses QuasiTypes $\mathfrak{C}$ and QuasiTypes $\mathfrak{C}$ misses QuasiAdjs $\mathfrak{C}$.

(77) Let η be a set. Then

(i) if η is a quasi-term of $\mathfrak{C}$, then η is not a quasi-adjective of $\mathfrak{C}$,

(ii) if η is a quasi-term of $\mathfrak{C}$, then η is not a quasi-type of $\mathfrak{C}$, and

(iii) if η is a quasi-type of $\mathfrak{C}$, then η is not a quasi-adjective of $\mathfrak{C}$.

Let us consider $\mathfrak{C}$, A, ϑ. We introduce $A * \vartheta$ as a synonym of $\langle A, \vartheta\rangle$.

Let us consider $\mathfrak{C}$, A, ϑ. Then $A * \vartheta$ is a quasi-type of $\mathfrak{C}$.

Let us consider $\mathfrak{C}$, θ. Note that $\theta_{\mathbf{1}}$ is finite.

Let us consider $\mathfrak{C}$, θ. We introduce adjs θ as a synonym of $\theta_{\mathbf{1}}$. We introduce the base of θ as a synonym of $\theta_{\mathbf{2}}$.

Let us consider $\mathfrak{C}$, θ. Then adjs θ is a subset of QuasiAdjs $\mathfrak{C}$. Then the base of θ is a pure expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$.

One can prove the following propositions:

(78) adjs$(A * \vartheta) = A$ and the base of $A * \vartheta = \vartheta$.

(79) Let A_1, A_2 be finite subsets of QuasiAdjs $\mathfrak{C}$ and ϑ_1, ϑ_2 be pure expressions of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$. If $A_1 * \vartheta_1 = A_2 * \vartheta_2$, then $A_1 = A_2$ and $\vartheta_1 = \vartheta_2$.

(80) $\theta =$ adjs $\theta *$ the base of θ.

(81) For all quasi-types θ_1, θ_2 of $\mathfrak{C}$ such that $\operatorname{adjs}\theta_1 = \operatorname{adjs}\theta_2$ and the base of $\theta_1 =$ the base of θ_2 holds $\theta_1 = \theta_2$.

Let us consider $\mathfrak{C}$, θ and let α be a quasi-adjective of $\mathfrak{C}$. The functor $\alpha * \theta$ yields a quasi-type of $\mathfrak{C}$ and is defined by:

(Def. 44) $\alpha * \theta = \langle\{\alpha\} \cup \operatorname{adjs}\theta$, the base of $\theta\rangle$.

We now state three propositions:

(82) For every quasi-adjective α of $\mathfrak{C}$ holds $\operatorname{adjs}(\alpha * \theta) = \{\alpha\} \cup \operatorname{adjs}\theta$ and the base of $\alpha * \theta =$ the base of θ.

(83) For every quasi-adjective α of $\mathfrak{C}$ holds $\alpha * (\alpha * \theta) = \alpha * \theta$.

(84) For all quasi-adjectives α, β of $\mathfrak{C}$ holds $\alpha * (\beta * \theta) = \beta * (\alpha * \theta)$.

8. Variables in Quasi-types

Let Σ be a non void signature, let s be a sort symbol of Σ, let X be a non-empty many sorted set indexed by the carrier of Σ, and let τ be a term of Σ over X. Note that $(\operatorname{Var}\tau)(s)$ is finite.

Let Σ be a non void signature, let s be a sort symbol of Σ, let X be a non empty yielding many sorted set indexed by the carrier of Σ, and let τ be an element of $\operatorname{Free}_\Sigma(X)$. Observe that $(\operatorname{Var}_\Sigma \tau)(s)$ is finite.

Let Σ be a non void signature, let X be a non empty yielding many sorted set indexed by the carrier of Σ, and let s be a sort symbol of Σ. The functor vars^X_s yielding a function from $\bigcup$(the sorts of $\operatorname{Free}_\Sigma(X)$) into $2^{X(s)}$ is defined by:

(Def. 45) For every element τ of $\operatorname{Free}_\Sigma(X)$ holds $(\operatorname{vars}^X_s)(\tau) = (\operatorname{Var}_\Sigma \tau)(s)$.

Let $\mathfrak{C}$ be an initialized constructor signature and let η be an expression of $\mathfrak{C}$. The functor $\operatorname{Var}\eta$ yielding a subset of Vars is defined by:

(Def. 46) $\operatorname{Var}\eta = (\operatorname{Var}_{\mathfrak{C}}\eta)(\mathbf{term}_{\mathfrak{C}})$.

Let us consider $\mathfrak{C}$, η. Note that $\operatorname{Var}\eta$ is finite.

Let us consider $\mathfrak{C}$, η. The functor $\operatorname{vars}(\eta)$ yielding a finite subset of Vars is defined as follows:

(Def. 47) $\operatorname{vars}(\eta) = \operatorname{varcl}\operatorname{Var}\eta$.

The following propositions are true:

(85) $\operatorname{varcl}\operatorname{vars}(\eta) = \operatorname{vars}(\eta)$.

(86) For every variable x holds $\operatorname{Var}(x_{\mathfrak{C}}) = \{x\}$.

(87) For every variable x holds $\operatorname{vars}(x_{\mathfrak{C}}) = \{x\} \cup \operatorname{vars}(x)$.

