Contents

Formaliz. Math. 16 (**1**)

FORMALIZED MATHEMATICS
Vol. **16**, No. **1**, Pages 1–5, **2008**

The Vector Space of Subsets of a Set Based on Symmetric Difference

Jesse Alama
Department of Philosophy
Stanford University
USA

Summary. For each set X, the power set of X forms a vector space over the field $\mathbf{Z}_2$ (the two-element field $\{0,1\}$ with addition and multiplication done modulo 2): vector addition is disjoint union, and scalar multiplication is defined by the two equations ($1 \cdot x := x$, $0 \cdot x := \emptyset$ for subsets x of X). See [10], Exercise 2.K, for more information.

MML identifier: `BSPACE`, version: `7.8.05 4.89.993`

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

1. Preliminaries: Induction on Sequences of Elements of a 1-sorted Structure

Let S be a 1-sorted structure. The functor ε_S yielding a finite sequence of elements of S is defined as follows:

(Def. 1) $\varepsilon_S = \varepsilon_{(\Omega_S)}$.

In the sequel S denotes a 1-sorted structure, i denotes an element of $\mathbb{N}$, p denotes a finite sequence, and X denotes a set.

We now state two propositions:

(1) For every finite sequence p of elements of S such that $i \in \operatorname{dom} p$ holds $p(i) \in S$.

(2) If for every natural number i such that $i \in \operatorname{dom} p$ holds $p(i) \in S$, then p is a finite sequence of elements of S.

ISSN 1426–2630(p), 1898-9934(e)

The scheme *IndSeqS* deals with a 1-sorted structure $\mathcal{A}$ and a unary predicate $\mathcal{P}$, and states that:

For every finite sequence p of elements of $\mathcal{A}$ holds $\mathcal{P}[p]$

provided the parameters have the following properties:

- $\mathcal{P}[\varepsilon_{\mathcal{A}}]$, and
- For every finite sequence p of elements of $\mathcal{A}$ and for every element x of $\mathcal{A}$ such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \frown \langle x \rangle]$.

2. The Two-element Field $\mathbf{Z}_2$

The field $\mathbf{Z}_2$ is defined by:

(Def. 2) $\mathbf{Z}_2 = \mathbb{Z}_2^{\mathrm{R}}$.

One can prove the following propositions:

(3) $\Omega_{\mathbf{Z}_2} = \{0, 1\}$.

(4) For every element a of $\mathbf{Z}_2$ holds $a = 0$ or $a = 1$.

(5) $0_{\mathbf{Z}_2} = 0$.

(6) $1_{\mathbf{Z}_2} = 1$.

(7) $1_{\mathbf{Z}_2} + 1_{\mathbf{Z}_2} = 0_{\mathbf{Z}_2}$.

(8) For every element x of $\mathbf{Z}_2$ holds $x = 0_{\mathbf{Z}_2}$ iff $x \neq 1_{\mathbf{Z}_2}$.

3. Set-theoretical Preliminaries

Let X, x be sets. The functor $X^{@}x$ yields an element of $\mathbf{Z}_2$ and is defined as follows:

(Def. 3) $X^{@}x = \begin{cases} 1_{\mathbf{Z}_2}, & \text{if } x \in X, \\ 0_{\mathbf{Z}_2}, & \text{otherwise.} \end{cases}$

Next we state several propositions:

(9) For all sets X, x holds $X^{@}x = 1_{\mathbf{Z}_2}$ iff $x \in X$.

(10) For all sets X, x holds $X^{@}x = 0_{\mathbf{Z}_2}$ iff $x \notin X$.

(11) For all sets X, x holds $X^{@}x \neq 0_{\mathbf{Z}_2}$ iff $X^{@}x = 1_{\mathbf{Z}_2}$.

(12) For all sets X, x, y holds $X^{@}x = X^{@}y$ iff $x \in X$ is equivalent to $y \in X$.

(13) For all sets X, Y, x holds $X^{@}x = Y^{@}x$ iff $x \in X$ is equivalent to $x \in Y$.

(14) For every set x holds $\emptyset^{@}x = 0_{\mathbf{Z}_2}$.

(15) For every set X and for all subsets u, v of X and for every element x of X holds $(u \dot{-} v)^{@}x = u^{@}x + v^{@}x$.

(16) For all sets X, Y holds $X = Y$ iff for every set x holds $X^{@}x = Y^{@}x$.

4. The Boolean Vector Space of Subsets of a Set

Let X be a set, let a be an element of $\mathbf{Z}_2$, and let c be a subset of X. The functor $a \cdot c$ yields a subset of X and is defined as follows:

(Def. 4)(i) $a \cdot c = c$ if $a = 1_{\mathbf{Z}_2}$,

(ii) $a \cdot c = \emptyset_X$ if $a = 0_{\mathbf{Z}_2}$.

Let X be a set. The functor Σ_X yields a binary operation on 2^X and is defined by:

(Def. 5) For all subsets c, d of X holds $\Sigma_X(c, d) = c \dot{-} d$.

We now state four propositions:

(17) For every element a of $\mathbf{Z}_2$ and for all subsets c, d of X holds $a \cdot (c \dot{-} d) = (a \cdot c) \dot{-} (a \cdot d)$.

(18) For all elements a, b of $\mathbf{Z}_2$ and for every subset c of X holds $(a + b) \cdot c = (a \cdot c) \dot{-} (b \cdot c)$.

(19) For every subset c of X holds $1_{\mathbf{Z}_2} \cdot c = c$.

(20) For all elements a, b of $\mathbf{Z}_2$ and for every subset c of X holds $a \cdot (b \cdot c) = a \cdot b \cdot c$.

Let X be a set. The functor $\cdot_X$ yielding a function from (the carrier of $\mathbf{Z}_2$) $\times$ 2^X into 2^X is defined by:

(Def. 6) For every element a of $\mathbf{Z}_2$ and for every subset c of X holds $\cdot_X(a, c) = a \cdot c$.

Let X be a set. The functor B_X yielding a non empty vector space structure over $\mathbf{Z}_2$ is defined as follows:

(Def. 7) $B_X = \langle 2^X, \Sigma_X, \emptyset_X, \cdot_X \rangle$.

The following propositions are true:

(21) B_X is Abelian.

(22) B_X is add-associative.

(23) B_X is right zeroed.

(24) B_X is right complementable.

(25) For every element a of $\mathbf{Z}_2$ and for all elements x, y of B_X holds $a \cdot (x + y) = a \cdot x + a \cdot y$.

(26) For all elements a, b of $\mathbf{Z}_2$ and for every element x of B_X holds $(a + b) \cdot x = a \cdot x + b \cdot x$.

(27) For all elements a, b of $\mathbf{Z}_2$ and for every element x of B_X holds $(a \cdot b) \cdot x = a \cdot (b \cdot x)$.

(28) For every element x of B_X holds $\mathbf{1}_{\mathbf{Z}_2} \cdot x = x$.

(29) B_X is vector space-like.

Let X be a set. One can verify that B_X is vector space-like, Abelian, right complementable, add-associative, and right zeroed.

5. The Linear Independence and Linear Span of Singleton Subsets

Let X be a set. We say that X is singleton if and only if:

(Def. 8) X is non empty and trivial.

One can check that every set which is singleton is also non empty and trivial and every set which is non empty and trivial is also singleton.

Let X be a set and let f be a subset of X. Let us observe that f is singleton if and only if:

(Def. 9) There exists a set x such that $x \in X$ and $f = \{x\}$.

Let X be a set. The functor S_X is defined as follows:

(Def. 10) $S_X = \{f \subseteq X\colon f \text{ is singleton}\}$.

Let X be a set. Then S_X is a subset of B_X.

Let X be a non empty set. One can check that S_X is non empty.

The following proposition is true

(30) For every non empty set X and for every subset f of X such that f is an element of S_X holds f is singleton.

Let F be a field, let V be a vector space over F, let l be a linear combination of V, and let x be an element of V. Then $l(x)$ is an element of F.

Let X be a non empty set, let s be a finite sequence of elements of B_X, and let x be an element of X. The functor $s^{@}x$ yielding a finite sequence of elements of $\mathbf{Z}_2$ is defined as follows:

(Def. 11) $\mathrm{len}(s^{@}x) = \mathrm{len}\, s$ and for every natural number j such that $1 \leq j \leq \mathrm{len}\, s$ holds $(s^{@}x)(j) = s(j)^{@}x$.

The following propositions are true:

(31) For every non empty set X and for every element x of X holds $\varepsilon_{(B_X)}{}^{@}x = \varepsilon_{(\mathbf{Z}_2)}$.

(32) For every set X and for all elements u, v of B_X and for every element x of X holds $(u+v)^{@}x = u^{@}x + v^{@}x$.

(33) Let X be a non empty set, s be a finite sequence of elements of B_X, f be an element of B_X, and x be an element of X. Then $(s \frown \langle f \rangle)^{@}x = (s^{@}x) \frown \langle f^{@}x \rangle$.

(34) Let X be a non empty set, s be a finite sequence of elements of B_X, and x be an element of X. Then $(\sum s)^{@}x = \sum s^{@}x$.

(35) Let X be a non empty set, l be a linear combination of B_X, and x be an element of B_X. If $x \in$ the support of l, then $l(x) = \mathbf{1}_{\mathbf{Z}_2}$.

(36) $S_\emptyset = \emptyset$.

(37) S_X is linearly independent.

(38) For every element f of B_X such that there exists a set x such that $x \in X$ and $f = \{x\}$ holds $f \in S_X$.

(39) For every finite set X and for every subset A of X there exists a linear combination l of S_X such that $\sum l = A$.

(40) For every finite set X holds $\mathrm{Lin}(S_X) = B_X$.

(41) For every finite set X holds S_X is a basis of B_X.

Let X be a finite set. Observe that S_X is finite.

Let X be a finite set. One can verify that B_X is finite dimensional.

Next we state three propositions:

(42) $\overline{\overline{S_X}} = \overline{\overline{X}}$.

(43) $\overline{\overline{\Omega_{B_X}}} = 2^{\overline{\overline{X}}}$.

(44) $\dim(B_\emptyset) = 0$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[3] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[7] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[9] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[10] John L. Kelley. *General Topology*, volume 27 of *Graduate Texts in Mathematics*. Springer-Verlag, 1955.
[11] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[12] Christoph Schwarzweller. The ring of integers, euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[13] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[14] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[15] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 1990.
[16] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[17] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1(**5**):877–882, 1990.
[18] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[20] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[21] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received October 9, 2007

FORMALIZED MATHEMATICS
Vol. **16**, No. **1**, Pages 7–17, **2008**

Euler's Polyhedron Formula

Jesse Alama
Department of Philosophy
Stanford University
USA

Summary. Euler's polyhedron theorem states for a polyhedron p, that

$$V - E + F = 2,$$

where V, E, and F are, respectively, the number of vertices, edges, and faces of p. The formula was first stated in print by Euler in 1758 [11]. The proof given here is based on Poincaré's linear algebraic proof, stated in [17] (with a corrected proof in [18]), as adapted by Imre Lakatos in the latter's *Proofs and Refutations* [15].

As is well known, Euler's formula is not true for all polyhedra. The condition on polyhedra considered here is that of being a homology sphere, which says that the cycles (chains whose boundary is zero) are exactly the bounding chains (chains that are the boundary of a chain of one higher dimension).

The present proof actually goes beyond the three-dimensional version of the polyhedral formula given by Lakatos; it is dimension-free, in the sense that it gives a formula in which the dimension of the polyhedron is a parameter. The classical Euler relation $V - E + F = 2$ is corresponds to the case where the dimension of the polyhedron is 3.

The main theorem, expressed in the language of the present article, is

$$\texttt{Sum alternating} - \texttt{characteristic} - \texttt{sequence}(\texttt{p}) = 0,$$

where p is a polyhedron. The alternating characteristic sequence of a polyhedron is the sequence

$$-N(-1), +N(0), -N(1), \ldots, (-1)^{\dim(p)} * N(\dim(p)),$$

where $N(k)$ is the number of polytopes of p of dimension k. The special case of $\dim(p) = 3$ yields Euler's classical relation. ($N(-1)$ and $N(3)$ will turn out to be equal, by definition, to 1.)

Two other special cases are proved: the first says that a one-dimensional "polyhedron" that is a homology sphere consists of just two vertices (and thus consists of just a single edge); the second special case asserts that a two-dimensional polyhedron that is a homology sphere (a polygon) has as many vertices as edges.

A treatment of the more general version of Euler's relation can be found in [12] and [6]. The former contains a proof of Steinitz's theorem, which shows

ISSN 1426–2630(p), 1898-9934(e)

that the abstract polyhedra treated in Poincaré's proof, which might not appear to be about polyhedra in the usual sense of the word, are in fact embeddable in $\mathbf{R}^3$ under certain conditions. It would be valuable to formalize a proof of Steinitz's theorem and relate it to the development contained here.

MML identifier: `POLYFORM`, version: `7.8.05 4.89.993`

The terminology and notation used here are introduced in the following articles: [9], [27], [28], [7], [8], [21], [10], [4], [22], [3], [5], [14], [19], [26], [23], [13], [25], [24], [16], [20], [29], [1], and [2].

1. Set-theoretical Preliminaries

The following propositions are true:

(1) For all sets X, c, d such that there exist sets a, b such that $a \neq b$ and $X = \{a, b\}$ and c, $d \in X$ and $c \neq d$ holds $X = \{c, d\}$.

(2) For every function f such that f is one-to-one holds $\overline{\overline{\mathrm{dom}\, f}} = \overline{\overline{\mathrm{rng}\, f}}$.

2. Arithmetical Preliminaries

In the sequel n denotes a natural number and k denotes an integer.

Next we state the proposition

(3) If $1 \leq k$, then k is a natural number.

Let a be an integer and let b be a natural number. Then $a \cdot b$ is an element of $\mathbb{Z}$.

One can prove the following propositions:

(4) 1 is odd.

(5) 2 is even.

(6) 3 is odd.

(7) 4 is even.

(8) If n is even, then $(-1)^n = 1$.

(9) If n is odd, then $(-1)^n = -1$.

(10) $(-1)^n$ is an integer.

Let a be an integer and let n be a natural number. Then a^n is an element of $\mathbb{Z}$.

We now state four propositions:

(11) For all finite sequences p, q, r holds $\mathrm{len}(p \frown q) \leq \mathrm{len}(p \frown (q \frown r))$.

(12) $1 < n + 2$.

(13) $(-1)^2 = 1$.

(14) For every natural number n holds $(-1)^n = (-1)^{n+2}$.

3. Preliminaries on Finite Sequences

Let f be a finite sequence of elements of $\mathbb{Z}$ and let k be a natural number. Observe that f_k is integer.

The following propositions are true:

(15) Let a, b, s be finite sequences of elements of $\mathbb{Z}$. Suppose that

(i) $\operatorname{len} s > 0$,

(ii) $\operatorname{len} a = \operatorname{len} s$,

(iii) $\operatorname{len} s = \operatorname{len} b$,

(iv) for every natural number n such that $1 \leq n \leq \operatorname{len} s$ holds $s_n = a_n + b_n$, and

(v) for every natural number k such that $1 \leq k < \operatorname{len} s$ holds $b_k = -a_{k+1}$.

Then $\sum s = a_1 + b_{\operatorname{len} s}$.

(16) For all finite sequences p, q, r holds $\operatorname{len}(p \frown q \frown r) = \operatorname{len} p + \operatorname{len} q + \operatorname{len} r$.

(17) For every set x and for all finite sequences p, q holds $(\langle x \rangle \frown p \frown q)_1 = x$.

(18) For every set x and for all finite sequences p, q holds $(p \frown q \frown \langle x \rangle)_{\operatorname{len} p + \operatorname{len} q + 1} = x$.

(19) For all finite sequences p, q, r and for every natural number k such that $\operatorname{len} p < k \leq \operatorname{len}(p \frown q)$ holds $(p \frown q \frown r)_k = q_{k - \operatorname{len} p}$.

Let a be an integer. Then $\langle a \rangle$ is a finite sequence of elements of $\mathbb{Z}$.

Let a, b be integers. Then $\langle a, b \rangle$ is a finite sequence of elements of $\mathbb{Z}$.

Let a, b, c be integers. Then $\langle a, b, c \rangle$ is a finite sequence of elements of $\mathbb{Z}$.

Let p, q be finite sequences of elements of $\mathbb{Z}$. Then $p \frown q$ is a finite sequence of elements of $\mathbb{Z}$.

We now state four propositions:

(20) For all finite sequences p, q of elements of $\mathbb{Z}$ holds $\sum p \frown q = (\sum p) + \sum q$.

(21) For every integer k and for every finite sequence p of elements of $\mathbb{Z}$ holds $\sum \langle k \rangle \frown p = k + \sum p$.

(22) For all finite sequences p, q, r of elements of $\mathbb{Z}$ holds $\sum p \frown q \frown r = (\sum p) + \sum q + \sum r$.

(23) For every element a of $\mathbf{Z}_2$ holds $\sum \langle a \rangle = a$.

4. Polyhedra and Incidence Matrices

Let X, Y be sets. An incidence matrix of X and Y is an element of $\{0_{\mathbf{Z}_2}, 1_{\mathbf{Z}_2}\}^{X \times Y}$.

We now state the proposition

(24) For all sets X, Y holds $X \times Y \longmapsto 1_{\mathbf{Z}_2}$ is an incidence matrix of X and Y.

Polyhedron is defined by the condition (Def. 1).

(Def. 1) There exists a finite sequence-yielding finite sequence F and there exists a function yielding finite sequence I such that

(i) $\operatorname{len} I = \operatorname{len} F - 1$,

(ii) for every natural number n such that $1 \leq n < \operatorname{len} F$ holds $I(n)$ is an incidence matrix of $\operatorname{rng} F(n)$ and $\operatorname{rng} F(n+1)$,

(iii) for every natural number n such that $1 \leq n \leq \operatorname{len} F$ holds $F(n)$ is non empty and $F(n)$ is one-to-one, and

(iv) it $= \langle F, I \rangle$.

In the sequel p denotes a polyhedron, k denotes an integer, and n denotes a natural number.

Let us consider p. Then $p_{\mathbf{1}}$ is a finite sequence-yielding finite sequence. Then $p_{\mathbf{2}}$ is a function yielding finite sequence.

Let p be a polyhedron. The functor $\dim(p)$ yielding an element of $\mathbb{N}$ is defined by:

(Def. 2) $\dim(p) = \operatorname{len}(p_{\mathbf{1}})$.