(88) Let p be a decorated tree yielding finite sequence. Suppose $\eta = \langle c$, the carrier of $\mathfrak{C}\rangle$-tree(p). Then $\operatorname{Var}\eta = \bigcup\{\operatorname{Var}\tau; \tau$ ranges over quasi-terms of $\mathfrak{C}$: $\tau \in \operatorname{rng} p\}$.

(89) Let p be a decorated tree yielding finite sequence. Suppose $\eta = \langle c$, the carrier of $\mathfrak{C}\rangle$-tree(p). Then $\mathrm{vars}(\eta) = \bigcup\{\mathrm{vars}(\tau); \tau$ ranges over quasi-terms of $\mathfrak{C}$: $\tau \in \mathrm{rng}\, p\}$.

(90) If $\mathrm{len}\, p = \mathrm{len}\,\mathrm{Arity}(c)$, then $\mathrm{Var}(c^{\to}(p)) = \bigcup\{\mathrm{Var}\,\tau; \tau$ ranges over quasi-terms of $\mathfrak{C}$: $\tau \in \mathrm{rng}\, p\}$.

(91) If $\mathrm{len}\, p = \mathrm{len}\,\mathrm{Arity}(c)$, then $\mathrm{vars}(c^{\to}(p)) = \bigcup\{\mathrm{vars}(\tau); \tau$ ranges over quasi-terms of $\mathfrak{C}$: $\tau \in \mathrm{rng}\, p\}$.

(92) For every many sorted signature Σ and for every set o holds $\mathrm{Var}_\Sigma(\langle o$, the carrier of $\Sigma\rangle$-tree$(\emptyset)) = \mathbf{0}_{\text{the carrier of } \Sigma}$.

(93) Let Σ be a many sorted signature, o be a set, and τ be a decorated tree. Then $\mathrm{Var}_\Sigma(\langle o$, the carrier of $\Sigma\rangle$-tree$(\langle\tau\rangle)) = \mathrm{Var}_\Sigma\,\tau$.

(94) $\mathrm{Var}(\mathbf{non}_{\mathfrak{C}}(\alpha)) = \mathrm{Var}\,\alpha$.

(95) $\mathrm{vars}(\mathbf{non}_{\mathfrak{C}}(\alpha)) = \mathrm{vars}(\alpha)$.

(96) Let Σ be a many sorted signature, o be a set, and τ_1, τ_2 be decorated trees. Then $\mathrm{Var}_\Sigma(\langle o$, the carrier of $\Sigma\rangle$-tree$(\langle\tau_1, \tau_2\rangle)) = \mathrm{Var}_\Sigma\,\tau_1 \cup \mathrm{Var}_\Sigma\,\tau_2$.

(97) $\mathrm{Var}(*_{\mathfrak{C}}(\alpha, \tau)) = \mathrm{Var}\,\alpha \cup \mathrm{Var}\,\tau$.

(98) $\mathrm{vars}(*_{\mathfrak{C}}(\alpha, \tau)) = \mathrm{vars}(\alpha) \cup \mathrm{vars}(\tau)$.

(99) $\mathrm{Var}\,\mathrm{non}\,\alpha = \mathrm{Var}\,\alpha$.

(100) $\mathrm{vars}(\mathrm{non}\,\alpha) = \mathrm{vars}(\alpha)$.

Let us consider $\mathfrak{C}$ and let θ be a quasi-type of $\mathfrak{C}$. The functor $\mathrm{Var}\,\theta$ yields a subset of Vars and is defined as follows:

(Def. 48) $\mathrm{Var}\,\theta = \bigcup((\mathrm{vars}^{\mathrm{Vars}\,\mathfrak{C}}_{\mathbf{term}_{\mathfrak{C}}})^{\circ}\, \mathrm{adjs}\,\theta) \cup \mathrm{Var}\,(\text{the base of } \theta)$.

Let us consider $\mathfrak{C}$ and let θ be a quasi-type of $\mathfrak{C}$. Note that $\mathrm{Var}\,\theta$ is finite.

Let us consider $\mathfrak{C}$ and let θ be a quasi-type of $\mathfrak{C}$. The functor $\mathrm{vars}(\theta)$ yields a finite subset of Vars and is defined by:

(Def. 49) $\mathrm{vars}(\theta) = \mathrm{varcl}\,\mathrm{Var}\,\theta$.

We now state several propositions:

(101) For every quasi-type θ of $\mathfrak{C}$ holds $\mathrm{varcl}\,\mathrm{vars}(\theta) = \mathrm{vars}(\theta)$.

(102) For every quasi-type θ of $\mathfrak{C}$ and for every quasi-adjective α of $\mathfrak{C}$ holds $\mathrm{Var}(\alpha * \theta) = \mathrm{Var}\,\alpha \cup \mathrm{Var}\,\theta$.

(103) For every quasi-type θ of $\mathfrak{C}$ and for every quasi-adjective α of $\mathfrak{C}$ holds $\mathrm{vars}(\alpha * \theta) = \mathrm{vars}(\alpha) \cup \mathrm{vars}(\theta)$.

(104) $\mathrm{Var}(A * \vartheta) = \bigcup\{\mathrm{Var}\,\alpha; \alpha$ ranges over quasi-adjectives of $\mathfrak{C}$: $\alpha \in A\} \cup \mathrm{Var}\,\vartheta$.

(105) $\mathrm{vars}(A * \vartheta) = \bigcup\{\mathrm{vars}(\alpha); \alpha$ ranges over quasi-adjectives of $\mathfrak{C}$: $\alpha \in A\} \cup \mathrm{vars}(\vartheta)$.