Let p be a polyhedron and let k be an integer. The functor $P_{k,p}$ yielding a finite set is defined by the conditions (Def. 3).

(Def. 3)(i) If $k < -1$, then $P_{k,p} = \emptyset$,

(ii) if $k = -1$, then $P_{k,p} = \{\emptyset\}$,

(iii) if $-1 < k < \dim(p)$, then $P_{k,p} = \operatorname{rng} p_{\mathbf{1}}(k+1)$,

(iv) if $k = \dim(p)$, then $P_{k,p} = \{p\}$, and

(v) if $k > \dim(p)$, then $P_{k,p} = \emptyset$.

One can prove the following two propositions:

(25) If $-1 < k < \dim(p)$, then $k+1$ is a natural number and $1 \leq k+1 \leq \dim(p)$.

(26) $P_{k,p}$ is non empty iff $-1 \leq k \leq \dim(p)$.

Let p be a polyhedron and let k be an integer. Let us assume that $-1 \leq k \leq \dim(p)$. k-polytope of p is defined by:

(Def. 4) It $\in P_{k,p}$.

Next we state the proposition

(27) If $k < \dim(p)$, then $k - 1 < \dim(p)$.

Let p be a polyhedron and let k be an integer. The functor $\eta_{p,k}$ yielding an incidence matrix of $P_{k-1,p}$ and $P_{k,p}$ is defined by the conditions (Def. 5).

(Def. 5)(i) If $k < 0$, then $\eta_{p,k} = \emptyset$,

(ii) if $k = 0$, then $\eta_{p,k} = \{\emptyset\} \times P_{0,p} \longmapsto 1_{\mathbf{Z}_2}$,

(iii) if $0 < k < \dim(p)$, then $\eta_{p,k} = p_{\mathbf{2}}(k)$,

(iv) if $k = \dim(p)$, then $\eta_{p,k} = P_{\dim(p)-1,p} \times \{p\} \longmapsto 1_{\mathbf{Z}_2}$, and

(v) if $k > \dim(p)$, then $\eta_{p,k} = \emptyset$.

Let p be a polyhedron and let k be an integer. The functor $S_{k,p}$ yielding a finite sequence is defined by the conditions (Def. 6).

(Def. 6)(i) If $k < -1$, then $S_{k,p} = \varepsilon_{\emptyset}$,

(ii) if $k = -1$, then $S_{k,p} = \langle \emptyset \rangle$,

(iii) if $-1 < k < \dim(p)$, then $S_{k,p} = p_{\mathbf{1}}(k+1)$,

(iv) if $k = \dim(p)$, then $S_{k,p} = \langle p \rangle$, and

(v) if $k > \dim(p)$, then $S_{k,p} = \varepsilon_{\emptyset}$.

Let p be a polyhedron and let k be an integer. The functor $N_{p,k}$ yielding an element of $\mathbb{N}$ is defined as follows:

(Def. 7) $N_{p,k} = \overline{\overline{P_{k,p}}}$.

Let p be a polyhedron. The functor V_p yields an element of $\mathbb{N}$ and is defined by:

(Def. 8) $V_p = N_{p,0}$.

The functor E_p yields an element of $\mathbb{N}$ and is defined by:

(Def. 9) $E_p = N_{p,1}$.

The functor F_p yielding an element of $\mathbb{N}$ is defined by:

(Def. 10) $F_p = N_{p,2}$.

Next we state several propositions:

(28) $\mathrm{dom}(S_{k,p}) = \mathrm{Seg}(N_{p,k})$.

(29) $\mathrm{len}(S_{k,p}) = N_{p,k}$.

(30) $\mathrm{rng}(S_{k,p}) = P_{k,p}$.

(31) $N_{p,-1} = 1$.

(32) $N_{p,\dim(p)} = 1$.

Let p be a polyhedron, let k be an integer, and let n be a natural number. Let us assume that $1 \leq n \leq N_{p,k}$ and $-1 \leq k \leq \dim(p)$. The functor $P^n_{p,k}$ yielding an element of $P_{k,p}$ is defined by:

(Def. 11) $P^n_{p,k} = S_{k,p}(n)$.

We now state three propositions:

(33) Suppose $-1 \leq k \leq \dim(p)$. Let x be a k-polytope of p. Then there exists a natural number n such that $x = P^n_{p,k}$ and $1 \leq n \leq N_{p,k}$.

(34) $S_{k,p}$ is one-to-one.

(35) Suppose $-1 \leq k \leq \dim(p)$. Let m, n be natural numbers. If $1 \leq n \leq N_{p,k}$ and $1 \leq m \leq N_{p,k}$ and $P^n_{p,k} = P^m_{p,k}$, then $m = n$.

Let p be a polyhedron, let k be an integer, let x be a $(k-1)$-polytope of p, and let y be a k-polytope of p. Let us assume that $0 \leq k \leq \dim(p)$. The functor $x(y)$ yields an element of $\mathbf{Z}_2$ and is defined by:

(Def. 12) $x(y) = \eta_{p,k}(x, y)$.

5. The Chain Spaces and their Subspaces. Boundary of a k-chain

Let p be a polyhedron and let k be an integer. The functor $C_{k,p}$ yielding a finite dimensional vector space over $\mathbf{Z}_2$ is defined by:

(Def. 13) $C_{k,p} = B_{P_{k,p}}$.

We now state two propositions:

(36) For every k-polytope x of p holds $0_{C_{k,p}}{}^{@}x = 0_{\mathbf{Z}_2}$.

(37) $N_{p,k} = \dim(C_{k,p})$.

Let p be a polyhedron and let k be an integer. The functor k-chains p yielding a non empty finite set is defined by:

(Def. 14) k-chains $p = 2^{P_{k,p}}$.

Let p be a polyhedron, let k be an integer, let x be a $(k-1)$-polytope of p, and let v be an element of $C_{k,p}$. The functor $v(x)$ yielding a finite sequence of elements of $\mathbf{Z}_2$ is defined by the conditions (Def. 15).

(Def. 15)(i) If $P_{k-1,p}$ is empty, then $v(x) = \varepsilon_{\emptyset}$, and

(ii) if $P_{k-1,p}$ is non empty, then $\mathrm{len}(v(x)) = N_{p,k}$ and for every natural number n such that $1 \leq n \leq N_{p,k}$ holds $v(x)(n) = (v^{@}P^n_{p,k}) \cdot x(P^n_{p,k})$.

We now state several propositions:

(38) For all elements c, d of $C_{k,p}$ and for every k-polytope x of p holds $(c+d)^{@}x = c^{@}x + d^{@}x$.

(39) For all elements c, d of $C_{k,p}$ and for every $(k-1)$-polytope x of p holds $(c+d)(x) = c(x) + d(x)$.

(40) For all elements c, d of $C_{k,p}$ and for every $(k-1)$-polytope x of p holds $\sum(c(x) + d(x)) = (\sum c(x)) + \sum d(x)$.

(41) For all elements c, d of $C_{k,p}$ and for every $(k-1)$-polytope x of p holds $\sum(c+d)(x) = (\sum c(x)) + \sum d(x)$.

(42) For every element c of $C_{k,p}$ and for every element a of $\mathbf{Z}_2$ and for every k-polytope x of p holds $(a \cdot c)^{@}x = a \cdot (c^{@}x)$.

(43) For every element c of $C_{k,p}$ and for every element a of $\mathbf{Z}_2$ and for every k-polytope x of p holds $(a \cdot c)(x) = a \cdot c(x)$.

(44) For all elements c, d of $C_{k,p}$ holds $c = d$ iff for every k-polytope x of p holds $c^{@}x = d^{@}x$.

(45) For all elements c, d of $C_{k,p}$ holds $c = d$ iff for every k-polytope x of p holds $x \in c$ iff $x \in d$.

The scheme *ChainEx* deals with a polyhedron $\mathcal{A}$, an integer $\mathcal{B}$, and a unary predicate $\mathcal{P}$, and states that:

There exists a subset c of $P_{\mathcal{B},\mathcal{A}}$ such that for every $\mathcal{B}$-polytope x of $\mathcal{A}$ holds $x \in c$ iff $\mathcal{P}[x]$ and $x \in P_{\mathcal{B},\mathcal{A}}$

for all values of the parameters.

Let p be a polyhedron, let k be an integer, and let v be an element of $C_{k,p}$. The functor ∂v yields an element of $C_{k-1,p}$ and is defined by the conditions (Def. 16).

(Def. 16)(i) If $P_{k-1,p}$ is empty, then $\partial v = 0_{C_{k-1,p}}$, and

(ii) if $P_{k-1,p}$ is non empty, then for every $(k-1)$-polytope x of p holds $x \in \partial v$ iff $\sum v(x) = 1_{\mathbf{Z}_2}$.

One can prove the following proposition

(46) For every element c of $C_{k,p}$ and for every $(k-1)$-polytope x of p holds $\partial c^{@} x = \sum c(x)$.

Let p be a polyhedron and let k be an integer. The functor $\partial_k p$ yields a function from $C_{k,p}$ into $C_{k-1,p}$ and is defined by:

(Def. 17) For every element c of $C_{k,p}$ holds $\partial_k p(c) = \partial c$.

One can prove the following propositions:

(47) For all elements c, d of $C_{k,p}$ holds $\partial(c + d) = \partial c + \partial d$.

(48) For every element a of $\mathbf{Z}_2$ and for every element c of $C_{k,p}$ holds $\partial(a \cdot c) = a \cdot \partial c$.

(49) $\partial_k p$ is a linear transformation from $C_{k,p}$ to $C_{k-1,p}$.

Let p be a polyhedron and let k be an integer. Then $\partial_k p$ is a linear transformation from $C_{k,p}$ to $C_{k-1,p}$.

Let p be a polyhedron and let k be an integer. The functor $Z_{k,p}$ yielding a subspace of $C_{k,p}$ is defined as follows:

(Def. 18) $Z_{k,p} = \ker \partial_k p$.

Let p be a polyhedron and let k be an integer. The functor $|Z_{k,p}|$ yields a non empty subset of k-chains p and is defined by:

(Def. 19) $|Z_{k,p}| = \Omega_{Z_{k,p}}$.

Let p be a polyhedron and let k be an integer. The functor $B_{k,p}$ yields a subspace of $C_{k,p}$ and is defined as follows:

(Def. 20) $B_{k,p} = \mathrm{im}(\partial_{k+1} p)$.

Let p be a polyhedron and let k be an integer. The functor $|B_{k,p}|$ yielding a non empty subset of k-chains p is defined by:

(Def. 21) $|B_{k,p}| = \Omega_{B_{k,p}}$.

Let p be a polyhedron and let k be an integer. The functor $\mathrm{BZ}_{k,p}$ yields a subspace of $C_{k,p}$ and is defined as follows:

(Def. 22) $\mathrm{BZ}_{k,p} = B_{k,p} \cap Z_{k,p}$.

Let p be a polyhedron and let k be an integer.

The functor k-bounding-circuits p yields a non empty subset of k-chains p and is defined as follows:

(Def. 23) k-bounding-circuits $p = \Omega_{\mathrm{BZ}_{k,p}}$.

The following proposition is true

(50) $\dim(C_{k,p}) = \mathrm{rank}(\partial_k p) + \mathrm{nullity}(\partial_k p)$.

6. Simply Connected and Eulerian Polyhedra

Let p be a polyhedron. We say that p is being a homology sphere if and only if:

(Def. 24) For every integer k holds $|Z_{k,p}| = |B_{k,p}|$.

The following proposition is true

(51) p is being a homology sphere iff for every integer n holds $Z_{n,p} = B_{n,p}$.

Let p be a polyhedron. The functor $\widehat{p}$ yielding a finite sequence of elements of $\mathbb{Z}$ is defined as follows:

(Def. 25) $\mathrm{len}\,\widehat{p} = \dim(p) + 2$ and for every natural number k such that $1 \leq k \leq \dim(p) + 2$ holds $\widehat{p}(k) = (-1)^k \cdot N_{p,k-2}$.

Let p be a polyhedron. The functor $\bar{p}$ yields a finite sequence of elements of $\mathbb{Z}$ and is defined by:

(Def. 26) $\mathrm{len}\,\bar{p} = \dim(p)$ and for every natural number k such that $1 \leq k \leq \dim(p)$ holds $\bar{p}(k) = (-1)^{k+1} \cdot N_{p,k-1}$.

Let p be a polyhedron. The functor $\overline{p}$ yielding a finite sequence of elements of $\mathbb{Z}$ is defined as follows:

(Def. 27) $\mathrm{len}\,\overline{p} = \dim(p) + 1$ and for every natural number k such that $1 \leq k \leq \dim(p) + 1$ holds $\overline{p}(k) = (-1)^{k+1} \cdot N_{p,k-1}$.

One can prove the following proposition

(52) If $1 \leq n \leq \mathrm{len}\,\bar{p}$, then $\bar{p}(n) = (-1)^{n+1} \cdot \dim(B_{n-2,p}) + (-1)^{n+1} \cdot \dim(Z_{n-1,p})$.

Let p be a polyhedron. We say that p is Eulerian if and only if:

(Def. 28) $\sum \bar{p} = 1 + (-1)^{\dim(p)+1}$.

One can prove the following proposition

(53) $\overline{p} = \bar{p} ^\frown \langle (-1)^{\dim(p)} \rangle$.

Let p be a polyhedron. Let us observe that p is Eulerian if and only if:

(Def. 29) $\sum \overline{p} = 1$.

One can prove the following proposition

(54) $\widehat{p} = \langle -1 \rangle \frown \overline{p}$.

Let p be a polyhedron. Let us observe that p is Eulerian if and only if:

(Def. 30) $\sum \widehat{p} = 0$.

7. The Extremal Chain Spaces

The following propositions are true:

(55) $P_{0,p}$ is non empty.

(56) $\overline{\overline{\Omega_{C_{-1,p}}}} = 2$.

(57) $\Omega_{C_{-1,p}} = \{\emptyset, \{\emptyset\}\}$.

(58) For every k-polytope x of p and for every $(k-1)$-polytope e of p such that $k = 0$ and $e = \emptyset$ holds $e(x) = 1_{\mathbf{Z}_2}$.

(59) Let k be an integer, x be a k-polytope of p, v be an element of $C_{k,p}$, e be a $(k-1)$-polytope of p, and n be a natural number. If $k = 0$ and $v = \{x\}$ and $e = \emptyset$ and $x = P^n_{p,k}$ and $1 \leq n \leq N_{p,k}$, then $v(e)(n) = 1_{\mathbf{Z}_2}$.

(60) Let k be an integer, x be a k-polytope of p, e be a $(k-1)$-polytope of p, v be an element of $C_{k,p}$, and m, n be natural numbers. Suppose $k = 0$ and $v = \{x\}$ and $x = P^n_{p,k}$ and $1 \leq m \leq N_{p,k}$ and $1 \leq n \leq N_{p,k}$ and $m \neq n$. Then $v(e)(m) = 0_{\mathbf{Z}_2}$.

(61) Let k be an integer, x be a k-polytope of p, v be an element of $C_{k,p}$, and e be a $(k-1)$-polytope of p. If $k = 0$ and $v = \{x\}$ and $e = \emptyset$, then $\sum v(e) = 1_{\mathbf{Z}_2}$.

(62) For every 0-polytope x of p holds $\partial_0 p(\{x\}) = \{\emptyset\}$.

(63) $\dim(B_{(-1),p}) = 1$.

(64) $\overline{\overline{\Omega_{C_{\dim(p),p}}}} = 2$.

(65) $\{p\}$ is an element of $C_{\dim(p),p}$.

(66) $\{p\} \in \Omega_{C_{\dim(p),p}}$.

(67) $P_{\dim(p)-1,p}$ is non empty.

Let p be a polyhedron. Note that $P_{\dim(p)-1,p}$ is non empty.

The following propositions are true:

(68) $\Omega_{C_{\dim(p),p}} = \{0_{C_{\dim(p),p}}, \{p\}\}$.

(69) For every element x of $C_{\dim(p),p}$ holds $x = 0_{C_{\dim(p),p}}$ or $x = \{p\}$.

(70) For all elements x, y of $C_{\dim(p),p}$ such that $x \neq y$ holds $x = 0_{C_{\dim(p),p}}$ or $y = 0_{C_{\dim(p),p}}$.

(71) $S_{\dim(p),p} = \langle p \rangle$.

(72) $P^1_{p,\dim(p)} = p$.

(73) For every element c of $C_{\dim(p),p}$ and for every $\dim(p)$-polytope x of p such that $c = \{p\}$ holds $c^{@}x = 1_{\mathbf{Z}_2}$.

(74) For every $(\dim(p) - 1)$-polytope x of p and for every $\dim(p)$-polytope c of p such that $c = p$ holds $x(c) = 1_{\mathbf{Z}_2}$.

(75) For every $(\dim(p)-1)$-polytope x of p and for every element c of $C_{\dim(p),p}$ such that $c = \{p\}$ holds $c(x) = \langle 1_{\mathbf{Z}_2} \rangle$.

(76) For every $(\dim(p)-1)$-polytope x of p and for every element c of $C_{\dim(p),p}$ such that $c = \{p\}$ holds $\sum c(x) = 1_{\mathbf{Z}_2}$.

(77) $\partial_{\dim(p)} p(\{p\}) = P_{\dim(p)-1,p}$.

(78) $\partial_{\dim(p)} p$ is one-to-one.

(79) $\dim(B_{\dim(p)-1,p}) = 1$.

(80) If p is being a homology sphere, then $\dim(Z_{\dim(p)-1,p}) = 1$.

(81) If $1 < n < \dim(p) + 2$, then $\widehat{p}(n) = \bar{p}(n - 1)$.

(82) $\widehat{p} = \langle -1 \rangle \frown \bar{p} \frown \langle (-1)^{\dim(p)} \rangle$.

8. A Generalized Euler Relation and its 1−, 2−, and 3−dimensional Special Cases

One can prove the following propositions:

(83) If $\dim(p)$ is odd, then $\sum \widehat{p} = (\sum \bar{p}) - 2$.

(84) If $\dim(p)$ is even, then $\sum \widehat{p} = \sum \bar{p}$.

(85) If $\dim(p) = 1$, then $\sum \bar{p} = N_{p,0}$.

(86) If $\dim(p) = 2$, then $\sum \bar{p} = N_{p,0} - N_{p,1}$.

(87) If $\dim(p) = 3$, then $\sum \bar{p} = (N_{p,0} - N_{p,1}) + N_{p,2}$.

(88) If $\dim(p) = 0$, then p is Eulerian.