(106) $\mathrm{Var}(\emptyset_{\mathrm{QuasiAdjs}\,\mathfrak{C}} * \vartheta) = \mathrm{Var}\,\vartheta$.

(107) η is ground iff $\mathrm{Var}\,\eta = \emptyset$.

Let us consider $\mathfrak{C}$ and let θ be a quasi-type of $\mathfrak{C}$. We say that θ is ground if and only if:

(Def. 50) $\operatorname{Var}\theta = \emptyset$.

Let us consider $\mathfrak{C}$. Observe that there exists an expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$ which is ground and pure and there exists a quasi-adjective of $\mathfrak{C}$ which is ground.

Next we state the proposition

(108) For every ground pure expression τ of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$ holds $\emptyset_{\mathrm{QuasiAdjs}\,\mathfrak{C}} * \tau$ is ground.

Let us consider $\mathfrak{C}$ and let τ be a ground pure expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$. Note that $\emptyset_{\mathrm{QuasiAdjs}\,\mathfrak{C}} * \tau$ is ground.

Let us consider $\mathfrak{C}$. Note that there exists a quasi-type of $\mathfrak{C}$ which is ground.

Let us consider $\mathfrak{C}$, let θ be a ground quasi-type of $\mathfrak{C}$, and let α be a ground quasi-adjective of $\mathfrak{C}$. Observe that $\alpha * \theta$ is ground.

9. Smooth Type Widening

The strict non empty poset VarPoset is defined by:

(Def. 51) $\mathrm{VarPoset} = (\langle\{\mathrm{varcl}\,A : A \text{ ranges over finite subsets of Vars}\}, \subseteq\rangle)^{\mathrm{op}}$.

One can prove the following propositions:

(109) For all elements x, y of VarPoset holds $x \leq y$ iff $y \subseteq x$.

(110) For every x holds x is an element of VarPoset iff x is a finite subset of Vars and $\mathrm{varcl}\,x = x$.

One can check that VarPoset has g.l.b.'s and l.u.b.'s.

The following proposition is true

(111) For all elements V_1, V_2 of VarPoset holds $V_1 \sqcup V_2 = V_1 \cap V_2$ and $V_1 \sqcap V_2 = V_1 \cup V_2$.

Let V_1, V_2 be elements of VarPoset. One can verify that functors $V_1 \sqcup V_2$ and $V_1 \cap V_2$ and functors $V_1 \sqcap V_2$ and $V_1 \cup V_2$ can be identified.

One can prove the following proposition

(112) For every non empty subset X of VarPoset holds $\sup X$ exists in VarPoset and $\sup X = \bigcap X$.

One can verify that VarPoset is up-complete.

The following proposition is true

(113) $\top_{\mathrm{VarPoset}} = \emptyset$.

Let us consider C. The functor vars-function C yielding a function from QuasiTypes C into the carrier of VarPoset is defined by:

(Def. 52) For every quasi-type T of C holds $(\text{vars-function}\,C)(T) = \mathrm{vars}(T)$.

Let L be a non empty poset. We say that L is smooth if and only if the condition (Def. 53) is satisfied.

(Def. 53) There exists an initialized constructor signature C and there exists a function f from L into VarPoset such that

(i) the carrier of $L \subseteq \mathrm{QuasiTypes}\, C$,

(ii) $f = \text{vars-function}\, C \restriction$the carrier of L, and

(iii) for all elements x, y of L holds f preserves sup of $\{x, y\}$.

Let C be an initialized constructor signature and let T be a ground quasi-type of C. One can check that $\langle \{T\}, \mathrm{id}_{\{T\}} \rangle$ is smooth.

10. Structural Induction

The scheme *StructInd* deals with an initialized constructor signature $\mathcal{A}$, an expression $\mathcal{B}$ of $\mathcal{A}$, and a unary predicate $\mathcal{P}$, and states that:

$\mathcal{P}[\mathcal{B}]$

provided the following conditions are satisfied:

- For every variable x holds $\mathcal{P}[x_{\mathcal{A}}]$,
- Let c be a constructor operation symbol of $\mathcal{A}$ and p be a finite sequence of elements of QuasiTerms $\mathcal{A}$. Suppose $\mathrm{len}\, p = \mathrm{len}\, \mathrm{Arity}(c)$ and for every quasi-term τ of $\mathcal{A}$ such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$. Then $\mathcal{P}[c^{\urcorner}(p)]$,
- For every expression α of $\mathcal{A}$ from $\mathbf{adj}_{\mathcal{A}}$ such that $\mathcal{P}[\alpha]$ holds $\mathcal{P}[\mathbf{non}_{\mathcal{A}}(\alpha)]$, and
- Let α be an expression of $\mathcal{A}$ from $\mathbf{adj}_{\mathcal{A}}$. Suppose $\mathcal{P}[\alpha]$. Let τ be an expression of $\mathcal{A}$ from $\mathbf{type}_{\mathcal{A}}$. If $\mathcal{P}[\tau]$, then $\mathcal{P}[*_{\mathcal{A}}(\alpha, \tau)]$.

Let Σ be a many sorted signature. We say that Σ has an operation for each sort if and only if:

(Def. 54) The carrier of $\Sigma \subseteq \mathrm{rng}\,$(the result sort of Σ).

Let X be a many sorted set indexed by the carrier of Σ. We say that X has missing variables if and only if:

(Def. 55) $X^{-1}(\{\emptyset\}) \subseteq \mathrm{rng}\,$(the result sort of Σ).

The following proposition is true

(114) Let Σ be a non void signature and X be a many sorted set indexed by the carrier of Σ. Then X has missing variables if and only if for every sort symbol s of Σ such that $X(s) = \emptyset$ there exists an operation symbol o of Σ such that the result sort of $o = s$.

Observe that MaxConstrSign has an operation for each sort. Let $\mathfrak{C}$ be a constructor signature. Observe that Vars $\mathfrak{C}$ has missing variables.

Let Σ be a many sorted signature. Observe that every many sorted set indexed by the carrier of Σ which is non-empty has also missing variables.

Let Σ be a many sorted signature. Observe that there exists a many sorted set indexed by the carrier of Σ which has missing variables.

One can verify that there exists a constructor signature which is initialized and strict and has an operation for each sort.

Let $\mathfrak{C}$ be a many sorted signature with an operation for each sort. Observe that every many sorted set indexed by the carrier of $\mathfrak{C}$ has missing variables.

Let G be a non empty tree construction structure. Then the terminals of G is a subset of G. Then the nonterminals of G is a subset of G.

Next we state a number of propositions:

(115) Let D_1, D_2 be non empty tree construction structures. Suppose the rules of $D_1 \subseteq$ the rules of D_2. Then

(i) the nonterminals of $D_1 \subseteq$ the nonterminals of D_2,

(ii) (the carrier of D_1) $\cap$ (the terminals of D_2) $\subseteq$ the terminals of D_1, and

(iii) if the terminals of $D_1 \subseteq$ the terminals of D_2, then the carrier of $D_1 \subseteq$ the carrier of D_2.

(116) Let D_1, D_2 be non empty tree construction structures. Suppose the terminals of $D_1 \subseteq$ the terminals of D_2 and the rules of $D_1 \subseteq$ the rules of D_2. Then $\mathrm{TS}(D_1) \subseteq \mathrm{TS}(D_2)$.

(117) Let Σ be a many sorted signature and X, Y be many sorted sets indexed by the carrier of Σ. If $X \subseteq Y$, then if X has missing variables, then Y has missing variables.

(118) For every set Σ and for all many sorted sets X, Y indexed by Σ such that $X \subseteq Y$ holds $\bigcup \mathrm{coprod}(X) \subseteq \bigcup \mathrm{coprod}(Y)$.

(119) Let Σ be a non void signature and X, Y be many sorted sets indexed by the carrier of Σ. If $X \subseteq Y$, then the carrier of $\mathrm{DTConMSA}(X) \subseteq$ the carrier of $\mathrm{DTConMSA}(Y)$.

(120) Let Σ be a non void signature and X be a many sorted set indexed by the carrier of Σ. Suppose X has missing variables. Then the nonterminals of $\mathrm{DTConMSA}(X) =$ (the operation symbols of Σ) $\times$ {the carrier of Σ} and the terminals of $\mathrm{DTConMSA}(X) = \bigcup \mathrm{coprod}(X)$.

(121) Let Σ be a non void signature and X, Y be many sorted sets indexed by the carrier of Σ. Suppose $X \subseteq Y$ and X has missing variables. Then the terminals of $\mathrm{DTConMSA}(X) \subseteq$ the terminals of $\mathrm{DTConMSA}(Y)$ and the rules of $\mathrm{DTConMSA}(X) \subseteq$ the rules of $\mathrm{DTConMSA}(Y)$ and $\mathrm{TS}(\mathrm{DTConMSA}(X)) \subseteq \mathrm{TS}(\mathrm{DTConMSA}(Y))$.

(122) For every set τ holds $\tau \in$ the terminals of $\mathrm{DTConMSA}(\mathrm{Vars}\,\mathfrak{C})$ iff there exists a variable x such that $\tau = \langle x, \mathbf{term}_{\mathfrak{C}} \rangle$.

(123) Let τ be a set. Then $\tau \in$ the nonterminals of $\mathrm{DTConMSA}(\mathrm{Vars}\,\mathfrak{C})$ if and only if one of the following conditions is satisfied:

(i) $\tau = \langle *_{\mathfrak{C}}$, the carrier of $\mathfrak{C}\rangle$, or

(ii) $\tau = \langle \mathbf{non}_{\mathfrak{C}}$, the carrier of $\mathfrak{C}\rangle$, or

(iii) there exists a constructor operation symbol c of $\mathfrak{C}$ such that $\tau = \langle c$, the carrier of $\mathfrak{C}\rangle$.

(124) Let Σ be a non void signature, X be a many sorted set indexed by the carrier of Σ with missing variables, and τ be a set. Suppose $\tau \in \bigcup$(the sorts of $\mathrm{Free}_\Sigma(X)$). Then τ is a term of Σ over $X \cup$((the carrier of Σ) $\longmapsto \{0\}$).

(125) Let Σ be a non void signature, X be a many sorted set indexed by the carrier of Σ with missing variables, and τ be a term of Σ over $X \cup$((the carrier of Σ) $\longmapsto \{0\}$). If $\tau \in \bigcup$(the sorts of $\mathrm{Free}_\Sigma(X)$), then $\tau \in$ (the sorts of $\mathrm{Free}_\Sigma(X)$)(the sort of τ).