(89) If p is being a homology sphere, then p is Eulerian.

(90) If p is being a homology sphere and $\dim(p) = 1$, then $V_p = 2$.

(91) If p is being a homology sphere and $\dim(p) = 2$, then $V_p = E_p$.

(92) If p is being a homology sphere and $\dim(p) = 3$, then $(V_p - E_p) + F_p = 2$.

References

[1] Jesse Alama. The rank+nullity theorem. *Formalized Mathematics*, 15(**3**):137–142, 2007.
[2] Jesse Alama. The vector space of subsets of a set based on symmetric difference. *Formalized Mathematics*, 16(**1**):1–5, 2008.
[3] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[4] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[6] Arne Brøndsted. *An Introduction to Convex Polytopes.* Graduate Texts in Mathematics. Springer, 1983.

[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. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[11] Leonhard Euler. Elementa doctrinae solidorum. *Novi Commentarii Academiae Scientarum Petropolitanae*, 4:109–140, 1758.
[12] Branko Grünbaum. *Convex Polytopes*. Number 221 in Graduate Texts in Mathematics. Springer, 2nd edition, 2003.
[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] Imre Lakatos. *Proofs and Refutations: The Logic of Mathematical Discovery*. Cambridge University Press, 1976. Edited by John Worrall and Elie Zahar.
[16] Michał Muzalewski. Rings and modules – part II. *Formalized Mathematics*, 2(**4**):579–585, 1991.
[17] Henri Poincaré. Sur la généralisation d'un théorème d'Euler relatif aux polyèdres. *Comptes Rendus de Séances de l'Academie des Sciences*, 117:144, 1893.
[18] Henri Poincaré. Complément à l'analysis situs. *Rendiconti del Circolo Matematico di Palermo*, 13:285–343, 1899.
[19] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.
[20] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.
[21] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[22] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[23] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[24] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1(**5**):877–882, 1990.
[25] Wojciech A. Trybulec. Subspaces and cosets of subspaces in vector space. *Formalized Mathematics*, 1(**5**):865–870, 1990.
[26] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[27] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[28] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[29] Mariusz Żynel. The Steinitz theorem and the dimension of a vector space. *Formalized Mathematics*, 5(**3**):423–428, 1996.

Received October 9, 2007

FORMALIZED MATHEMATICS
Vol. **16**, No. **1**, Pages 19–21, **2008**

Uniform Boundedness Principle

Hideki Sakurai
Shinshu University
Nagano, Japan

Hisayoshi Kunimune
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article at first, we proved the lemma of the inferior limit and the superior limit. Next, we proved the Baire category theorem (Banach space version) [20], [9], [3], quoted it and proved the uniform boundedness principle. Moreover, the proof of the Banach-Steinhaus theorem is added.

MML identifier: `LOPBAN_5`, version: `7.8.05 4.89.993`

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

1. Uniform Boundedness Principle

The following two propositions are true:

(1) For every sequence s_1 of real numbers and for every real number r such that s_1 is bounded and $0 \leq r$ holds $\liminf(r\, s_1) = r \cdot \liminf s_1$.

(2) For every sequence s_1 of real numbers and for every real number r such that s_1 is bounded and $0 \leq r$ holds $\limsup(r\, s_1) = r \cdot \limsup s_1$.

Let X be a real Banach space. One can verify that MetricSpaceNorm X is complete.

Let X be a real Banach space, let x_0 be a point of X, and let r be a real number. The functor $\mathrm{Ball}(x_0, r)$ yielding a subset of X is defined as follows:

(Def. 1) $\mathrm{Ball}(x_0, r) = \{x; x$ ranges over points of X: $\|x_0 - x\| < r\}$.

The following propositions are true:

(3) Let X be a real Banach space and Y be a sequence of subsets of X. Suppose $\bigcup \mathrm{rng}\, Y =$ the carrier of X and for every element n of $\mathbb{N}$ holds $Y(n)$ is closed. Then there exists an element n_0 of $\mathbb{N}$ and there exists

ISSN 1426–2630(p), 1898-9934(e)

a real number r and there exists a point x_0 of X such that $0 < r$ and $\mathrm{Ball}(x_0, r) \subseteq Y(n_0)$.

(4) Let X, Y be real normed spaces and f be a bounded linear operator from X into Y. Then

(i) f is Lipschitzian on the carrier of X and continuous on the carrier of X, and

(ii) for every point x of X holds f is continuous in x.

(5) Let X be a real Banach space, Y be a real normed space, and T be a subset of the real norm space of bounded linear operators from X into Y. Suppose that for every point x of X there exists a real number K such that $0 \leq K$ and for every point f of the real norm space of bounded linear operators from X into Y such that $f \in T$ holds $\|f(x)\| \leq K$. Then there exists a real number L such that

(i) $0 \leq L$, and

(ii) for every point f of the real norm space of bounded linear operators from X into Y such that $f \in T$ holds $\|f\| \leq L$.

Let X, Y be real normed spaces, let H be a function from $\mathbb{N}$ into the carrier of the real norm space of bounded linear operators from X into Y, and let x be a point of X. The functor $H\#x$ yields a sequence of Y and is defined by:

(Def. 2) For every element n of $\mathbb{N}$ holds $(H\#x)(n) = H(n)(x)$.

The following proposition is true

(6) Let X be a real Banach space, Y be a real normed space, v_1 be a sequence of the real norm space of bounded linear operators from X into Y, and t_1 be a function from X into Y. Suppose that for every point x of X holds $v_1\#x$ is convergent and $t_1(x) = \lim(v_1\#x)$. Then

(i) t_1 is a bounded linear operator from X into Y,

(ii) for every point x of X holds $\|t_1(x)\| \leq \liminf\|v_1\| \cdot \|x\|$, and

(iii) for every point t_2 of the real norm space of bounded linear operators from X into Y such that $t_2 = t_1$ holds $\|t_2\| \leq \liminf\|v_1\|$.

2. Banach-Steinhaus Theorem

We now state two propositions:

(7) Let X be a real Banach space, X_0 be a subset of LinearTopSpaceNorm X, Y be a real Banach space, and v_1 be a sequence of the real norm space of bounded linear operators from X into Y. Suppose that

(i) X_0 is dense,

(ii) for every point x of X such that $x \in X_0$ holds $v_1\#x$ is convergent, and

(iii) for every point x of X there exists a real number K such that $0 \leq K$ and for every element n of $\mathbb{N}$ holds $\|(v_1\#x)(n)\| \leq K$.

Let x be a point of X. Then $v_1\#x$ is convergent.

(8) Let X, Y be real Banach spaces, X_0 be a subset of LinearTopSpaceNorm X, and v_1 be a sequence of the real norm space of bounded linear operators from X into Y. Suppose that (i) X_0 is dense,

(ii) for every point x of X such that $x \in X_0$ holds $v_1 \# x$ is convergent, and

(iii) for every point x of X there exists a real number K such that $0 \leq K$ and for every element n of $\mathbb{N}$ holds $\|(v_1 \# x)(n)\| \leq K$.

Then there exists a point t_1 of the real norm space of bounded linear operators from X into Y such that for every point x of X holds $v_1 \# x$ is convergent and $t_1(x) = \lim(v_1 \# x)$ and $\|t_1(x)\| \leq \liminf \|v_1\| \cdot \|x\|$ and $\|t_1\| \leq \liminf \|v_1\|$.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[2] Czesław Byliński. Introduction to real linear topological spaces. *Formalized Mathematics*, 13(**1**):99–107, 2005.
[3] N. J. Dunford and T. Schwartz. *Linear operators I.* Interscience Publ., 1958.
[4] Noboru Endou, Yasunari Shidama, and Katsumasa Okamura. Baire's category theorem and some spaces generated from real normed space. *Formalized Mathematics*, 14(**4**):213–219, 2006.
[5] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[6] Stanisława Kanas, Adam Lecko, and Mariusz Startek. Metric spaces. *Formalized Mathematics*, 1(**3**):607–610, 1990.
[7] Jarosław Kotowicz. Convergent sequences and the limit of sequences. *Formalized Mathematics*, 1(**2**):273–275, 1990.
[8] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[9] Isao Miyadera. *Functional Analysis.* Riko-Gaku-Sya, 1972.
[10] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.
[11] Takaya Nishiyama, Keiji Ohkubo, and Yasunari Shidama. The continuous functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):269–275, 2004.
[12] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[13] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[14] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.
[15] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[16] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[17] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[18] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[19] Mirosław Wysocki and Agata Darmochwał. Subsets of topological spaces. *Formalized Mathematics*, 1(**1**):231–237, 1990.
[20] Kosaku Yoshida. *Functional Analysis.* Springer, 1980.
[21] Bo Zhang, Hiroshi Yamazaki, and Yatsuka Nakamura. Inferior limit and superior limit of sequences of real numbers. *Formalized Mathematics*, 13(**3**):375–381, 2005.

Received October 9, 2007

FORMALIZED MATHEMATICS
Vol. **16**, No. **1**, Pages 23–28, **2008**

Gauss Lemma and Law of Quadratic Reciprocity

Li Yan
Qingdao University of Science and Technology
China

Xiquan Liang
Qingdao University of Science and Technology
China

Junjie Zhao
Qingdao University of Science and Technology
China

Summary. In this paper, we defined the quadratic residue and proved its fundamental properties on the base of some useful theorems. Then we defined the Legendre symbol and proved its useful theorems [14], [12]. Finally, Gauss Lemma and Law of Quadratic Reciprocity are proven.

MML identifier: `INT_5`, version: `7.8.05 4.89.993`

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

For simplicity, we adopt the following convention: i, i_1, i_2, i_3, j, a, b, x denote integers, d, e, n denote natural numbers, f, f' denote finite sequences of elements of $\mathbb{Z}$, g, g_1, g_2 denote finite sequences of elements of $\mathbb{R}$, and p denotes a prime number.

We now state two propositions:

(1) If $i_1 \mid i_2$ and $i_1 \mid i_3$, then $i_1 \mid i_2 - i_3$.

(2) If $i \mid a$ and $i \mid a - b$, then $i \mid b$.

Let us consider f. The functor $\mathcal{P}_{\mathbb{Z}}(f)$ yields a function from $\mathbb{Z}$ into $\mathbb{Z}$ and is defined by the condition (Def. 1).

ISSN 1426–2630(p), 1898-9934(e)

(Def. 1) Let x be an element of $\mathbb{Z}$. Then there exists a finite sequence f' of elements of $\mathbb{Z}$ such that $\operatorname{len} f' = \operatorname{len} f$ and for every d such that $d \in \operatorname{dom} f'$ holds $f'(d) = f(d) \cdot x^{d -' 1}$ and $(\mathcal{P}_{\mathbb{Z}}(f))(x) = \sum f'$.

Let f be a finite sequence of elements of $\mathbb{Z}$ and let x be an integer. Observe that $(\mathcal{P}_{\mathbb{Z}}(f))(x)$ is integer.

We now state two propositions:

(3) If $\operatorname{len} f = 1$, then $\mathcal{P}_{\mathbb{Z}}(f) = \mathbb{Z} \longmapsto f(1)$.

(4) If $\operatorname{len} f = 1$, then for every element x of $\mathbb{Z}$ holds $(\mathcal{P}_{\mathbb{Z}}(f))(x) = f(1)$.

In the sequel f' denotes a finite sequence of elements of $\mathbb{R}$.

Next we state three propositions:

(5) Let given g, g_1, g_2. Suppose $\operatorname{len} g = n+1$ and $\operatorname{len} g_1 = \operatorname{len} g$ and $\operatorname{len} g_2 = \operatorname{len} g$ and for every d such that $d \in \operatorname{dom} g$ holds $g(d) = g_1(d) - g_2(d)$. Then there exists f' such that $\operatorname{len} f' = \operatorname{len} g - 1$ and for every d such that $d \in \operatorname{dom} f'$ holds $f'(d) = g_1(d) - g_2(d+1)$ and $\sum g = ((\sum f') + g_1(n+1)) - g_2(1)$.

(6) Suppose $\operatorname{len} f = n + 2$. Let a be an integer. Then there exists a finite sequence f' of elements of $\mathbb{Z}$ and there exists an integer r such that $\operatorname{len} f' = n+1$ and for every element x of $\mathbb{Z}$ holds $(\mathcal{P}_{\mathbb{Z}}(f))(x) = (x-a) \cdot (\mathcal{P}_{\mathbb{Z}}(f'))(x) + r$ and $f(n+2) = f'(n+1)$.

(7) If $p \mid i \cdot j$, then $p \mid i$ or $p \mid j$.

In the sequel f', g are finite sequences of elements of $\mathbb{Z}$.

The following proposition is true

(8) Let given f. Suppose $\operatorname{len} f = n+1$ and $p > 2$ and $p \nmid f(n+1)$. Let given f'. Suppose for every d such that $d \in \operatorname{dom} f'$ holds $(\mathcal{P}_{\mathbb{Z}}(f))(f'(d)) \bmod p = 0$ and for all d, e such that d, $e \in \operatorname{dom} f'$ and $d \neq e$ holds $f'(d) \not\equiv f'(e) \pmod{p}$. Then $\operatorname{len} f' \leq n$.

Let a be an integer and let m be a natural number. We say that a is quadratic residue mod m if and only if:

(Def. 2) There exists an integer x such that $(x^{\mathbf{2}} - a) \bmod m = 0$.

In the sequel b, m denote natural numbers.

We now state four propositions:

(9) If $a \gcd m = 1$, then $a^{\mathbf{2}}$ is quadratic residue mod m.

(10) 1 is quadratic residue mod 2.

(11) If $i \gcd m = 1$ and i is quadratic residue mod m and $i \equiv j \pmod{m}$, then j is quadratic residue mod m.

(12) If $i \mid j$, then $i \gcd j = |i|$.

Let k be an integer and let a be a natural number. One can verify that k^a is integer.

One can prove the following propositions:

(13) For all integers i, j, m such that $i \bmod m = j \bmod m$ holds $i^n \bmod m = j^n \bmod m$.

(14) If $a \gcd p = 1$ and $(x^{\mathbf{2}} - a) \bmod p = 0$, then x and p are relative prime.

(15) Suppose $p > 2$ and $a \gcd p = 1$ and a is quadratic residue mod p. Then there exist integers x, y such that $(x^{\mathbf{2}} - a) \bmod p = 0$ and $(y^{\mathbf{2}} - a) \bmod p = 0$ and $x \not\equiv y \pmod{p}$.

Let f be a finite sequence of elements of $\mathbb{N}$ and let us consider d. One can check that $f(d)$ is natural.

The following propositions are true:

(16) Suppose $p > 2$. Then there exists a finite sequence f of elements of $\mathbb{N}$ such that

(i) $\operatorname{len} f = (p -' 1) \div 2$,

(ii) for every d such that $d \in \operatorname{dom} f$ holds $\gcd(f(d), p) = 1$,

(iii) for every d such that $d \in \operatorname{dom} f$ holds $f(d)$ is quadratic residue mod p, and

(iv) for all d, e such that $d, e \in \operatorname{dom} f$ and $d \neq e$ holds $f(d) \not\equiv f(e) \pmod{p}$.

(17) If $p > 2$ and $a \gcd p = 1$ and a is quadratic residue mod p, then $a^{(p -' 1) \div 2} \bmod p = 1$.

(18) If $p > 2$ and $b \gcd p = 1$ and b is not quadratic residue mod p, then $b^{(p -' 1) \div 2} \bmod p = p - 1$.

(19) If $p > 2$ and $a \gcd p = 1$ and a is not quadratic residue mod p, then $a^{(p -' 1) \div 2} \bmod p = p - 1$.

(20) If $p > 2$ and $a \gcd p = 1$ and a is quadratic residue mod p, then $(a^{(p -' 1) \div 2} - 1) \bmod p = 0$.

(21) If $p > 2$ and $a \gcd p = 1$ and a is not quadratic residue mod p, then $(a^{(p -' 1) \div 2} + 1) \bmod p = 0$.

In the sequel b is an integer.

We now state three propositions:

(22) Suppose $p > 2$ and $a \gcd p = 1$ and $b \gcd p = 1$ and a is quadratic residue mod p and b is quadratic residue mod p. Then $a \cdot b$ is quadratic residue mod p.

(23) Suppose $p > 2$ and $a \gcd p = 1$ and $b \gcd p = 1$ and a is quadratic residue mod p and b is not quadratic residue mod p. Then $a \cdot b$ is not quadratic residue mod p.

(24) Suppose $p > 2$ and $a \gcd p = 1$ and $b \gcd p = 1$ and a is not quadratic residue mod p and b is not quadratic residue mod p. Then $a \cdot b$ is quadratic residue mod p.

Let a be an integer and let p be a prime number. The functor $\left(\frac{a}{p}\right)$ yielding an integer is defined by:

(Def. 3) $\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is quadratic residue mod } p, \\ -1, & \text{otherwise.} \end{cases}$

One can prove the following propositions:

(25) $\left(\frac{a}{p}\right) = 1$ or $\left(\frac{a}{p}\right) = -1$.

(26) If $a \gcd p = 1$, then $\left(\frac{a^{\mathbf{2}}}{p}\right) = 1$.

(27) $\left(\frac{1}{p}\right) = 1$.

(28) If $p > 2$ and $a \gcd p = 1$, then $\left(\frac{a}{p}\right) \equiv a^{(p-'1)\div 2} \pmod{p}$.

(29) If $p > 2$ and $a \gcd p = 1$ and $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(30) If $p > 2$ and $a \gcd p = 1$ and $b \gcd p = 1$, then $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

(31) If for every d such that $d \in \operatorname{dom} f'$ holds $f'(d) = 1$ or $f'(d) = -1$, then $\prod f' = 1$ or $\prod f' = -1$.

In the sequel m denotes an integer.

One can prove the following propositions:

(32) For all g, f' such that $\operatorname{len} g = \operatorname{len} f'$ and for every d such that $d \in \operatorname{dom} g$ holds $g(d) \equiv f'(d) \pmod{m}$ holds $\prod g \equiv \prod f' \pmod{m}$.

(33) For all g, f' such that $\operatorname{len} g = \operatorname{len} f'$ and for every d such that $d \in \operatorname{dom} g$ holds $g(d) \equiv -f'(d) \pmod{m}$ holds $\prod g \equiv (-1)^{\operatorname{len} g} \cdot \prod f' \pmod{m}$.

In the sequel f denotes a finite sequence of elements of $\mathbb{N}$.

Next we state several propositions:

(34) Suppose $p > 2$ and for every d such that $d \in \operatorname{dom} f$ holds $\gcd(f(d), p) = 1$. Then there exists a finite sequence f' of elements of $\mathbb{Z}$ such that $\operatorname{len} f' = \operatorname{len} f$ and for every d such that $d \in \operatorname{dom} f'$ holds $f'(d) = \left(\frac{f(d)}{p}\right)$ and $\left(\frac{\prod f}{p}\right) = \prod f'$.

(35) If $p > 2$ and $\gcd(d, p) = 1$ and $\gcd(e, p) = 1$, then $\left(\frac{d^{\mathbf{2}} \cdot e}{p}\right) = \left(\frac{e}{p}\right)$.

(36) If $p > 2$, then $\left(\frac{-1}{p}\right) = (-1)^{(p-'1)\div 2}$.

(37) If $p > 2$ and $p \bmod 4 = 1$, then -1 is quadratic residue mod p.

(38) If $p > 2$ and $p \bmod 4 = 3$, then -1 is not quadratic residue mod p.

(39) Let D be a non empty set, g be a finite sequence of elements of D, and i, j be natural numbers. Then g is one-to-one if and only if $\operatorname{Swap}(g, i, j)$ is one-to-one.

(40) Let g be a finite sequence of elements of $\mathbb{N}$. Suppose $\operatorname{len} g = n$ and for every d such that $d \in \operatorname{dom} g$ holds $g(d) > 0$ and $g(d) \leq n$ and g is one-to-one. Then $\operatorname{rng} g = \operatorname{Seg} n$.

In the sequel a, m are natural numbers.

Next we state several propositions:

(41) Let g be a finite sequence of elements of $\mathbb{N}$. Suppose $p > 2$ and $\gcd(a,p) = 1$ and $g = a \cdot \mathrm{idseq}((p -' 1) \div 2)$ and $m = \overline{\overline{\{k \in \mathbb{N}: k \in \mathrm{rng}(g \bmod p) \wedge k > \frac{p}{2}\}}}$. Then $\left(\frac{a}{p}\right) = (-1)^m$.

(42) If $p > 2$, then $\left(\frac{2}{p}\right) = (-1)^{(p^2 -' 1) \div 8}$.

(43) If $p > 2$ and if $p \bmod 8 = 1$ or $p \bmod 8 = 7$, then 2 is quadratic residue mod p.

(44) If $p > 2$ and if $p \bmod 8 = 3$ or $p \bmod 8 = 5$, then 2 is not quadratic residue mod p.

(45) For all natural numbers a, b such that $a \bmod 2 = b \bmod 2$ holds $(-1)^a = (-1)^b$.

In the sequel g, g, h, k denote finite sequences of elements of $\mathbb{R}$.

Next we state two propositions:

(46) If $\mathrm{len}\, g = \mathrm{len}\, h$ and $\mathrm{len}\, g = \mathrm{len}\, k$, then $g \frown g - h \frown k = (g - h) \frown (g - k)$.

(47) For every finite sequence g of elements of $\mathbb{R}$ and for every real number m holds $\sum(\mathrm{len}\, g \mapsto m - g) = \mathrm{len}\, g \cdot m - \sum g$.

In the sequel X denotes a finite set and F denotes a finite sequence of elements of 2^X.

Let us consider X, F. Then $\overline{\overline{F}}$ is a cardinal yielding finite sequence of elements of $\mathbb{N}$.

The following proposition is true

(48) Let g be a finite sequence of elements of 2^X. Suppose $\mathrm{len}\, g = n$ and for all d, e such that d, $e \in \mathrm{dom}\, g$ and $d \neq e$ holds $g(d)$ misses $g(e)$. Then $\overline{\overline{\bigcup \mathrm{rng}\, g}} = \sum \overline{\overline{g}}$.

In the sequel q is a prime number.

The following three propositions are true:

(49) If $p > 2$ and $q > 2$ and $p \neq q$, then $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{((p -' 1) \div 2) \cdot ((q -' 1) \div 2)}$.

(50) If $p > 2$ and $q > 2$ and $p \neq q$ and $p \bmod 4 = 3$ and $q \bmod 4 = 3$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

(51) If $p > 2$ and $q > 2$ and $p \neq q$ and $p \bmod 4 = 1$ or $q \bmod 4 = 1$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

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. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

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

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

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

[7] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 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] Zhang Dexin. *Integer Theory.* Science Publication, China, 1965.
[13] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.
[14] Hua Loo Keng. *Introduction to Number Theory.* Beijing Science Publication, China, 1957.
[15] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.
[16] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[17] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[18] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[19] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.
[20] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[22] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[23] Bo Zhang, Hiroshi Yamazaki, and Yatsuka Nakamura. Set sequences and monotone class. *Formalized Mathematics*, 13(**4**):435–441, 2005.

Received October 9, 2007

FORMALIZED MATHEMATICS
Vol. **16**, No. **1**, Pages 29–33, **2008**

Regular Expression Quantifiers – at least m Occurrences

Michał Trybulec
Motorola Software Group
Cracow, Poland

Summary. This is the second article on regular expression quantifiers. [4] introduced the quantifiers m to n occurrences and optional occurrence. In the sequel, the quantifiers: at least m occurrences and positive closure (at least 1 occurrence) are introduced. Notation and terminology were taken from [8], several properties of regular expressions from [7].

MML identifier: `FLANG_3`, version: `7.8.05 4.89.993`

The notation and terminology used here are introduced in the following papers: [5], [1], [6], [2], [3], and [4].

1. Preliminaries

For simplicity, we follow the rules: E, x denote sets, A, B, C denote subsets of E^{ω}, a, b denote elements of E^{ω}, and k, l, m, n denote natural numbers.

The following proposition is true

(1) If $B \subseteq A^*$, then $(A^*) \frown B \subseteq A^*$ and $B \frown A^* \subseteq A^*$.

2. At least m Occurrences

Let us consider E, A, n. The functor $A^{n,\cdots}$ yielding a subset of E^{ω} is defined as follows:

(Def. 1) $A^{n,\cdots} = \bigcup \{B : \bigvee_m \, (n \leq m \ \wedge \ B = A^m)\}$.

We now state a number of propositions:

ISSN 1426–2630(p), 1898-9934(e)

(2) $x \in A^{n,\cdots}$ iff there exists m such that $n \leq m$ and $x \in A^m$.
(3) If $n \leq m$, then $A^m \subseteq A^{n,\cdots}$.
(4) $A^{n,\cdots} = \emptyset$ iff $n > 0$ and $A = \emptyset$.
(5) If $m \leq n$, then $A^{n,\cdots} \subseteq A^{m,\cdots}$.
(6) If $k \leq m$, then $A^{m,n} \subseteq A^{k,\cdots}$.
(7) If $m \leq n+1$, then $A^{m,n} \cup (A^{(n+1),\cdots}) = A^{m,\cdots}$.
(8) $A^n \cup (A^{(n+1),\cdots}) = A^{n,\cdots}$.
(9) $A^{n,\cdots} \subseteq A^*$.
(10) $\langle\rangle_E \in A^{n,\cdots}$ iff $n = 0$ or $\langle\rangle_E \in A$.
(11) $A^{n,\cdots} = A^*$ iff $\langle\rangle_E \in A$ or $n = 0$.
(12) $A^* = A^{0,n} \cup (A^{(n+1),\cdots})$.
(13) If $A \subseteq B$, then $A^{n,\cdots} \subseteq B^{n,\cdots}$.
(14) If $x \in A$ and $x \neq \langle\rangle_E$, then $A^{n,\cdots} \neq \{\langle\rangle_E\}$.
(15) $A^{n,\cdots} = \{\langle\rangle_E\}$ iff $A = \{\langle\rangle_E\}$ or $n = 0$ and $A = \emptyset$.
(16) $A^{(n+1),\cdots} = (A^{n,\cdots}) \frown A$.
(17) $(A^{m,\cdots}) \frown A^* = A^{m,\cdots}$.
(18) $(A^{m,\cdots}) \frown (A^{n,\cdots}) = A^{(m+n),\cdots}$.
(19) If $n > 0$, then $(A^{m,\cdots})^n = A^{m \cdot n,\cdots}$.
(20) $(A^{n,\cdots})^* = (A^{n,\cdots})?$.
(21) If $A \subseteq C^{m,\cdots}$ and $B \subseteq C^{n,\cdots}$, then $A \frown B \subseteq C^{(m+n),\cdots}$.
(22) $A^{(n+k),\cdots} = (A^{n,\cdots}) \frown A^k$.
(23) $A \frown (A^{n,\cdots}) = (A^{n,\cdots}) \frown A$.
(24) $(A^k) \frown (A^{n,\cdots}) = (A^{n,\cdots}) \frown A^k$.
(25) $(A^{k,l}) \frown (A^{n,\cdots}) = (A^{n,\cdots}) \frown A^{k,l}$.
(26) If $\langle\rangle_E \in B$, then $A \subseteq A \frown (B^{n,\cdots})$ and $A \subseteq (B^{n,\cdots}) \frown A$.
(27) $(A^{m,\cdots}) \frown (A^{n,\cdots}) = (A^{n,\cdots}) \frown (A^{m,\cdots})$.
(28) If $A \subseteq B^{k,\cdots}$ and $n > 0$, then $A^n \subseteq B^{k,\cdots}$.
(29) If $A \subseteq B^{k,\cdots}$ and $n > 0$, then $A^{n,\cdots} \subseteq B^{k,\cdots}$.
(30) $(A^*) \frown A = A^{1,\cdots}$.
(31) $(A^*) \frown A^k = A^{k,\cdots}$.
(32) $(A^{m,\cdots}) \frown A^* = (A^*) \frown (A^{m,\cdots})$.
(33) If $k \leq l$, then $(A^{n,\cdots}) \frown A^{k,l} = A^{(n+k),\cdots}$.
(34) If $k \leq l$, then $(A^*) \frown A^{k,l} = A^{k,\cdots}$.
(35) $A^{mn,\cdots} \subseteq A^{m \cdot n,\cdots}$.
(36) $A^{mn,\cdots} \subseteq (A^{n,\cdots})^m$.
(37) If $a \in C^{m,\cdots}$ and $b \in C^{n,\cdots}$, then $a \frown b \in C^{(m+n),\cdots}$.
(38) If $A^{k,\cdots} = \{x\}$, then $x = \langle\rangle_E$.

(39) If $A \subseteq B^*$, then $A^{n,\cdots} \subseteq B^*$.

(40) $A? \subseteq A^{k,\cdots}$ iff $k = 0$ or $\langle\rangle_E \in A$.

(41) $(A^{k,\cdots}) \frown A? = A^{k,\cdots}$.

(42) $(A^{k,\cdots}) \frown A? = A? \frown (A^{k,\cdots})$.

(43) If $B \subseteq A^*$, then $(A^{k,\cdots}) \frown B \subseteq A^{k,\cdots}$ and $B \frown (A^{k,\cdots}) \subseteq A^{k,\cdots}$.

(44) $A \cap B^{k,\cdots} \subseteq (A^{k,\cdots}) \cap (B^{k,\cdots})$.

(45) $(A^{k,\cdots}) \cup (B^{k,\cdots}) \subseteq (A \cup B)^{k,\cdots}$.

(46) $\langle x \rangle \in A^{k,\cdots}$ iff $\langle x \rangle \in A$ but $\langle\rangle_E \in A$ or $k \leq 1$.

(47) If $A \subseteq B^{k,\cdots}$, then $B^{k,\cdots} = (B \cup A)^{k,\cdots}$.

3. Positive Closure

Let us consider E, A. The functor A^+ yielding a subset of E^ω is defined as follows:

(Def. 2) $A^+ = \bigcup\{B : \bigvee_n \ (n > 0 \ \wedge \ B = A^n)\}$.

Next we state a number of propositions:

(48) $x \in A^+$ iff there exists n such that $n > 0$ and $x \in A^n$.

(49) If $n > 0$, then $A^n \subseteq A^+$.

(50) $A^+ = A^{1,\cdots}$.

(51) $A^+ = \emptyset$ iff $A = \emptyset$.

(52) $A^+ = (A^*) \frown A$.

(53) $A^* = \{\langle\rangle_E\} \cup A^+$.

(54) $A^+ = A^{1,n} \cup (A^{(n+1),\cdots})$.

(55) $A^+ \subseteq A^*$.

(56) $\langle\rangle_E \in A^+$ iff $\langle\rangle_E \in A$.

(57) $A^+ = A^*$ iff $\langle\rangle_E \in A$.

(58) If $A \subseteq B$, then $A^+ \subseteq B^+$.

(59) $A \subseteq A^+$.

(60) $A^{*+} = A^*$ and $A^{+*} = A^*$.

(61) If $A \subseteq B^*$, then $A^+ \subseteq B^*$.

(62) $A^{++} = A^+$.

(63) If $x \in A$ and $x \neq \langle\rangle_E$, then $A^+ \neq \{\langle\rangle_E\}$.

(64) $A^+ = \{\langle\rangle_E\}$ iff $A = \{\langle\rangle_E\}$.

(65) $A^+? = A^*$ and $A?^+ = A^*$.

(66) If a, $b \in C^+$, then $a \frown b \in C^+$.

(67) If $A \subseteq C^+$ and $B \subseteq C^+$, then $A \frown B \subseteq C^+$.

(68) $A \frown A \subseteq A^+$.

(69) If $A^{+} = \{x\}$, then $x = \langle\rangle_E$.
(70) $A \frown A^{+} = A^{+} \frown A$.
(71) $(A^{k}) \frown A^{+} = A^{+} \frown A^{k}$.
(72) $(A^{m,n}) \frown A^{+} = A^{+} \frown A^{m,n}$.
(73) If $\langle\rangle_E \in B$, then $A \subseteq A \frown B^{+}$ and $A \subseteq B^{+} \frown A$.
(74) $A^{+} \frown A^{+} = A^{2,\cdots}$.
(75) $A^{+} \frown A^{k} = A^{(k+1),\cdots}$.
(76) $A^{+} \frown A = A^{2,\cdots}$.
(77) If $k \leq l$, then $A^{+} \frown A^{k,l} = A^{(k+1),\cdots}$.
(78) If $A \subseteq B^{+}$ and $n > 0$, then $A^{n} \subseteq B^{+}$.
(79) $A^{+} \frown A? = A? \frown A^{+}$.
(80) $A^{+} \frown A? = A^{+}$.
(81) $A? \subseteq A^{+}$ iff $\langle\rangle_E \in A$.
(82) If $A \subseteq B^{+}$, then $A^{+} \subseteq B^{+}$.
(83) If $A \subseteq B^{+}$, then $B^{+} = (B \cup A)^{+}$.
(84) If $n > 0$, then $A^{n,\cdots} \subseteq A^{+}$.
(85) If $m > 0$, then $A^{m,n} \subseteq A^{+}$.
(86) $(A^{*}) \frown A^{+} = A^{+} \frown A^{*}$.
(87) ${A^{+}}^{k} \subseteq A^{k,\cdots}$.
(88) ${A^{+}}^{m,n} \subseteq A^{m,\cdots}$.
(89) If $A \subseteq B^{+}$ and $n > 0$, then $A^{n,\cdots} \subseteq B^{+}$.
(90) $A^{+} \frown (A^{k,\cdots}) = A^{(k+1),\cdots}$.
(91) $A^{+} \frown (A^{k,\cdots}) = (A^{k,\cdots}) \frown A^{+}$.
(92) $A^{+} \frown A^{*} = A^{+}$.
(93) If $B \subseteq A^{*}$, then $A^{+} \frown B \subseteq A^{+}$ and $B \frown A^{+} \subseteq A^{+}$.
(94) $(A \cap B)^{+} \subseteq A^{+} \cap B^{+}$.
(95) $A^{+} \cup B^{+} \subseteq (A \cup B)^{+}$.
(96) $\langle x\rangle \in A^{+}$ iff $\langle x\rangle \in A$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Karol Pąk. The Catalan numbers. Part II. *Formalized Mathematics*, 14(**4**):153–159, 2006.
[3] Michał Trybulec. Formal languages – concatenation and closure. *Formalized Mathematics*, 15(**1**):11–15, 2007.
[4] Michał Trybulec. Regular expression quantifiers – m to n occurrences. *Formalized Mathematics*, 15(**2**):53–58, 2007.
[5] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[6] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.

[7] William M. Waite and Gerhard Goos. *Compiler Construction.* Springer-Verlag New York Inc., 1984.
[8] Larry Wall, Tom Christiansen, and Jon Orwant. *Programming Perl, Third Edition.* O'Reilly Media, 2000.

Received October 9, 2007

FORMALIZED MATHEMATICS
Vol. 16, No. 1, Pages 35–43, 2008

Complete Spaces

Karol Pąk
Institute of Computer Science
University of Białystok
Poland

Summary. This paper is a continuation of [12]. First some definitions needed to formulate Cantor's theorem on complete spaces and show several facts about them are introduced. Next section contains the proof of Cantor's theorem and some properties of complete spaces resulting from this theorem. Moreover, countable compact spaces and proofs of auxiliary facts about them is defined. I also show the important condition that every metric space is compact if and only if it is countably compact. Then I prove that every metric space is compact if and only if it is a complete and totally bounded space. I also introduce the definition of the metric space with the well metric. This article is based on [13].

MML identifier: `COMPL_SP`, version: `7.8.05 4.89.993`

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

1. Preliminaries

We follow the rules: i, n, m denote natural numbers, x, X, Y denote sets, and r denotes a real number.

Let M be a non empty metric structure and let S be a sequence of subsets of M. We say that S is bounded if and only if:

(Def. 1) For every i holds $S(i)$ is bounded.

Let M be a non empty reflexive metric structure. Observe that there exists a sequence of subsets of M which is bounded and non-empty.

Let M be a reflexive non empty metric structure and let S be a sequence of subsets of M. The functor $\varnothing S$ yielding a sequence of real numbers is defined by:

ISSN 1426–2630(p), 1898-9934(e)

(Def. 2) For every i holds $(\varnothing S)(i) = \varnothing S(i)$.

We now state several propositions:

(1) Let M be a reflexive non empty metric structure and S be a bounded sequence of subsets of M. Then $\varnothing S$ is lower bounded.

(2) Let M be a reflexive non empty metric structure and S be a bounded sequence of subsets of M. If S is descending, then $\varnothing S$ is upper bounded and $\varnothing S$ is non-increasing.

(3) Let M be a reflexive non empty metric structure and S be a bounded sequence of subsets of M. If S is ascending, then $\varnothing S$ is non-decreasing.