(126) Let G be a non empty tree construction structure, s be an element of G, and p be a finite sequence. Suppose $s \Rightarrow p$. Then p is a finite sequence of elements of the carrier of G.

(127) Let Σ be a non void signature, X, Y be many sorted sets indexed by the carrier of Σ, g_1 be a symbol of DTConMSA(X), g_2 be a symbol of DTConMSA(Y), p_1 be a finite sequence of elements of the carrier of DTConMSA(X), and p_2 be a finite sequence of elements of the carrier of DTConMSA(Y). If $g_1 = g_2$ and $p_1 = p_2$ and $g_1 \Rightarrow p_1$, then $g_2 \Rightarrow p_2$.

(128) Let Σ be a non void signature and X be a many sorted set indexed by the carrier of Σ with missing variables. Then $\bigcup$(the sorts of $\mathrm{Free}_\Sigma(X)$) = TS(DTConMSA(X)).

Let Σ be a non void signature and let X be a many sorted set indexed by the carrier of Σ. A unary operation on $\bigcup$(the sorts of $\mathrm{Free}_\Sigma(X)$) is said to be a transformation of Σ-terms over X if:

(Def. 56) For every sort symbol s of Σ holds it$^\circ$(the sorts of $\mathrm{Free}_\Sigma(X)$)(s) $\subseteq$ (the sorts of $\mathrm{Free}_\Sigma(X)$)(s).

The following two propositions are true:

(129) Let Σ be a non void signature, X be a non empty many sorted set indexed by the carrier of Σ, and f be a unary operation on $\bigcup$(the sorts of $\mathrm{Free}_\Sigma(X)$). Then f is a transformation of Σ-terms over X if and only if for every sort symbol s of Σ and for every set α such that $\alpha \in$ (the sorts of $\mathrm{Free}_\Sigma(X)$)(s) holds $f(\alpha) \in$ (the sorts of $\mathrm{Free}_\Sigma(X)$)(s).

(130) Let Σ be a non void signature, X be a non empty many sorted set indexed by the carrier of Σ, f be a transformation of Σ-terms over X, s be a sort symbol of Σ, and p be a finite sequence of elements of (the sorts of $\mathrm{Free}_\Sigma(X)$)(s). Then $f \cdot p$ is a finite sequence of elements of (the sorts of $\mathrm{Free}_\Sigma(X)$)(s) and $\overline{\overline{(f \cdot p\ \textbf{qua}\ \text{set})}} = \operatorname{len} p$.

Let Σ be a non void signature, let X be a many sorted set indexed by the carrier of Σ, and let τ be a transformation of Σ-terms over X. We say that τ is substitution if and only if the condition (Def. 57) is satisfied.

(Def. 57) Let o be an operation symbol of Σ and p, p' be finite sequences of elements of $\mathrm{Free}_\Sigma(X)$. Suppose $\langle o$, the carrier of $\Sigma\rangle$-tree(p) $\in \bigcup$(the sorts of

$\mathrm{Free}_{\Sigma}(X)$) and $p' = \tau \cdot p$. Then $\tau(\langle o$, the carrier of $\Sigma\rangle$-tree$(p)) = \langle o$, the carrier of $\Sigma\rangle$-tree(p').

The scheme *StructDef* deals with an initialized constructor signature $\mathcal{A}$, two unary functors $\mathcal{F}$ and $\mathcal{G}$ yielding expressions of $\mathcal{A}$, and two binary functors $\mathcal{H}$ and $\mathcal{I}$ yielding expressions of $\mathcal{A}$, and states that:

There exists a transformation f of $\mathcal{A}$-terms over $\mathrm{Vars}\,\mathcal{A}$ such that

(i) for every variable x holds $f(x_{\mathcal{A}}) = \mathcal{F}(x)$,

(ii) for every constructor operation symbol c of $\mathcal{A}$ and for all finite sequences p, p' of elements of $\mathrm{QuasiTerms}\,\mathcal{A}$ such that $\mathrm{len}\,p = \mathrm{len}\,\mathrm{Arity}(c)$ and $p' = f \cdot p$ holds $f(c\urcorner(p)) = \mathcal{H}(c, p')$,

(iii) for every expression α of $\mathcal{A}$ from $\mathbf{adj}_{\mathcal{A}}$ holds $f(\mathbf{non}_{\mathcal{A}}(\alpha)) = \mathcal{G}(f(\alpha))$, and

(iv) for every expression α of $\mathcal{A}$ from $\mathbf{adj}_{\mathcal{A}}$ and for every expression τ of $\mathcal{A}$ from $\mathbf{type}_{\mathcal{A}}$ holds $f(*_{\mathcal{A}}(\alpha, \tau)) = \mathcal{I}(f(\alpha), f(\tau))$

provided the parameters meet the following requirements:

- For every variable x holds $\mathcal{F}(x)$ is a quasi-term of $\mathcal{A}$,
- Let c be a constructor operation symbol of $\mathcal{A}$ and p be a finite sequence of elements of $\mathrm{QuasiTerms}\,\mathcal{A}$. Suppose $\mathrm{len}\,p = \mathrm{len}\,\mathrm{Arity}(c)$. Then $\mathcal{H}(c, p)$ is an expression of $\mathcal{A}$ from the result sort of c,
- For every expression α of $\mathcal{A}$ from $\mathbf{adj}_{\mathcal{A}}$ holds $\mathcal{G}(\alpha)$ is an expression of $\mathcal{A}$ from $\mathbf{adj}_{\mathcal{A}}$, and
- Let α be an expression of $\mathcal{A}$ from $\mathbf{adj}_{\mathcal{A}}$ and τ be an expression of $\mathcal{A}$ from $\mathbf{type}_{\mathcal{A}}$. Then $\mathcal{I}(\alpha, \tau)$ is an expression of $\mathcal{A}$ from $\mathbf{type}_{\mathcal{A}}$.