(4) Let M be a non empty reflexive metric structure and S be a bounded sequence of subsets of M. Suppose S is descending and $\lim \varnothing S = 0$. Let F be a sequence of M. If for every i holds $F(i) \in S(i)$, then F is Cauchy.

(5) Let M be a reflexive symmetric triangle non empty metric structure and p be a point of M. If $0 \leq r$, then $\varnothing \overline{\mathrm{Ball}}(p, r) \leq 2 \cdot r$.

Let M be a metric structure and let U be a subset of M. We say that U is open if and only if:

(Def. 3) $U \in$ the open set family of M.

Let M be a metric structure and let A be a subset of M. We say that A is closed if and only if:

(Def. 4) A^{c} is open.

Let M be a metric structure. Note that there exists a subset of M which is open and empty and there exists a subset of M which is closed and empty.

Let M be a non empty metric structure. One can verify that there exists a subset of M which is open and non empty and there exists a subset of M which is closed and non empty.

One can prove the following proposition

(6) Let M be a metric structure, A be a subset of M, and A' be a subset of M_{top} such that $A' = A$. Then

(i) A is open iff A' is open, and

(ii) A is closed iff A' is closed.

Let T be a topological structure and let S be a sequence of subsets of T. We say that S is open if and only if:

(Def. 5) For every i holds $S(i)$ is open.

We say that S is closed if and only if:

(Def. 6) For every i holds $S(i)$ is closed.

Let T be a topological space. Observe that there exists a sequence of subsets of T which is open and there exists a sequence of subsets of T which is closed.

Let T be a non empty topological space. One can verify that there exists a sequence of subsets of T which is open and non-empty and there exists a sequence of subsets of T which is closed and non-empty.

Let M be a metric structure and let S be a sequence of subsets of M. We say that S is open if and only if:

(Def. 7) For every i holds $S(i)$ is open.

We say that S is closed if and only if:

(Def. 8) For every i holds $S(i)$ is closed.

Let M be a non empty metric space. Note that there exists a sequence of subsets of M which is non-empty, bounded, and open and there exists a sequence of subsets of M which is non-empty, bounded, and closed.

The following propositions are true:

(7) Let M be a metric structure, S be a sequence of subsets of M, and S' be a sequence of subsets of M_{top} such that $S' = S$. Then

(i) S is open iff S' is open, and

(ii) S is closed iff S' is closed.

(8) Let M be a reflexive symmetric triangle non empty metric structure and S, C_1 be subsets of M. Suppose S is bounded. Let S' be a subset of M_{top}. If $S = S'$ and $C_1 = \overline{S'}$, then C_1 is bounded and $\varnothing S = \varnothing C_1$.

2. Cantor's Theorem on Complete Spaces

The following propositions are true:

(9) Let M be a non empty metric space and C be a sequence of M. Then there exists a non-empty closed sequence S of subsets of M such that

(i) S is descending,

(ii) if C is Cauchy, then S is bounded and $\lim \varnothing S = 0$, and

(iii) for every i there exists a subset U of M_{top} such that $U = \{C(j); j$ ranges over elements of $\mathbb{N}$: $j \geq i\}$ and $S(i) = \overline{U}$.

(10) Let M be a non empty metric space. Then M is complete if and only if for every non-empty bounded closed sequence S of subsets of M such that S is descending and $\lim \varnothing S = 0$ holds $\bigcap S$ is non empty.

(11) Let T be a non empty topological space and S be a non-empty sequence of subsets of T. Suppose S is descending. Let F be a family of subsets of T. If $F = \operatorname{rng} S$, then F is centered.

(12) Let M be a non empty metric structure, S be a sequence of subsets of M, and F be a family of subsets of M_{top} such that $F = \operatorname{rng} S$. Then

(i) if S is open, then F is open, and

(ii) if S is closed, then F is closed.

(13) Let T be a non empty topological space, F be a family of subsets of T, and S be a sequence of subsets of T. Suppose $\operatorname{rng} S \subseteq F$. Then there exists a sequence R of subsets of T such that

(i) R is descending,
(ii) if F is centered, then R is non-empty,
(iii) if F is open, then R is open,
(iv) if F is closed, then R is closed, and
(v) for every i holds $R(i) = \bigcap\{S(j); j$ ranges over elements of $\mathbb{N}$: $j \leq i\}$.

(14) Let M be a non empty metric space. Then M is complete if and only if for every family F of subsets of $M_{\rm top}$ such that F is closed and centered and for every real number r such that $r > 0$ there exists a subset A of M such that $A \in F$ and A is bounded and $\varnothing A < r$ holds $\bigcap F$ is non empty.

(15) Let M be a non empty metric space, A be a non empty subset of M, B be a subset of M, and B' be a subset of $M\restriction A$. If $B = B'$, then B' is bounded iff B is bounded.

(16) Let M be a non empty metric space, A be a non empty subset of M, B be a subset of M, and B' be a subset of $M\restriction A$. If $B = B'$ and B is bounded, then $\varnothing B' \leq \varnothing B$.

(17) For every non empty metric space M and for every non empty subset A of M holds every sequence of $M\restriction A$ is a sequence of M.

(18) Let M be a non empty metric space, A be a non empty subset of M, S be a sequence of $M\restriction A$, and S' be a sequence of M. If $S = S'$, then S' is Cauchy iff S is Cauchy.

(19) Let M be a non empty metric space. Suppose M is complete. Let A be a non empty subset of M and A' be a subset of $M_{\rm top}$. If $A = A'$, then $M\restriction A$ is complete iff A' is closed.

3. Countable Compact Spaces

Let T be a topological structure. We say that T is countably-compact if and only if the condition (Def. 9) is satisfied.

(Def. 9) Let F be a family of subsets of T. Suppose F is a cover of T, open, and countable. Then there exists a family G of subsets of T such that $G \subseteq F$ and G is a cover of T and finite.

We now state a number of propositions:

(20) For every topological structure T such that T is compact holds T is countably-compact.

(21) Let T be a non empty topological space. Then T is countably-compact if and only if for every family F of subsets of T such that F is centered, closed, and countable holds $\bigcap F \neq \emptyset$.

(22) Let T be a non empty topological space. Then T is countably-compact if and only if for every non-empty closed sequence S of subsets of T such that S is descending holds $\bigcap S \neq \emptyset$.

(23) Let T be a non empty topological space, F be a family of subsets of T, and S be a sequence of subsets of T. Suppose $\operatorname{rng} S \subseteq F$ and S is non-empty. Then there exists a non-empty closed sequence R of subsets of T such that

(i) R is descending,

(ii) if F is locally finite and S is one-to-one, then $\bigcap R = \emptyset$, and

(iii) for every i there exists a family S_1 of subsets of T such that $R(i) = \overline{\bigcup S_1}$ and $S_1 = \{S(j); j$ ranges over elements of $\mathbb{N}$: $j \geq i\}$.

(24) For every function F such that $\operatorname{dom} F$ is infinite and $\operatorname{rng} F$ is finite there exists x such that $x \in \operatorname{rng} F$ and $F^{-1}(\{x\})$ is infinite.

(25) Let X be a non empty set and F be a sequence of subsets of X. Suppose F is descending. Let S be a function from $\mathbb{N}$ into X. If for every n holds $S(n) \in F(n)$, then if $\operatorname{rng} S$ is finite, then $\bigcap F$ is non empty.

(26) Let T be a non empty topological space. Then T is countably-compact if and only if for every family F of subsets of T such that F is locally finite and has non empty elements holds F is finite.

(27) Let T be a non empty topological space. Then T is countably-compact if and only if for every family F of subsets of T such that F is locally finite and for every subset A of T such that $A \in F$ holds $\overline{\overline{A}} = 1$ holds F is finite.

(28) Let T be a T_1 non empty topological space. Then T is countably-compact if and only if for every subset A of T such that A is infinite holds $\operatorname{Der} A$ is non empty.

(29) Let T be a T_1 non empty topological space. Then T is countably-compact if and only if for every subset A of T such that A is infinite and countable holds $\operatorname{Der} A$ is non empty.

The scheme *Th39* deals with a non empty set $\mathcal{A}$ and a binary predicate $\mathcal{P}$, and states that:

There exists a subset A of $\mathcal{A}$ such that

(i) for all elements x, y of $\mathcal{A}$ such that x, $y \in A$ and $x \neq y$ holds $\mathcal{P}[x, y]$, and

(ii) for every element x of $\mathcal{A}$ there exists an element y of $\mathcal{A}$ such that $y \in A$ and not $\mathcal{P}[x, y]$

provided the following conditions are satisfied:

- For all elements x, y of $\mathcal{A}$ holds $\mathcal{P}[x, y]$ iff $\mathcal{P}[y, x]$, and
- For every element x of $\mathcal{A}$ holds not $\mathcal{P}[x, x]$.

We now state several propositions:

(30) Let M be a reflexive symmetric non empty metric structure and r be a real number. Suppose $r > 0$. Then there exists a subset A of M such that

(i) for all points p, q of M such that $p \neq q$ and p, $q \in A$ holds $\rho(p, q) \geq r$, and

(ii) for every point p of M there exists a point q of M such that $q \in A$ and $p \in \mathrm{Ball}(q, r)$.

(31) Let M be a reflexive symmetric triangle non empty metric structure. Then M is totally bounded if and only if for every real number r and for every subset A of M such that $r > 0$ and for all points p, q of M such that $p \neq q$ and $p, q \in A$ holds $\rho(p, q) \geq r$ holds A is finite.

(32) Let M be a reflexive symmetric triangle non empty metric structure. If M_{top} is countably-compact, then M is totally bounded.

(33) For every non empty metric space M such that M is totally bounded holds M_{top} is second-countable.

(34) Let T be a non empty topological space. Suppose T is second-countable. Let F be a family of subsets of T. Suppose F is a cover of T and open. Then there exists a family G of subsets of T such that $G \subseteq F$ and G is a cover of T and countable.

4. The Main Theorem

The following three propositions are true:

(35) For every non empty metric space M holds M_{top} is compact iff M_{top} is countably-compact.

(36) Let X be a set and F be a family of subsets of X. Suppose F is finite. Let A be a subset of X. Suppose A is infinite and $A \subseteq \bigcup F$. Then there exists a subset Y of X such that $Y \in F$ and $Y \cap A$ is infinite.

(37) For every non empty metric space M holds M_{top} is compact iff M is totally bounded and complete.

5. Well Spaces

Let T be a set, let S be a function from $\mathbb{N}$ into T, and let i be a natural number. Then $S(i)$ is an element of T.

The following proposition is true

(38) Let M be a metric structure, a be a point of M, and given x. Then $x \in X \times ((\text{the carrier of } M) \setminus \{a\}) \cup \{\langle X, a\rangle\}$ if and only if there exists a set y and there exists a point b of M such that $x = \langle y, b\rangle$ but $y \in X$ and $b \neq a$ or $y = X$ and $b = a$.

Let M be a metric structure, let a be a point of M, and let X be a set. The functor well-dist(a, X) yields a function from $(X \times ((\text{the carrier of } M) \setminus \{a\}) \cup \{\langle X, a\rangle\}) \times (X \times ((\text{the carrier of } M) \setminus \{a\}) \cup \{\langle X, a\rangle\})$ into $\mathbb{R}$ and is defined by the condition (Def. 10).

(Def. 10) Let x, y be elements of $X \times ((\text{the carrier of } M) \setminus \{a\}) \cup \{\langle X, a\rangle\}$, x_1, y_1 be sets, and x_2, y_2 be points of M such that $x = \langle x_1, x_2\rangle$ and $y = \langle y_1, y_2\rangle$. Then

(i) if $x_1 = y_1$, then $(\text{well-dist}(a, X))(x, y) = \rho(x_2, y_2)$, and

(ii) if $x_1 \neq y_1$, then $(\text{well-dist}(a, X))(x, y) = \rho(x_2, a) + \rho(a, y_2)$.

We now state the proposition

(39) Let M be a metric structure, a be a point of M, and X be a non empty set. Then

(i) if well-dist(a, X) is reflexive, then M is reflexive,

(ii) if well-dist(a, X) is symmetric, then M is symmetric,

(iii) if well-dist(a, X) is triangle and reflexive, then M is triangle, and

(iv) if well-dist(a, X) is discernible and reflexive, then M is discernible.

Let M be a metric structure, let a be a point of M, and let X be a set. The functor WellSpace(a, X) yields a strict metric structure and is defined as follows:

(Def. 11) $\text{WellSpace}(a, X) = \langle X \times ((\text{the carrier of } M) \setminus \{a\}) \cup \{\langle X, a\rangle\}, \text{well-dist}(a, X)\rangle$.

Let M be a metric structure, let a be a point of M, and let X be a set. One can check that WellSpace(a, X) is non empty.

Let M be a reflexive metric structure, let a be a point of M, and let X be a set. Note that WellSpace(a, X) is reflexive.

Let M be a symmetric metric structure, let a be a point of M, and let X be a set. Observe that WellSpace(a, X) is symmetric.

Let M be a symmetric triangle reflexive metric structure, let a be a point of M, and let X be a set. One can verify that WellSpace(a, X) is triangle.

Let M be a metric space, let a be a point of M, and let X be a set. Observe that WellSpace(a, X) is discernible.

We now state several propositions:

(40) Let M be a triangle reflexive non empty metric structure, a be a point of M, and X be a non empty set. If WellSpace(a, X) is complete, then M is complete.

(41) Let M be a symmetric triangle reflexive non empty metric structure, a be a point of M, and S be a sequence of WellSpace(a, X). Suppose S is Cauchy. Then

(i) for every point X_1 of WellSpace(a, X) such that $X_1 = \langle X, a\rangle$ and for every r such that $r > 0$ there exists n such that for every m such that $m \geq n$ holds $\rho(S(m), X_1) < r$, or

(ii) there exist n, Y such that for every m such that $m \geq n$ there exists a point p of M such that $S(m) = \langle Y, p\rangle$.

(42) Let M be a symmetric triangle reflexive non empty metric structure and a be a point of M. If M is complete, then WellSpace(a, X) is complete.

(43) Let M be a symmetric triangle reflexive non empty metric structure. Suppose M is complete. Let a be a point of M. Given a point b of M such that $\rho(a, b) \neq 0$. Let X be an infinite set. Then

(i) WellSpace(a, X) is complete, and

(ii) there exists a non-empty bounded sequence S of subsets of WellSpace(a, X) such that S is closed and descending and $\bigcap S$ is empty.

(44) There exists a non empty metric space M such that

(i) M is complete, and

(ii) there exists a non-empty bounded sequence S of subsets of M such that S is closed and descending and $\bigcap S$ is empty.

References

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

[2] Grzegorz Bancerek. Countable sets and Hessenberg's theorem. *Formalized Mathematics*, 2(**1**):65–69, 1991.

[3] Józef Białas and Yatsuka Nakamura. Dyadic numbers and T_4 topological spaces. *Formalized Mathematics*, 5(**3**):361–366, 1996.

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

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

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

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

[8] Agata Darmochwał. Compact spaces. *Formalized Mathematics*, 1(**2**):383–386, 1990.

[9] Agata Darmochwał. Families of subsets, subspaces and mappings in topological spaces. *Formalized Mathematics*, 1(**2**):257–261, 1990.

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

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

[12] Alicia de la Cruz. Totally bounded metric spaces. *Formalized Mathematics*, 2(**4**):559–562, 1991.

[13] Ryszard Engelking. *General Topology*, volume 60 of *Monografie Matematyczne*. PWN – Polish Scientific Publishers, Warsaw, 1977.

[14] Adam Grabowski. On the Kuratowski limit operators. *Formalized Mathematics*, 11(**4**):399–409, 2003.

[15] Adam Grabowski. On the boundary and derivative of a set. *Formalized Mathematics*, 13(**1**):139–146, 2005.

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

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

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

[19] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.

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

[21] Robert Milewski. Bases of continuous lattices. *Formalized Mathematics*, 7(**2**):285–294, 1998.

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

[23] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[24] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[25] Michał Trybulec. Formal languages – concatenation and closure. *Formalized Mathematics*, 15(**1**):11–15, 2007.
[26] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[27] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[28] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[29] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Received October 12, 2007

FORMALIZED MATHEMATICS
Vol. 16, No. 1, Pages 45–49, 2008

Difference and Difference Quotient. Part II

Bo Li
Qingdao University of Science and Technology
China

Yanping Zhuang
Qingdao University of Science and Technology
China

Xiquan Liang
Qingdao University of Science and Technology
China

Summary. In this article, we give some important properties of forward difference, backward difference, central difference and difference quotient and forward difference, backward difference, central difference and difference quotient formulas of some special functions [11].

MML identifier: `DIFF_2`, version: `7.8.09 4.97.1001`

The articles [8], [1], [4], [2], [3], [5], [7], [12], [13], [6], [9], and [10] provide the notation and terminology for this paper.

We follow the rules: h, r, r_1, r_2, x_0, x_1, x_2, x_3, x_4, x_5, x, a, b, c, k denote real numbers and f, f_1, f_2 denote functions from $\mathbb{R}$ into $\mathbb{R}$.

Next we state a number of propositions:

(1)[1] $\Delta[f](x, x+h) = \frac{(\vec{\Delta}_h[f])(1)(x)}{h}$.

(2) If $h \neq 0$, then $\Delta[f](x, x+h, x+2 \cdot h) = \frac{(\vec{\Delta}_h[f])(2)(x)}{2 \cdot h^{\mathbf{2}}}$.

(3) $\Delta[f](x-h, x) = \frac{(\vec{\nabla}_h[f])(1)(x)}{h}$.

(4) If $h \neq 0$, then $\Delta[f](x - 2 \cdot h, x - h, x) = \frac{(\vec{\nabla}_h[f])(2)(x)}{2 \cdot h^{\mathbf{2}}}$.

(5) $\Delta[r\, f](x_0, x_1, x_2) = r \cdot \Delta[f](x_0, x_1, x_2)$.

(6) $\Delta[f_1 + f_2](x_0, x_1, x_2) = \Delta[f_1](x_0, x_1, x_2) + \Delta[f_2](x_0, x_1, x_2)$.

[1]The notation $\Delta(f, x, y)$ has been changed to $\Delta[f](x, y)$. More in Addenda.

ISSN 1426–2630(p), 1898-9934(e)

(7) $\Delta[r_1\, f_1 + r_2\, f_2](x_0, x_1, x_2) = r_1 \cdot \Delta[f_1](x_0, x_1, x_2) + r_2 \cdot \Delta[f_2](x_0, x_1, x_2)$.

(8) $\Delta[r\, f](x_0, x_1, x_2, x_3) = r \cdot \Delta[f](x_0, x_1, x_2, x_3)$.

(9) $\Delta[f_1 + f_2](x_0, x_1, x_2, x_3) = \Delta[f_1](x_0, x_1, x_2, x_3) + \Delta[f_2](x_0, x_1, x_2, x_3)$.

(10) $\Delta[r_1\, f_1 + r_2\, f_2](x_0, x_1, x_2, x_3) = r_1 \cdot \Delta[f_1](x_0, x_1, x_2, x_3) + r_2 \cdot \Delta[f_2](x_0, x_1, x_2, x_3)$.

Let f be a real-yielding function and let x_0, x_1, x_2, x_3, x_4 be real numbers. The functor $\Delta[f](x_0, x_1, x_2, x_3, x_4)$ yielding a real number is defined as follows:

(Def. 1) $\Delta[f](x_0, x_1, x_2, x_3, x_4) = \frac{\Delta[f](x_0,x_1,x_2,x_3) - \Delta[f](x_1,x_2,x_3,x_4)}{x_0 - x_4}$.

Next we state three propositions:

(11) $\Delta[r\, f](x_0, x_1, x_2, x_3, x_4) = r \cdot \Delta[f](x_0, x_1, x_2, x_3, x_4)$.

(12) $\Delta[f_1 + f_2](x_0, x_1, x_2, x_3, x_4) = \Delta[f_1](x_0, x_1, x_2, x_3, x_4) + \Delta[f_2](x_0, x_1, x_2, x_3, x_4)$.

(13) $\Delta[r_1\, f_1 + r_2\, f_2](x_0, x_1, x_2, x_3, x_4) = r_1 \cdot \Delta[f_1](x_0, x_1, x_2, x_3, x_4) + r_2 \cdot \Delta[f_2](x_0, x_1, x_2, x_3, x_4)$.

Let f be a real-yielding function and let x_0, x_1, x_2, x_3, x_4, x_5 be real numbers. The functor $\Delta[f](x_0, x_1, x_2, x_3, x_4, x_5)$ yields a real number and is defined as follows:

(Def. 2) $\Delta[f](x_0, x_1, x_2, x_3, x_4, x_5) = \frac{\Delta[f](x_0,x_1,x_2,x_3,x_4) - \Delta[f](x_1,x_2,x_3,x_4,x_5)}{x_0 - x_5}$.

We now state a number of propositions:

(14) $\Delta[r\, f](x_0, x_1, x_2, x_3, x_4, x_5) = r \cdot \Delta[f](x_0, x_1, x_2, x_3, x_4, x_5)$.

(15) $\Delta[f_1 + f_2](x_0, x_1, x_2, x_3, x_4, x_5) = \Delta[f_1](x_0, x_1, x_2, x_3, x_4, x_5) + \Delta[f_2](x_0, x_1, x_2, x_3, x_4, x_5)$.

(16) $\Delta[r_1\, f_1 + r_2\, f_2](x_0, x_1, x_2, x_3, x_4, x_5) = r_1 \cdot \Delta[f_1](x_0, x_1, x_2, x_3, x_4, x_5) + r_2 \cdot \Delta[f_2](x_0, x_1, x_2, x_3, x_4, x_5)$.

(17) If x_0, x_1, x_2 are mutually different, then $\Delta[f](x_0, x_1, x_2) = \frac{f(x_0)}{(x_0 - x_1) \cdot (x_0 - x_2)} + \frac{f(x_1)}{(x_1 - x_0) \cdot (x_1 - x_2)} + \frac{f(x_2)}{(x_2 - x_0) \cdot (x_2 - x_1)}$.

(18) If x_0, x_1, x_2, x_3 are mutually different, then $\Delta[f](x_0, x_1, x_2, x_3) = \Delta[f](x_1, x_2, x_3, x_0)$ and $\Delta[f](x_0, x_1, x_2, x_3) = \Delta[f](x_3, x_2, x_1, x_0)$.

(19) If x_0, x_1, x_2, x_3 are mutually different, then $\Delta[f](x_0, x_1, x_2, x_3) = \Delta[f](x_1, x_0, x_2, x_3)$ and $\Delta[f](x_0, x_1, x_2, x_3) = \Delta[f](x_1, x_2, x_0, x_3)$.

(20) If f is constant, then $\Delta[f](x_0, x_1, x_2) = 0$.

(21) If $x_0 \neq x_1$, then $\Delta[a\square{+}b](x_0, x_1) = a$.

(22) If x_0, x_1, x_2 are mutually different, then $\Delta[a\square{+}b](x_0, x_1, x_2) = 0$.

(23) If x_0, x_1, x_2, x_3 are mutually different, then $\Delta[a\square{+}b](x_0, x_1, x_2, x_3) = 0$.

(24) For every x holds $(\Delta_h[a\square{+}b])(x) = a \cdot h$.

(25) For every x holds $(\nabla_h[a\square{+}b])(x) = a \cdot h$.

(26) For every x holds $(\delta_h[a\square{+}b])(x) = a \cdot h$.

(27) If for every x holds $f(x) = a \cdot x^{\mathbf{2}} + b \cdot x + c$ and $x_0 \neq x_1$, then $\Delta[f](x_0, x_1) = a \cdot (x_0 + x_1) + b$.

(28) If for every x holds $f(x) = a \cdot x^{\mathbf{2}} + b \cdot x + c$ and x_0, x_1, x_2 are mutually different, then $\Delta[f](x_0, x_1, x_2) = a$.

(29) If for every x holds $f(x) = a \cdot x^{\mathbf{2}} + b \cdot x + c$ and x_0, x_1, x_2, x_3 are mutually different, then $\Delta[f](x_0, x_1, x_2, x_3) = 0$.

(30) If for every x holds $f(x) = a \cdot x^{\mathbf{2}} + b \cdot x + c$ and x_0, x_1, x_2, x_3, x_4 are mutually different, then $\Delta[f](x_0, x_1, x_2, x_3, x_4) = 0$.

(31) If for every x holds $f(x) = a \cdot x^{\mathbf{2}} + b \cdot x + c$, then for every x holds $(\Delta_h[f])(x) = 2 \cdot a \cdot h \cdot x + a \cdot h^{\mathbf{2}} + b \cdot h$.

(32) If for every x holds $f(x) = a \cdot x^{\mathbf{2}} + b \cdot x + c$, then for every x holds $(\nabla_h[f])(x) = (2 \cdot a \cdot h \cdot x - a \cdot h^{\mathbf{2}}) + b \cdot h$.

(33) If for every x holds $f(x) = a \cdot x^{\mathbf{2}} + b \cdot x + c$, then for every x holds $(\delta_h[f])(x) = 2 \cdot a \cdot h \cdot x + b \cdot h$.

(34) If for every x holds $f(x) = \frac{k}{x}$ and $x_0 \neq x_1$ and $x_0 \neq 0$ and $x_1 \neq 0$, then $\Delta[f](x_0, x_1) = -\frac{k}{x_0 \cdot x_1}$.

(35) If for every x holds $f(x) = \frac{k}{x}$ and $x_0 \neq 0$ and $x_1 \neq 0$ and $x_2 \neq 0$ and x_0, x_1, x_2 are mutually different, then $\Delta[f](x_0, x_1, x_2) = \frac{k}{x_0 \cdot x_1 \cdot x_2}$.

(36) Suppose for every x holds $f(x) = \frac{k}{x}$ and $x_0 \neq 0$ and $x_1 \neq 0$ and $x_2 \neq 0$ and $x_3 \neq 0$ and x_0, x_1, x_2, x_3 are mutually different. Then $\Delta[f](x_0, x_1, x_2, x_3) = -\frac{k}{x_0 \cdot x_1 \cdot x_2 \cdot x_3}$.

(37) Suppose for every x holds $f(x) = \frac{k}{x}$ and $x_0 \neq 0$ and $x_1 \neq 0$ and $x_2 \neq 0$ and $x_3 \neq 0$ and $x_4 \neq 0$ and x_0, x_1, x_2, x_3, x_4 are mutually different. Then $\Delta[f](x_0, x_1, x_2, x_3, x_4) = \frac{k}{x_0 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4}$.

(38) If for every x holds $f(x) = \frac{k}{x}$ and $x \neq 0$ and $x + h \neq 0$, then for every x holds $(\Delta_h[f])(x) = \frac{-k \cdot h}{(x+h) \cdot x}$.

(39) If for every x holds $f(x) = \frac{k}{x}$ and $x \neq 0$ and $x - h \neq 0$, then for every x holds $(\nabla_h[f])(x) = \frac{-k \cdot h}{(x-h) \cdot x}$.

(40) If for every x holds $f(x) = \frac{k}{x}$ and $x + \frac{h}{2} \neq 0$ and $x - \frac{h}{2} \neq 0$, then for every x holds $(\delta_h[f])(x) = \frac{-k \cdot h}{(x - \frac{h}{2}) \cdot (x + \frac{h}{2})}$.

(41) $\Delta[\text{the function sin}](x_0, x_1) = \frac{2 \cdot \cos(\frac{x_0 + x_1}{2}) \cdot \sin(\frac{x_0 - x_1}{2})}{x_0 - x_1}$.

(42) For every x holds $(\Delta_h[\text{the function sin}])(x) = 2 \cdot (\cos(\frac{2 \cdot x + h}{2}) \cdot \sin(\frac{h}{2}))$.

(43) For every x holds $(\nabla_h[\text{the function sin}])(x) = 2 \cdot (\cos(\frac{2 \cdot x - h}{2}) \cdot \sin(\frac{h}{2}))$.

(44) For every x holds $(\delta_h[\text{the function sin}])(x) = 2 \cdot (\cos x \cdot \sin(\frac{h}{2}))$.

(45) $\Delta[\text{the function cos}](x_0, x_1) = -\frac{2 \cdot \sin(\frac{x_0 + x_1}{2}) \cdot \sin(\frac{x_0 - x_1}{2})}{x_0 - x_1}$.

(46) For every x holds $(\Delta_h[\text{the function cos}])(x) = -2 \cdot (\sin(\frac{2 \cdot x + h}{2}) \cdot \sin(\frac{h}{2}))$.

(47) For every x holds $(\nabla_h[\text{the function cos}])(x) = -2 \cdot (\sin(\frac{2 \cdot x - h}{2}) \cdot \sin(\frac{h}{2}))$.

(48) For every x holds $(\delta_h[\text{the function cos}])(x) = -2 \cdot (\sin x \cdot \sin(\frac{h}{2}))$.

(49) $\Delta[(\text{the function sin})\ (\text{the function sin})](x_0, x_1) = \frac{\frac{1}{2} \cdot (\cos(2 \cdot x_1) - \cos(2 \cdot x_0))}{x_0 - x_1}$.

(50) For every x holds $(\Delta_h[(\text{the function sin})\ (\text{the function sin})])(x) = \frac{1}{2} \cdot (\cos(2 \cdot x) - \cos(2 \cdot (x + h)))$.

(51) For every x holds $(\nabla_h[(\text{the function sin})\ (\text{the function sin})])(x) = \frac{1}{2} \cdot (\cos(2 \cdot (x - h)) - \cos(2 \cdot x))$.

(52) For every x holds $(\delta_h[(\text{the function sin})\ (\text{the function sin})])(x) = \frac{1}{2} \cdot (\cos(2 \cdot x - h) - \cos(2 \cdot x + h))$.

(53) $\Delta[(\text{the function sin})\ (\text{the function cos})](x_0, x_1) = \frac{\frac{1}{2} \cdot (\sin(2 \cdot x_0) - \sin(2 \cdot x_1))}{x_0 - x_1}$.

(54) For every x holds $(\Delta_h[(\text{the function sin})\ (\text{the function cos})])(x) = \frac{1}{2} \cdot (\sin(2 \cdot (x + h)) - \sin(2 \cdot x))$.

(55) For every x holds $(\nabla_h[(\text{the function sin})\ (\text{the function cos})])(x) = \frac{1}{2} \cdot (\sin(2 \cdot x) - \sin(2 \cdot (x - h)))$.

(56) For every x holds $(\delta_h[(\text{the function sin})\ (\text{the function cos})])(x) = \frac{1}{2} \cdot (\sin(2 \cdot x + h) - \sin(2 \cdot x - h))$.

(57) $\Delta[(\text{the function cos})\ (\text{the function cos})](x_0, x_1) = \frac{\frac{1}{2} \cdot (\cos(2 \cdot x_0) - \cos(2 \cdot x_1))}{x_0 - x_1}$.

(58) For every x holds $(\Delta_h[(\text{the function cos})\ (\text{the function cos})])(x) = \frac{1}{2} \cdot (\cos(2 \cdot (x + h)) - \cos(2 \cdot x))$.

(59) For every x holds $(\nabla_h[(\text{the function cos})\ (\text{the function cos})])(x) = \frac{1}{2} \cdot (\cos(2 \cdot x) - \cos(2 \cdot (x - h)))$.

(60) For every x holds $(\delta_h[(\text{the function cos})\ (\text{the function cos})])(x) = \frac{1}{2} \cdot (\cos(2 \cdot x + h) - \cos(2 \cdot x - h))$.

(61) $\Delta[(\text{the function sin})\ (\text{the function sin})\ (\text{the function cos})](x_0, x_1) = -\frac{\frac{1}{2} \cdot (\sin(\frac{3 \cdot (x_1 + x_0)}{2}) \cdot \sin(\frac{3 \cdot (x_1 - x_0)}{2}) + \sin(\frac{x_0 + x_1}{2}) \cdot \sin(\frac{x_0 - x_1}{2}))}{x_0 - x_1}$.

(62) Let given x. Then $(\Delta_h[(\text{the function sin})\ (\text{the function sin})\ (\text{the function cos})])(x) = \frac{1}{2} \cdot (\sin(\frac{6 \cdot x + 3 \cdot h}{2}) \cdot \sin(\frac{3 \cdot h}{2}) - \sin(\frac{2 \cdot x + h}{2}) \cdot \sin(\frac{h}{2}))$.

(63) Let given x. Then $(\nabla_h[(\text{the function sin})\ (\text{the function sin})\ (\text{the function cos})])(x) = \frac{1}{2} \cdot (\sin(\frac{6 \cdot x - 3 \cdot h}{2}) \cdot \sin(\frac{3 \cdot h}{2})) - \frac{1}{2} \cdot (\sin(\frac{2 \cdot x - h}{2}) \cdot \sin(\frac{h}{2}))$.

(64) For every x holds $(\delta_h[(\text{the function sin})\ (\text{the function sin})\ (\text{the function cos})])(x) = -\frac{1}{2} \cdot (\sin x \cdot \sin(\frac{h}{2})) + \frac{1}{2} \cdot (\sin(3 \cdot x) \cdot \sin(\frac{3 \cdot h}{2}))$.

(65) $\Delta[(\text{the function sin})\ (\text{the function cos})\ (\text{the function cos})](x_0, x_1) = \frac{\frac{1}{2} \cdot (\cos(\frac{x_0 + x_1}{2}) \cdot \sin(\frac{x_0 - x_1}{2}) + \cos(\frac{3 \cdot (x_0 + x_1)}{2}) \cdot \sin(\frac{3 \cdot (x_0 - x_1)}{2}))}{x_0 - x_1}$.

(66) Let given x. Then $(\Delta_h[(\text{the function sin})\ (\text{the function cos})\ (\text{the function cos})])(x) = \frac{1}{2} \cdot (\cos(\frac{2 \cdot x + h}{2}) \cdot \sin(\frac{h}{2}) + \cos(\frac{6 \cdot x + 3 \cdot h}{2}) \cdot \sin(\frac{3 \cdot h}{2}))$.

(67) Let given x. Then $(\nabla_h[(\text{the function sin})\ (\text{the function cos})\ (\text{the function cos})])(x) = \frac{1}{2} \cdot (\cos(\frac{2 \cdot x - h}{2}) \cdot \sin(\frac{h}{2}) + \cos(\frac{6 \cdot x - 3 \cdot h}{2}) \cdot \sin(\frac{3 \cdot h}{2}))$.

(68) For every x holds $(\delta_h[$(the function sin) (the function cos) (the function cos)$])(x) = \frac{1}{2} \cdot (\cos x \cdot \sin(\frac{h}{2}) + \cos(3 \cdot x) \cdot \sin(\frac{3 \cdot h}{2}))$.

(69) If $x_0 \in \mathrm{dom}$ (the function tan) and $x_1 \in \mathrm{dom}$ (the function tan), then $\Delta[$the function tan$](x_0, x_1) = \frac{\sin(x_0 - x_1)}{\cos x_0 \cdot \cos x_1 \cdot (x_0 - x_1)}$.

(70) If $x_0 \in \mathrm{dom}$ (the function cot) and $x_1 \in \mathrm{dom}$ (the function cot), then $\Delta[$the function cot$](x_0, x_1) = -\frac{\sin(x_0 - x_1)}{\sin x_0 \cdot \sin x_1 \cdot (x_0 - x_1)}$.

(71) Suppose $x_0 \in \mathrm{dom}$ (the function cosec) and $x_1 \in \mathrm{dom}$ (the function cosec). Then $\Delta[$the function cosec$](x_0, x_1) = \frac{2 \cdot \cos(\frac{x_1 + x_0}{2}) \cdot \sin(\frac{x_1 - x_0}{2})}{\sin x_1 \cdot \sin x_0 \cdot (x_0 - x_1)}$.

(72) Suppose $x_0 \in \mathrm{dom}$ (the function sec) and $x_1 \in \mathrm{dom}$ (the function sec). Then $\Delta[$the function sec$](x_0, x_1) = -\frac{2 \cdot \sin(\frac{x_1 + x_0}{2}) \cdot \sin(\frac{x_1 - x_0}{2})}{\cos x_1 \cdot \cos x_0 \cdot (x_0 - x_1)}$.

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. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[4] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[5] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[6] Bo Li, Yan Zhang, and Xiquan Liang. Difference and difference quotient. *Formalized Mathematics*, 14(**3**):115–119, 2006.
[7] Beata Perkowska. Functional sequence from a domain to a domain. *Formalized Mathematics*, 3(**1**):17–21, 1992.
[8] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[9] Andrzej Trybulec and Yatsuka Nakamura. On the decomposition of a simple closed curve into two arcs. *Formalized Mathematics*, 10(**3**):163–167, 2002.
[10] Peng Wang and Bo Li. Several differentiation formulas of special functions. Part V. *Formalized Mathematics*, 15(**3**):73–79, 2007.
[11] Renhong Wang. *Numerical approximation*. Higher Education Press, Beijing, 1999.
[12] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[13] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

Received October 25, 2007

FORMALIZED MATHEMATICS
Vol. **16**, No. **1**, Pages 51–55, **2008**

The First Mean Value Theorem for Integrals

Keiko Narita
Hirosaki-city
Aomori, Japan

Noboru Endou
Gifu National College of Technology
Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we prove the first mean value theorem for integrals [16]. The formalization of various theorems about the properties of the Lebesgue integral is also presented.