11. Substitution

Let A be a set, let x, y be sets, and let α, β be elements of A. Then $\mathrm{IFIN}(x, y, \alpha, \beta)$ is an element of A.

Let $\mathfrak{C}$ be an initialized constructor signature. A valuation of $\mathfrak{C}$ is a partial function from Vars to $\mathrm{QuasiTerms}\,\mathfrak{C}$.

Let $\mathfrak{C}$ be an initialized constructor signature and let f be a valuation of $\mathfrak{C}$. We say that f is irrelevant if and only if:

(Def. 58) For every variable x such that $x \in \mathrm{dom}\,f$ there exists a variable y such that $f(x) = y_{\mathfrak{C}}$.

Let $\mathfrak{C}$ be an initialized constructor signature and let f be a valuation of $\mathfrak{C}$. We introduce f is relevant as an antonym of f is irrelevant.

Let X, Y be sets. Observe that there exists a partial function from X to Y which is empty.

Let $\mathfrak{C}$ be an initialized constructor signature. Observe that every valuation of $\mathfrak{C}$ which is empty is also irrelevant.

Let $\mathfrak{C}$ be an initialized constructor signature. Note that there exists a valuation of $\mathfrak{C}$ which is empty, irrelevant, and one-to-one.

Let $\mathfrak{C}$ be an initialized constructor signature and let X be a subset of Vars. The functor $\mathrm{idval}_{\mathfrak{C}}\,X$ yielding a valuation of $\mathfrak{C}$ is defined by:

(Def. 59) $\mathrm{idval}_{\mathfrak{C}}\,X = \{\langle x, x_{\mathfrak{C}}\rangle; x$ ranges over variables: $x \in X\}$.

Next we state the proposition

(131) For every subset X of Vars holds $\mathrm{dom}\,\mathrm{idval}_{\mathfrak{C}}\,X = X$ and for every variable x such that $x \in X$ holds $(\mathrm{idval}_{\mathfrak{C}}\,X)(x) = x_{\mathfrak{C}}$.

Let $\mathfrak{C}$ be an initialized constructor signature and let X be a subset of Vars. One can check that $\mathrm{idval}_{\mathfrak{C}}\,X$ is irrelevant and one-to-one.

Let $\mathfrak{C}$ be an initialized constructor signature and let X be an empty subset of Vars. One can check that $\mathrm{idval}_{\mathfrak{C}}\,X$ is empty.

Let us consider $\mathfrak{C}$ and let f be a valuation of $\mathfrak{C}$. The functor $f^{\#}$ yielding a transformation of $\mathfrak{C}$-terms over $\mathrm{Vars}\,\mathfrak{C}$ is defined by the conditions (Def. 60).

(Def. 60)(i) For every variable x holds if $x \in \mathrm{dom}\,f$, then $f^{\#}(x_{\mathfrak{C}}) = f(x)$ and if $x \notin \mathrm{dom}\,f$, then $f^{\#}(x_{\mathfrak{C}}) = x_{\mathfrak{C}}$,

(ii) for every constructor operation symbol c of $\mathfrak{C}$ and for all finite sequences p, p' of elements of $\mathrm{QuasiTerms}\,\mathfrak{C}$ such that $\mathrm{len}\,p = \mathrm{len}\,\mathrm{Arity}(c)$ and $p' = f^{\#} \cdot p$ holds $f^{\#}(c^{\to}(p)) = c^{\to}(p')$,

(iii) for every expression α of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ holds $f^{\#}(\mathbf{non}_{\mathfrak{C}}(\alpha)) = \mathbf{non}_{\mathfrak{C}}(f^{\#}(\alpha))$, and

(iv) for every expression α of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$ and for every expression τ of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$ holds $f^{\#}(*_{\mathfrak{C}}(\alpha, \tau)) = *_{\mathfrak{C}}(f^{\#}(\alpha), f^{\#}(\tau))$.

Let us consider $\mathfrak{C}$ and let f be a valuation of $\mathfrak{C}$. Observe that $f^{\#}$ is substitution.

In the sequel f denotes a valuation of $\mathfrak{C}$.

Let us consider $\mathfrak{C}$, f, η. The functor $\eta[f]$ yielding an expression of $\mathfrak{C}$ is defined as follows:

(Def. 61) $\eta[f] = f^{\#}(\eta)$.

Let us consider $\mathfrak{C}$, f and let p be a finite sequence. Let us assume that $\mathrm{rng}\,p \subseteq \bigcup(\text{the sorts of }\mathrm{Free}_{\mathfrak{C}}(\mathrm{Vars}\,\mathfrak{C}))$. The functor $p[f]$ yields a finite sequence and is defined as follows:

(Def. 62) $p[f] = f^{\#} \cdot p$.

Let us consider $\mathfrak{C}$, f and let p be a finite sequence of elements of $\mathrm{QuasiTerms}\,\mathfrak{C}$. Then $p[f]$ is a finite sequence of elements of $\mathrm{QuasiTerms}\,\mathfrak{C}$ and it can be characterized by the condition:

(Def. 63) $p[f] = f^{\#} \cdot p$.