MML identifier: `MESFUNC7`, version: `7.8.09 4.97.1001`

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

1. Lemmas for Extended Real Valued Functions

For simplicity, we use the following convention: X is a non empty set, S is a σ-field of subsets of X, M is a σ-measure on S, f, g are partial functions from X to $\overline{\mathbb{R}}$, and E is an element of S.

One can prove the following three propositions:

(1) If for every element x of X such that $x \in \operatorname{dom} f$ holds $f(x) \leq g(x)$, then $g - f$ is non-negative.

(2) For every set Y and for every partial function f from X to $\overline{\mathbb{R}}$ and for every real number r holds $(r\, f){\restriction}Y = r\,(f{\restriction}Y)$.

(3) Suppose f is integrable on M and g is integrable on M and $g - f$ is non-negative. Then there exists an element E of S such that $E = \operatorname{dom} f \cap \operatorname{dom} g$ and $\int f{\restriction}E \,\mathrm{d}M \leq \int g{\restriction}E \,\mathrm{d}M$.

ISSN 1426–2630(p), 1898-9934(e)

2. σ-Finite Sets

Let us consider X. One can verify that there exists a partial function from X to $\overline{\mathbb{R}}$ which is non-negative.

Let us consider X, f. Then $|f|$ is a non-negative partial function from X to $\overline{\mathbb{R}}$.

Next we state the proposition

(4) Suppose f is integrable on M. Then there exists a function F from $\mathbb{N}$ into S such that

(i) for every element n of $\mathbb{N}$ holds $F(n) = \mathrm{dom}\, f \cap \text{GTE-dom}(|f|, \overline{\mathbb{R}}(\frac{1}{n+1}))$,

(ii) $\mathrm{dom}\, f \setminus \text{EQ-dom}(f, 0_{\overline{\mathbb{R}}}) = \bigcup \mathrm{rng}\, F$, and

(iii) for every element n of $\mathbb{N}$ holds $F(n) \in S$ and $M(F(n)) < +\infty$.

3. The First Mean Value Theorem for Integrals

Let F be a binary relation. We introduce F is extreal-yielding as a synonym of F is extended real-valued.

Let k be a natural number and let x be an element of $\overline{\mathbb{R}}$. Then $k \mapsto x$ is a finite sequence of elements of $\overline{\mathbb{R}}$.

Let us note that there exists a finite sequence which is extreal-yielding.

The binary operation $\cdot_{\overline{\mathbb{R}}}$ on $\overline{\mathbb{R}}$ is defined by:

(Def. 2)[1] For all elements x, y of $\overline{\mathbb{R}}$ holds $\cdot_{\overline{\mathbb{R}}}(x, y) = x \cdot y$.

One can check that $\cdot_{\overline{\mathbb{R}}}$ is commutative and associative.

One can prove the following proposition

(5) $\mathbf{1}_{\cdot_{\overline{\mathbb{R}}}} = 1$.

One can check that $\cdot_{\overline{\mathbb{R}}}$ is unital.

Let F be an extreal-yielding finite sequence. The functor $\prod F$ yields an element of $\overline{\mathbb{R}}$ and is defined by:

(Def. 3) There exists a finite sequence f of elements of $\overline{\mathbb{R}}$ such that $f = F$ and $\prod F = \cdot_{\overline{\mathbb{R}}} \circledast f$.

Let x be an element of $\overline{\mathbb{R}}$ and let n be a natural number. Note that $n \mapsto x$ is extreal-yielding.

Let x be an element of $\overline{\mathbb{R}}$ and let k be a natural number. The functor x^k is defined by:

(Def. 4) $x^k = \prod(k \mapsto x)$.

Let x be an element of $\overline{\mathbb{R}}$ and let k be a natural number. Then x^k is an extended real number.

Let us note that $\varepsilon_{\overline{\mathbb{R}}}$ is extreal-yielding.

[1]The definition (Def. 1) has been removed.

Let r be an element of $\overline{\mathbb{R}}$. Note that $\langle r \rangle$ is extreal-yielding.

We now state two propositions:

(6) $\prod(\varepsilon_{\overline{\mathbb{R}}}) = 1$.

(7) For every element r of $\overline{\mathbb{R}}$ holds $\prod\langle r \rangle = r$.

Let f, g be extreal-yielding finite sequences. Observe that $f \frown g$ is extreal-yielding.

We now state three propositions:

(8) For every extreal-yielding finite sequence F and for every element r of $\overline{\mathbb{R}}$ holds $\prod(F \frown \langle r \rangle) = \prod F \cdot r$.

(9) For every element x of $\overline{\mathbb{R}}$ holds $x^1 = x$.

(10) For every element x of $\overline{\mathbb{R}}$ and for every natural number k holds $x^{k+1} = x^k \cdot x$.

Let k be a natural number and let us consider X, f. The functor f^k yields a partial function from X to $\overline{\mathbb{R}}$ and is defined by:

(Def. 5) $\mathrm{dom}(f^k) = \mathrm{dom}\, f$ and for every element x of X such that $x \in \mathrm{dom}(f^k)$ holds $f^k(x) = f(x)^k$.

Next we state several propositions:

(11) For every element x of $\overline{\mathbb{R}}$ and for every real number y and for every natural number k such that $x = y$ holds $x^k = y^k$.

(12) For every element x of $\overline{\mathbb{R}}$ and for every natural number k such that $0 \leq x$ holds $0 \leq x^k$.

(13) For every natural number k such that $1 \leq k$ holds $+\infty^k = +\infty$.

(14) Let k be a natural number and given X, S, f, E. If $E \subseteq \mathrm{dom}\, f$ and f is measurable on E, then $|f|^k$ is measurable on E.

(15) Suppose $\mathrm{dom}\, f \cap \mathrm{dom}\, g = E$ and f is finite and g is finite and f is measurable on E and g is measurable on E. Then $f\, g$ is measurable on E.

(16) If $\mathrm{rng}\, f$ is bounded, then f is finite.

(17) Let M be a σ-measure on S, f, g be partial functions from X to $\overline{\mathbb{R}}$, E be an element of S, and F be a non empty subset of $\overline{\mathbb{R}}$. Suppose $\mathrm{dom}\, f \cap \mathrm{dom}\, g = E$ and $\mathrm{rng}\, f = F$ and g is finite and f is measurable on E and $\mathrm{rng}\, f$ is bounded and g is integrable on M. Then $(f\, g){\restriction}E$ is integrable on M and there exists an element c of $\mathbb{R}$ such that $c \geq \inf F$ and $c \leq \sup F$ and $\int (f\, |g|){\restriction}E \,\mathrm{d}M = \overline{\mathbb{R}}(c) \cdot \int |g|{\restriction}E \,\mathrm{d}M$.

4. Selected Properties of Integrals

We use the following convention: E_1, E_2 denote elements of S, x, A denote sets, and a, b denote real numbers.

The following propositions are true:

(18) $|f|{\restriction}A = |f{\restriction}A|$.

(19) $\mathrm{dom}(|f| + |g|) = \mathrm{dom}\, f \cap \mathrm{dom}\, g$ and $\mathrm{dom}\, |f + g| \subseteq \mathrm{dom}\, |f|$.

(20) $|f|{\restriction}\mathrm{dom}\, |f + g| + |g|{\restriction}\mathrm{dom}\, |f + g| = (|f| + |g|){\restriction}\mathrm{dom}\, |f + g|$.

(21) If $x \in \mathrm{dom}\, |f + g|$, then $|f + g|(x) \leq (|f| + |g|)(x)$.

(22) Suppose f is integrable on M and g is integrable on M. Then there exists an element E of S such that $E = \mathrm{dom}(f+g)$ and $\int |f+g|{\restriction}E \,\mathrm{d}M \leq \int |f|{\restriction}E \,\mathrm{d}M + \int |g|{\restriction}E \,\mathrm{d}M$.

(23) $\max_{+}(\chi_{A,X}) = \chi_{A,X}$.

(24) If $M(E) < +\infty$, then $\chi_{E,X}$ is integrable on M and $\int \chi_{E,X} \,\mathrm{d}M = M(E)$ and $\int \chi_{E,X}{\restriction}E \,\mathrm{d}M = M(E)$.

(25) If $M(E_1 \cap E_2) < +\infty$, then $\int \chi_{(E_1),X}{\restriction}E_2 \,\mathrm{d}M = M(E_1 \cap E_2)$.

(26) Suppose f is integrable on M and $E \subseteq \mathrm{dom}\, f$ and $M(E) < +\infty$ and for every element x of X such that $x \in E$ holds $a \leq f(x) \leq b$. Then $\overline{\mathbb{R}}(a) \cdot M(E) \leq \int f{\restriction}E \,\mathrm{d}M \leq \overline{\mathbb{R}}(b) \cdot M(E)$.

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] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Józef Białas. Infimum and supremum of the set of real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):163–171, 1991.
[5] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.
[6] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.
[7] Józef Białas. Some properties of the intervals. *Formalized Mathematics*, 5(**1**):21–26, 1996.
[8] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[9] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[10] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[11] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[12] Noboru Endou and Yasunari Shidama. Integral of measurable function. *Formalized Mathematics*, 14(**2**):53–70, 2006.
[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] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[18] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[19] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.
[20] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[21] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[22] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received October 30, 2007

FORMALIZED MATHEMATICS
Vol. **16**, No. **1**, Pages 57–63, **2008**

Egoroff's Theorem

Noboru Endou
Gifu National College of Technology
Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Keiko Narita
Hirosaki-city
Aomori, Japan

Summary. The goal of this article is to prove Egoroff's Theorem [13]. However, there are not enough theorems related to sequence of measurable functions in Mizar Mathematical Library. So we proved many theorems about them. At the end of this article, we showed Egoroff's theorem.

MML identifier: `MESFUNC8`, version: `7.8.10 4.100.1011`

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

1. Selected Properties of Functional Sequences

In this paper n, k are natural numbers, X is a non empty set, and S is a σ-field of subsets of X.

Next we state several propositions:

(1) Let M be a σ-measure on S, F be a function from $\mathbb{N}$ into S, and given n. Then $\{x \in X\colon \bigwedge_k (n \leq k \Rightarrow x \in F(k))\}$ is an element of S.

(2) Let F be a sequence of subsets of X and n be an element of $\mathbb{N}$. Then (the superior set sequence of $F)(n) = \bigcup \mathrm{rng}(F \uparrow n)$ and (the inferior set sequence of $F)(n) = \bigcap \mathrm{rng}(F \uparrow n)$.

(3) Let M be a σ-measure on S and F be a sequence of subsets of S. Then there exists a function G from $\mathbb{N}$ into S such that $G =$ the inferior set sequence of F and $M(\liminf F) = \sup \mathrm{rng}(M \cdot G)$.

ISSN 1426–2630(p), 1898-9934(e)

(4) Let M be a σ-measure on S and F be a sequence of subsets of S. Suppose $M(\bigcup F) < +\infty$. Then there exists a function G from $\mathbb{N}$ into S such that $G =$ the superior set sequence of F and $M(\limsup F) = \inf \operatorname{rng}(M \cdot G)$.

(5) Let M be a σ-measure on S and F be a sequence of subsets of S. Suppose F is convergent. Then there exists a function G from $\mathbb{N}$ into S such that $G =$ the inferior set sequence of F and $M(\lim F) = \sup \operatorname{rng}(M \cdot G)$.

(6) Let M be a σ-measure on S and F be a sequence of subsets of S. Suppose F is convergent and $M(\bigcup F) < +\infty$. Then there exists a function G from $\mathbb{N}$ into S such that $G =$ the superior set sequence of F and $M(\lim F) = \inf \operatorname{rng}(M \cdot G)$.

Let X, Y be sets and let F be a sequence of partial functions from X into Y. We say that F has the same dom if and only if:

(Def. 1) $\operatorname{rng} F$ has common domain.

Let X, Y be sets and let F be a sequence of partial functions from X into Y. Let us observe that F has the same dom if and only if:

(Def. 2) For all natural numbers n, m holds $\operatorname{dom} F(n) = \operatorname{dom} F(m)$.

Let X, Y be sets. One can verify that there exists a sequence of partial functions from X into Y which has the same dom.

Let X be a non empty set and let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$. The functor $\inf f$ yielding a partial function from X to $\overline{\mathbb{R}}$ is defined as follows:

(Def. 3) $\operatorname{dom} \inf f = \operatorname{dom} f(0)$ and for every element x of X such that $x \in \operatorname{dom} \inf f$ holds $(\inf f)(x) = \inf(f\#x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$. The functor $\sup f$ yields a partial function from X to $\overline{\mathbb{R}}$ and is defined by:

(Def. 4) $\operatorname{dom} \sup f = \operatorname{dom} f(0)$ and for every element x of X such that $x \in \operatorname{dom} \sup f$ holds $(\sup f)(x) = \sup(f\#x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$. The inferior real sequence of f yields a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom and is defined by the condition (Def. 5).

(Def. 5) Let n be a natural number. Then

(i) dom (the inferior real sequence of $f)(n) = \operatorname{dom} f(0)$, and

(ii) for every element x of X such that $x \in$ dom (the inferior real sequence of $f)(n)$ holds (the inferior real sequence of $f)(n)(x) =$ (the inferior real sequence of $f\#x)(n)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$. The superior real sequence of f yields a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom and is defined by the condition (Def. 6).

(Def. 6) Let n be a natural number. Then

(i) dom (the superior real sequence of f)(n) = dom $f(0)$, and

(ii) for every element x of X such that $x \in$ dom (the superior real sequence of f)(n) holds (the superior real sequence of f)$(n)(x)$ = (the superior real sequence of $f\#x$)(n).

One can prove the following proposition

(7) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ and x be an element of X. Suppose $x \in \operatorname{dom} f(0)$. Then (the inferior real sequence of f)$\#x$ = the inferior real sequence of $f\#x$.

Let X, Y be sets. We see that the sequence of partial functions from X into Y is a function from $\mathbb{N}$ into $X \dot{\to} Y$.

Let X, Y be sets, let f be a sequence of partial functions from X into Y with the same dom, and let n be an element of $\mathbb{N}$. Observe that $f \uparrow n$ has the same dom.

Next we state three propositions:

(8) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom and n be an element of $\mathbb{N}$. Then (the inferior real sequence of f)(n) = $\inf(f \uparrow n)$.

(9) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom and n be an element of $\mathbb{N}$. Then (the superior real sequence of f)(n) = $\sup(f \uparrow n)$.

(10) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ and x be an element of X. Suppose $x \in \operatorname{dom} f(0)$. Then (the superior real sequence of f)$\#x$ = the superior real sequence of $f\#x$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$. The functor $\liminf f$ yielding a partial function from X to $\overline{\mathbb{R}}$ is defined as follows:

(Def. 8)[1] $\operatorname{dom} \liminf f = \operatorname{dom} f(0)$ and for every element x of X such that $x \in \operatorname{dom} \liminf f$ holds $(\liminf f)(x) = \liminf(f\#x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$. The functor $\limsup f$ yielding a partial function from X to $\overline{\mathbb{R}}$ is defined as follows:

(Def. 9) $\operatorname{dom} \limsup f = \operatorname{dom} f(0)$ and for every element x of X such that $x \in \operatorname{dom} \limsup f$ holds $(\limsup f)(x) = \limsup(f\#x)$.

We now state three propositions:

(11) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$. Then

(i) for every element x of X such that $x \in \operatorname{dom} \liminf f$ holds $(\liminf f)(x)$ = sup (the inferior real sequence of $f\#x$) and $(\liminf f)(x)$ = sup((the inferior real sequence of f)$\#x$) and $(\liminf f)(x)$ = (sup (the inferior real sequence of f))(x), and

[1] The definition (Def. 7) has been removed.

(ii) $\liminf f = \sup$ (the inferior real sequence of f).

(12) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$. Then

(i) for every element x of X such that $x \in \operatorname{dom} \limsup f$ holds $(\limsup f)(x) = \inf$ (the superior real sequence of $f\#x$) and $(\limsup f)(x) = \inf(($the superior real sequence of $f)\#x)$ and $(\limsup f)(x) = (\inf$ (the superior real sequence of $f))(x)$, and

(ii) $\limsup f = \inf$ (the superior real sequence of f).

(13) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ and x be an element of X. If $x \in \operatorname{dom} f(0)$, then $f\#x$ is convergent iff $(\limsup f)(x) = (\liminf f)(x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$. The functor $\lim f$ yielding a partial function from X to $\overline{\mathbb{R}}$ is defined by:

(Def. 10) $\operatorname{dom} \lim f = \operatorname{dom} f(0)$ and for every element x of X such that $x \in \operatorname{dom} \lim f$ holds $(\lim f)(x) = \lim(f\#x)$.

One can prove the following propositions:

(14) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ and x be an element of X. If $x \in \operatorname{dom} \lim f$ and $f\#x$ is convergent, then $(\lim f)(x) = (\limsup f)(x)$ and $(\lim f)(x) = (\liminf f)(x)$.

(15) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom, F be a sequence of subsets of S, and r be a real number. Suppose that for every natural number n holds $F(n) = \operatorname{dom} f(0) \cap \text{GT-dom}(f(n), \overline{\mathbb{R}}(r))$. Then $\bigcup \operatorname{rng} F = \operatorname{dom} f(0) \cap \text{GT-dom}(\sup f, \overline{\mathbb{R}}(r))$.

(16) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom, F be a sequence of subsets of S, and r be a real number. Suppose that for every natural number n holds $F(n) = \operatorname{dom} f(0) \cap \text{GTE-dom}(f(n), \overline{\mathbb{R}}(r))$. Then $\bigcap \operatorname{rng} F = \operatorname{dom} f(0) \cap \text{GTE-dom}(\inf f, \overline{\mathbb{R}}(r))$.

(17) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom, F be a sequence of subsets of S, and r be a real number. Suppose that for every natural number n holds $F(n) = \operatorname{dom} f(0) \cap \text{GT-dom}(f(n), \overline{\mathbb{R}}(r))$. Let n be a natural number. Then (the superior set sequence of $F)(n) = \operatorname{dom} f(0) \cap \text{GT-dom}(($the superior real sequence of $f)(n), \overline{\mathbb{R}}(r))$.