In the sequel x is a variable.

The following propositions are true:

(132) If $x \notin \mathrm{dom}\,f$, then $x_{\mathfrak{C}}[f] = x_{\mathfrak{C}}$.

(133) If $x \in \operatorname{dom} f$, then $x_{\mathfrak{C}}[f] = f(x)$.

(134) If $\operatorname{len} p = \operatorname{len} \operatorname{Arity}(c)$, then $c^{\to}(p)[f] = c^{\to}(p[f])$.

(135) $\mathbf{non}_{\mathfrak{C}}(\alpha)[f] = \mathbf{non}_{\mathfrak{C}}(\alpha[f])$.

(136) $*_{\mathfrak{C}}(\alpha, \tau)[f] = *_{\mathfrak{C}}(\alpha[f], \tau[f])$.

(137) For every subset X of Vars holds $\eta[\mathrm{idval}_{\mathfrak{C}}\, X] = \eta$.

(138) For every subset X of Vars holds $(\mathrm{idval}_{\mathfrak{C}}\, X)^{\#} = \mathrm{id}_{\bigcup (\text{the sorts of } \mathrm{Free}_{\mathfrak{C}}(\mathrm{Vars}\, \mathfrak{C}))}$.

(139) For every empty valuation f of $\mathfrak{C}$ holds $\eta[f] = \eta$.

(140) For every empty valuation f of $\mathfrak{C}$ holds $f^{\#} = \mathrm{id}_{\bigcup (\text{the sorts of } \mathrm{Free}_{\mathfrak{C}}(\mathrm{Vars}\, \mathfrak{C}))}$.

Let us consider $\mathfrak{C}$, f and let τ be a quasi-term of $\mathfrak{C}$. Then $\tau[f]$ is a quasi-term of $\mathfrak{C}$.

Let us consider $\mathfrak{C}$, f and let α be an expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$. Then $\alpha[f]$ is an expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$.

Let us consider $\mathfrak{C}$, f and let α be a positive expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$. Note that $\alpha[f]$ is positive.

Let us consider $\mathfrak{C}$, f and let α be a negative expression of $\mathfrak{C}$ from $\mathbf{adj}_{\mathfrak{C}}$. Observe that $\alpha[f]$ is negative.

Let us consider $\mathfrak{C}$, f and let α be a quasi-adjective of $\mathfrak{C}$. Then $\alpha[f]$ is a quasi-adjective of $\mathfrak{C}$.

We now state the proposition

(141) $(\mathrm{non}\, \alpha)[f] = \mathrm{non}(\alpha[f])$.

Let us consider $\mathfrak{C}$, f and let τ be an expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$. Then $\tau[f]$ is an expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$.

Let us consider $\mathfrak{C}$, f and let τ be a pure expression of $\mathfrak{C}$ from $\mathbf{type}_{\mathfrak{C}}$. Observe that $\tau[f]$ is pure.

One can prove the following two propositions:

(142) Let f be an irrelevant one-to-one valuation of $\mathfrak{C}$. Then there exists an irrelevant one-to-one valuation g of $\mathfrak{C}$ such that for all variables x, y holds $x \in \operatorname{dom} f$ and $f(x) = y_{\mathfrak{C}}$ if and only if $y \in \operatorname{dom} g$ and $g(y) = x_{\mathfrak{C}}$.

(143) Let f, g be irrelevant one-to-one valuations of $\mathfrak{C}$. Suppose that for all variables x, y such that $x \in \operatorname{dom} f$ and $f(x) = y_{\mathfrak{C}}$ holds $y \in \operatorname{dom} g$ and $g(y) = x_{\mathfrak{C}}$. Let given η. If $\mathrm{Var}\, \eta \subseteq \operatorname{dom} f$, then $\eta[f][g] = \eta$.

Let us consider $\mathfrak{C}$, f and let A be a subset of QuasiAdjs $\mathfrak{C}$. The functor $A[f]$ yielding a subset of QuasiAdjs $\mathfrak{C}$ is defined as follows:

(Def. 64) $A[f] = \{\alpha[f]; \alpha$ ranges over quasi-adjectives of $\mathfrak{C}$: $\alpha \in A\}$.

The following three propositions are true:

(144) For every subset A of QuasiAdjs $\mathfrak{C}$ and for every quasi-adjective α of $\mathfrak{C}$ such that $A = \{\alpha\}$ holds $A[f] = \{\alpha[f]\}$.

(145) For all subsets A, B of QuasiAdjs $\mathfrak{C}$ holds $(A \cup B)[f] = A[f] \cup B[f]$.

(146) For all subsets A, B of QuasiAdjs $\mathfrak{C}$ such that $A \subseteq B$ holds $A[f] \subseteq B[f]$.

Let $\mathfrak{C}$ be an initialized constructor signature, let f be a valuation of $\mathfrak{C}$, and let A be a finite subset of QuasiAdjs $\mathfrak{C}$. One can check that $A[f]$ is finite.

Let $\mathfrak{C}$ be an initialized constructor signature, let f be a valuation of $\mathfrak{C}$, and let θ be a quasi-type of $\mathfrak{C}$. The functor $\theta[f]$ yields a quasi-type of $\mathfrak{C}$ and is defined by:

(Def. 65) $\theta[f] = (\mathrm{adjs}\,\theta)[f] * (\text{the base of } \theta)[f]$.

Next we state two propositions:

(147) For every quasi-type θ of $\mathfrak{C}$ holds $\mathrm{adjs}(\theta[f]) = (\mathrm{adjs}\,\theta)[f]$ and the base of $\theta[f] = (\text{the base of } \theta)[f]$.

(148) For every quasi-type θ of $\mathfrak{C}$ and for every quasi-adjective α of $\mathfrak{C}$ holds $(\alpha * \theta)[f] = \alpha[f] * \theta[f]$.

Let $\mathfrak{C}$ be an initialized constructor signature and let f, g be valuations of $\mathfrak{C}$. The functor $f[g]$ yields a valuation of $\mathfrak{C}$ and is defined by:

(Def. 66) $\mathrm{dom}(f[g]) = \mathrm{dom}\, f \cup \mathrm{dom}\, g$ and for every variable x such that $x \in \mathrm{dom}(f[g])$ holds $f[g](x) = x_{\mathfrak{C}}[f][g]$.

Let $\mathfrak{C}$ be an initialized constructor signature and let f, g be irrelevant valuations of $\mathfrak{C}$. One can check that $f[g]$ is irrelevant.

The following three propositions are true:

(149) For all valuations f_1, f_2 of $\mathfrak{C}$ holds $\eta[f_1][f_2] = \eta[f_1[f_2]]$.

(150) For every subset A of QuasiAdjs $\mathfrak{C}$ and for all valuations f_1, f_2 of $\mathfrak{C}$ holds $A[f_1][f_2] = A[f_1[f_2]]$.

(151) For every quasi-type θ of $\mathfrak{C}$ and for all valuations f_1, f_2 of $\mathfrak{C}$ holds $\theta[f_1][f_2] = \theta[f_1[f_2]]$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[3] Grzegorz Bancerek. Introduction to trees. *Formalized Mathematics*, 1(**2**):421–427, 1990.

[4] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

[5] Grzegorz Bancerek. Tarski's classes and ranks. *Formalized Mathematics*, 1(**3**):563–567, 1990.

[6] Grzegorz Bancerek. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.

[7] Grzegorz Bancerek. König's lemma. *Formalized Mathematics*, 2(**3**):397–402, 1991.

[8] Grzegorz Bancerek. Sets and functions of trees and joining operations of trees. *Formalized Mathematics*, 3(**2**):195–204, 1992.

[9] Grzegorz Bancerek. Joining of decorated trees. *Formalized Mathematics*, 4(**1**):77–82, 1993.

[10] Grzegorz Bancerek. Terms over many sorted universal algebra. *Formalized Mathematics*, 5(**2**):191–198, 1996.

[11] Grzegorz Bancerek. Bounds in posets and relational substructures. *Formalized Mathematics*, 6(**1**):81–91, 1997.

[12] Grzegorz Bancerek. Directed sets, nets, ideals, filters, and maps. *Formalized Mathematics*, 6(**1**):93–107, 1997.

[13] Grzegorz Bancerek. On semilattice structure of Mizar types. *Formalized Mathematics*, 11(**4**):355–369, 2003.

[14] Grzegorz Bancerek. On the structure of Mizar types. In Herman Geuvers and Fairouz Kamareddine, editors, *Electronic Notes in Theoretical Computer Science*, volume 85. Elsevier, 2003.

[15] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[16] Grzegorz Bancerek and Artur Korniłowicz. Yet another construction of free algebra. *Formalized Mathematics*, 9(**4**):779–785, 2001.

[17] Grzegorz Bancerek and Yatsuka Nakamura. Full adder circuit. Part I. *Formalized Mathematics*, 5(**3**):367–380, 1996.

[18] Grzegorz Bancerek and Piotr Rudnicki. On defining functions on trees. *Formalized Mathematics*, 4(**1**):91–101, 1993.

[19] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[20] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[21] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[22] 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.

[23] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[24] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[25] Patricia L. Carlson and Grzegorz Bancerek. Context-free grammar – part 1. *Formalized Mathematics*, 2(**5**):683–687, 1991.

[26] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[27] Adam Grabowski and Robert Milewski. Boolean posets, posets under inclusion and products of relational structures. *Formalized Mathematics*, 6(**1**):117–121, 1997.

[28] Yatsuka Nakamura. Determinant of some matrices of field elements. *Formalized Mathematics*, 14(**1**):1–5, 2006.

[29] Yatsuka Nakamura, Piotr Rudnicki, Andrzej Trybulec, and Pauline N. Kawamoto. Preliminaries to circuits, I. *Formalized Mathematics*, 5(**2**):167–172, 1996.

[30] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[31] Beata Perkowska. Free many sorted universal algebra. *Formalized Mathematics*, 5(**1**):67–74, 1996.

[32] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[33] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

[34] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

[35] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

[36] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.

[37] Andrzej Trybulec. Many sorted algebras. *Formalized Mathematics*, 5(**1**):37–42, 1996.

[38] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.

[39] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.

[40] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski – Zorn lemma. *Formalized Mathematics*, 1(**2**):387–393, 1990.

[41] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[42] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[43] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received April 21, 2008

FORMALIZED MATHEMATICS
Volume **16**, Number **2**, **2008**

Addenda

Authors

MML Identifiers

ISSN 1426–2630(p), 1898-9934(e)