(18) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom, F be a sequence of subsets of S, and r be a real number. Suppose that for every natural number n holds $F(n) = \operatorname{dom} f(0) \cap \text{GTE-dom}(f(n), \overline{\mathbb{R}}(r))$. Let n be a natural number. Then (the inferior set sequence of $F)(n) = \operatorname{dom} f(0) \cap \text{GTE-dom}(($the inferior real sequence of $f)(n), \overline{\mathbb{R}}(r))$.

(19) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom and E be an element of S. Suppose $\operatorname{dom} f(0) = E$ and for every

natural number n holds $f(n)$ is measurable on E. Let given n. Then (the superior real sequence of $f)(n)$ is measurable on E.

(20) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom and E be an element of S. Suppose $\operatorname{dom} f(0) = E$ and for every natural number n holds $f(n)$ is measurable on E. Let n be a natural number. Then (the inferior real sequence of $f)(n)$ is measurable on E.

(21) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$, F be a sequence of subsets of S, and r be a real number. Suppose that for every natural number n holds $F(n) = \operatorname{dom} f(0) \cap \text{GTE-dom}((\text{the superior real sequence of } f)(n), \overline{\mathbb{R}}(r))$. Then $\bigcap F = \operatorname{dom} f(0) \cap \text{GTE-dom}(\limsup f, \overline{\mathbb{R}}(r))$.

(22) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$, F be a sequence of subsets of S, and r be a real number. Suppose that for every natural number n holds $F(n) = \operatorname{dom} f(0) \cap \text{GT-dom}((\text{the inferior real sequence of } f)(n), \overline{\mathbb{R}}(r))$. Then $\bigcup \operatorname{rng} F = \operatorname{dom} f(0) \cap \text{GT-dom}(\liminf f, \overline{\mathbb{R}}(r))$.

(23) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom and E be an element of S. Suppose $\operatorname{dom} f(0) = E$ and for every natural number n holds $f(n)$ is measurable on E. Then $\limsup f$ is measurable on E.

(24) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom and E be an element of S. Suppose $\operatorname{dom} f(0) = E$ and for every natural number n holds $f(n)$ is measurable on E. Then $\liminf f$ is measurable on E.

(25) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom and E be an element of S. Suppose that

(i) $\operatorname{dom} f(0) = E$,

(ii) for every natural number n holds $f(n)$ is measurable on E, and

(iii) for every element x of X such that $x \in E$ holds $f\#x$ is convergent.

Then $\lim f$ is measurable on E.

(26) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom, g be a partial function from X to $\overline{\mathbb{R}}$, and E be an element of S. Suppose that

(i) $\operatorname{dom} f(0) = E$,

(ii) for every natural number n holds $f(n)$ is measurable on E,

(iii) $\operatorname{dom} g = E$, and

(iv) for every element x of X such that $x \in E$ holds $f\#x$ is convergent and $g(x) = \lim(f\#x)$.

Then g is measurable on E.

(27) Let f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ and g be a partial function from X to $\overline{\mathbb{R}}$. Suppose that for every element x of X such that $x \in \operatorname{dom} g$ holds $f\#x$ is convergent to finite number and $g(x) = \lim(f\#x)$. Then g is finite.

2. Egoroff's Theorem

The following three propositions are true:

(28) Let M be a σ-measure on S, f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom, g be a partial function from X to $\overline{\mathbb{R}}$, and E be an element of S. Suppose that

(i) $M(E) < +\infty$,

(ii) $\mathrm{dom}\, f(0) = E$,

(iii) for every natural number n holds $f(n)$ is measurable on E and $f(n)$ is finite,

(iv) $\mathrm{dom}\, g = E$, and

(v) for every element x of X such that $x \in E$ holds $f\#x$ is convergent to finite number and $g(x) = \lim(f\#x)$.

Let r, e be real numbers. Suppose $0 < r$ and $0 < e$. Then there exists an element H of S and there exists a natural number N such that

(vi) $H \subseteq E$,

(vii) $M(H) < r$, and

(viii) for every natural number k such that $N < k$ and for every element x of X such that $x \in E \setminus H$ holds $|f(k)(x) - g(x)| < e$.

(29) Let X, Y be non empty sets, E be a set, and F, G be functions from X into Y. If for every element x of X holds $G(x) = E \setminus F(x)$, then $\bigcup \mathrm{rng}\, G = E \setminus \bigcap \mathrm{rng}\, F$.

(30) Let M be a σ-measure on S, f be a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom, g be a partial function from X to $\overline{\mathbb{R}}$, and E be an element of S. Suppose that

(i) $\mathrm{dom}\, f(0) = E$,

(ii) for every natural number n holds $f(n)$ is measurable on E,

(iii) $M(E) < +\infty$,

(iv) for every natural number n there exists an element L of S such that $L \subseteq E$ and $M(E \setminus L) = 0$ and for every element x of X such that $x \in L$ holds $|f(n)(x)| < +\infty$, and

(v) there exists an element G of S such that $G \subseteq E$ and $M(E \setminus G) = 0$ and for every element x of X such that $x \in E$ holds $f\#x$ is convergent to finite number and $\mathrm{dom}\, g = E$ and for every element x of X such that $x \in G$ holds $g(x) = \lim(f\#x)$.

Let e be a real number. Suppose $0 < e$. Then there exists an element F of S such that

(vi) $F \subseteq E$,

(vii) $M(E \setminus F) \leq e$, and

(viii) for every real number p such that $0 < p$ there exists a natural number N such that for every natural number n such that $N < n$ and for every element x of X such that $x \in F$ holds $|f(n)(x) - g(x)| < p$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[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] Józef Białas. Some properties of the intervals. *Formalized Mathematics*, 5(**1**):21–26, 1996.
[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] Noboru Endou and Yasunari Shidama. Integral of measurable function. *Formalized Mathematics*, 14(**2**):53–70, 2006.
[10] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Basic properties of extended real numbers. *Formalized Mathematics*, 9(**3**):491–494, 2001.
[11] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definitions and basic properties of measurable functions. *Formalized Mathematics*, 9(**3**):495–500, 2001.
[12] Adam Grabowski. On the Kuratowski limit operators. *Formalized Mathematics*, 11(**4**):399–409, 2003.
[13] P. R. Halmos. *Measure Theory*. Springer-Verlag, 1987.
[14] Jarosław Kotowicz and Yuji Sakai. Properties of partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 3(**2**):279–288, 1992.
[15] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.
[16] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[17] Beata Perkowska. Functional sequence from a domain to a domain. *Formalized Mathematics*, 3(**1**):17–21, 1992.
[18] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[19] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[20] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[21] 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.
[22] Bo Zhang, Hiroshi Yamazaki, and Yatsuka Nakamura. Limit of sequence of subsets. *Formalized Mathematics*, 13(**2**):347–352, 2005.

Received October 30, 2007

FORMALIZED MATHEMATICS
Vol. **16**, No. **1**, Pages 65–71, **2008**

BCI-algebras with Condition (S) and their Properties

Tao Sun
Qingdao University of Science and Technology
China

Junjie Zhao
Qingdao University of Science and Technology
China

Xiquan Liang
Qingdao University of Science and Technology
China

Summary. In this article we will first investigate the elementary properties of BCI-algebras with condition (S), see [8]. And then we will discuss the three classes of algebras: commutative, positive-implicative and implicative BCK-algebras with condition (S).

MML identifier: BCIALG_4, version: 7.8.09 4.97.1001

The papers [5], [12], [3], [1], [6], [2], [10], [9], [4], [11], and [7] provide the notation and terminology for this paper.

We introduce BCI stuctures with complements which are extensions of BCI structure with 0 and zero structure and are systems

⟨ a carrier, an external complement, an internal complement, a zero ⟩,

where the carrier is a set, the external complement and the internal complement are binary operations on the carrier, and the zero is an element of the carrier.

Let us mention that there exists a BCI structure with complements which is non empty and strict.

Let A be a BCI structure with complements and let x, y be elements of A. The functor $x \cdot y$ yields an element of A and is defined as follows:

(Def. 1) $x \cdot y =$ (the external complement of A)(x, y).

ISSN 1426–2630(p), 1898-9934(e)

Let $\mathfrak{B}$ be a non empty BCI structure with complements. We say that $\mathfrak{B}$ satisfies condition (S) if and only if:

(Def. 2) For all elements x, y, z of $\mathfrak{B}$ holds $x \setminus y \setminus z = x \setminus y \cdot z$.

The BCI structure the BCI S-example with complements is defined by:

(Def. 3) The BCI S-example $= \langle 1, \mathrm{op}_2, \mathrm{op}_2, \mathrm{op}_0 \rangle$.

Let us observe that the BCI S-example is strict, non empty, and trivial.

Let us observe that the BCI S-example is B, C, I, BCI-4, and BCK-5 and satisfies condition (S).

Let us note that there exists a non empty BCI structure with complements which is strict, B, C, I, and BCI-4 and satisfies condition (S).

A BCI-algebra with condition (S) is B C I BCI-4 non empty BCI structure with complements satisfying condition (S).

In the sequel $\mathfrak{X}$ is a non empty BCI structure with complements, x, d are elements of $\mathfrak{X}$, and n is an element of $\mathbb{N}$.

Let $\mathfrak{X}$ be a BCI-algebra with condition (S) and let x, y be elements of $\mathfrak{X}$. The functor ConditionS(x, y) yields a non empty subset of $\mathfrak{X}$ and is defined as follows:

(Def. 4) ConditionS$(x, y) = \{t \in \mathfrak{X}\colon t \setminus x \leq y\}$.

We now state four propositions:

(1) Let $\mathfrak{X}$ be a BCI-algebra with condition (S) and x, y, u, v be elements of $\mathfrak{X}$. If $u \in$ ConditionS(x, y) and $v \leq u$, then $v \in$ ConditionS(x, y).

(2) Let $\mathfrak{X}$ be a BCI-algebra with condition (S) and x, y be elements of $\mathfrak{X}$. Then there exists an element a of ConditionS(x, y) such that for every element z of ConditionS(x, y) holds $z \leq a$.

(3) $\mathfrak{X}$ is a BCI-algebra and for all elements x, y of $\mathfrak{X}$ holds $x \cdot y \setminus x \leq y$ and for every element t of $\mathfrak{X}$ such that $t \setminus x \leq y$ holds $t \leq x \cdot y$ if and only if $\mathfrak{X}$ is a BCI-algebra with condition (S).

(4) Let $\mathfrak{X}$ be a BCI-algebra with condition (S) and x, y be elements of $\mathfrak{X}$. Then there exists an element a of ConditionS(x, y) such that for every element z of ConditionS(x, y) holds $z \leq a$.

Let $\mathfrak{X}$ be a p-semisimple BCI-algebra. The adjoint p-group of $\mathfrak{X}$ yields a strict Abelian group and is defined by the conditions (Def. 5).

(Def. 5)(i) The carrier of the adjoint p-group of $\mathfrak{X}$ = the carrier of $\mathfrak{X}$,

(ii) for all elements x, y of $\mathfrak{X}$ holds (the addition of the adjoint p-group of $\mathfrak{X}$)$(x, y) = x \setminus (0_{\mathfrak{X}} \setminus y)$, and

(iii) $0_{\text{the adjoint p-group of } \mathfrak{X}} = 0_{\mathfrak{X}}$.

We now state a number of propositions:

(5) Let $\mathfrak{X}$ be a BCI-algebra. Then $\mathfrak{X}$ is p-semisimple if and only if for all elements x, y of $\mathfrak{X}$ such that $x \setminus y = 0_{\mathfrak{X}}$ holds $x = y$.

(6) Let $\mathfrak{X}$ be a BCI-algebra with condition (S). Suppose $\mathfrak{X}$ is p-semisimple. Let x, y be elements of $\mathfrak{X}$. Then $x \cdot y = x \setminus (0_{\mathfrak{X}} \setminus y)$.

(7) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, y of $\mathfrak{X}$ holds $x \cdot y = y \cdot x$.

(8) Let $\mathfrak{X}$ be a BCI-algebra with condition (S) and x, y, z be elements of $\mathfrak{X}$. If $x \leq y$, then $x \cdot z \leq y \cdot z$ and $z \cdot x \leq z \cdot y$.

(9) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for every element x of $\mathfrak{X}$ holds $0_{\mathfrak{X}} \cdot x = x$ and $x \cdot 0_{\mathfrak{X}} = x$.

(10) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, y, z of $\mathfrak{X}$ holds $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(11) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, y, z of $\mathfrak{X}$ holds $x \cdot y \cdot z = x \cdot z \cdot y$.

(12) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, y, z of $\mathfrak{X}$ holds $x \setminus y \setminus z = x \setminus y \cdot z$.

(13) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, y of $\mathfrak{X}$ holds $y \leq x \cdot (y \setminus x)$.

(14) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, y, z of $\mathfrak{X}$ holds $x \cdot z \setminus y \cdot z \leq x \setminus y$.

(15) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, y, z of $\mathfrak{X}$ holds $x \setminus y \leq z$ iff $x \leq y \cdot z$.

(16) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, y, z of $\mathfrak{X}$ holds $x \setminus y \leq (x \setminus z) \cdot (z \setminus y)$.

Let $\mathfrak{X}$ be a BCI-algebra with condition (S). One can check that the external complement of $\mathfrak{X}$ is commutative and associative.

Next we state three propositions:

(17) For every BCI-algebra $\mathfrak{X}$ with condition (S) holds $0_{\mathfrak{X}}$ is a unity w.r.t. the external complement of $\mathfrak{X}$.

(18) For every BCI-algebra $\mathfrak{X}$ with condition (S) holds $\mathbf{1}_{\text{the external complement of } \mathfrak{X}} = 0_{\mathfrak{X}}$.

(19) For every BCI-algebra $\mathfrak{X}$ with condition (S) holds the external complement of $\mathfrak{X}$ has a unity.

Let $\mathfrak{X}$ be a BCI-algebra with condition (S). The functor $\mathrm{power}_{\mathfrak{X}}$ yielding a function from (the carrier of $\mathfrak{X}$) $\times\, \mathbb{N}$ into the carrier of $\mathfrak{X}$ is defined as follows:

(Def. 6) For every element h of $\mathfrak{X}$ holds $\mathrm{power}_{\mathfrak{X}}(h, 0) = 0_{\mathfrak{X}}$ and for every n holds $\mathrm{power}_{\mathfrak{X}}(h, n+1) = \mathrm{power}_{\mathfrak{X}}(h, n) \cdot h$.

Let $\mathfrak{X}$ be a BCI-algebra with condition (S), let x be an element of $\mathfrak{X}$, and let us consider n. The functor x^n yields an element of $\mathfrak{X}$ and is defined by:

(Def. 7) $x^n = \mathrm{power}_{\mathfrak{X}}(x, n)$.

The following propositions are true:

(20) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for every element x of $\mathfrak{X}$ holds $x^0 = 0_{\mathfrak{X}}$.

(21) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for every element x of $\mathfrak{X}$ holds $x^{n+1} = x^n \cdot x$.

(22) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for every element x of $\mathfrak{X}$ holds $x^1 = x$.

(23) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for every element x of $\mathfrak{X}$ holds $x^2 = x \cdot x$.

(24) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for every element x of $\mathfrak{X}$ holds $x^3 = x \cdot x \cdot x$.

(25) For every BCI-algebra $\mathfrak{X}$ with condition (S) holds $(0_{\mathfrak{X}})^2 = 0_{\mathfrak{X}}$.

(26) For every BCI-algebra $\mathfrak{X}$ with condition (S) holds $(0_{\mathfrak{X}})^n = 0_{\mathfrak{X}}$.

(27) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, a of $\mathfrak{X}$ holds $x \setminus a \setminus a \setminus a = x \setminus a^3$.

(28) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, a of $\mathfrak{X}$ holds $(x \setminus a)^n = x \setminus a^n$.

Let $\mathfrak{X}$ be a non empty BCI structure with complements and let F be a finite sequence of elements of the carrier of $\mathfrak{X}$. The functor ProductS(F) yielding an element of $\mathfrak{X}$ is defined by:

(Def. 8) ProductS(F) = the external complement of $\mathfrak{X} \odot F$.

One can prove the following propositions:

(29) The external complement of $\mathfrak{X} \odot \langle d \rangle = d$.

(30) Let $\mathfrak{X}$ be a BCI-algebra with condition (S) and F_1, F_2 be finite sequences of elements of the carrier of $\mathfrak{X}$. Then ProductS($F_1 \frown F_2$) = ProductS(F_1) $\cdot$ ProductS(F_2).

(31) Let $\mathfrak{X}$ be a BCI-algebra with condition (S), F be a finite sequence of elements of the carrier of $\mathfrak{X}$, and a be an element of $\mathfrak{X}$. Then ProductS($F \frown \langle a \rangle$) = ProductS($F$) $\cdot\, a$.

(32) Let $\mathfrak{X}$ be a BCI-algebra with condition (S), F be a finite sequence of elements of the carrier of $\mathfrak{X}$, and a be an element of $\mathfrak{X}$. Then ProductS($\langle a \rangle \frown F$) = $a \cdot$ ProductS(F).

(33) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements a_1, a_2 of $\mathfrak{X}$ holds ProductS($\langle a_1, a_2 \rangle$) = $a_1 \cdot a_2$.

(34) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements a_1, a_2, a_3 of $\mathfrak{X}$ holds ProductS($\langle a_1, a_2, a_3 \rangle$) = $a_1 \cdot a_2 \cdot a_3$.

(35) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, a_1, a_2 of $\mathfrak{X}$ holds $x \setminus a_1 \setminus a_2 = x \setminus$ ProductS($\langle a_1, a_2 \rangle$).

(36) For every BCI-algebra $\mathfrak{X}$ with condition (S) and for all elements x, a_1, a_2, a_3 of $\mathfrak{X}$ holds $x \setminus a_1 \setminus a_2 \setminus a_3 = x \setminus$ ProductS($\langle a_1, a_2, a_3 \rangle$).

(37) Let $\mathfrak{X}$ be a BCI-algebra with condition (S), a, b be elements of $\mathrm{AtomSet}\,\mathfrak{X}$, and m_1 be an element of $\mathfrak{X}$. Suppose that for every element x of $\mathrm{BranchV}\,a$ holds $x \leq m_1$. Then there exists an element m_2 of $\mathfrak{X}$ such that for every element y of $\mathrm{BranchV}\,b$ holds $y \leq m_2$.

Let us observe that there exists a BCI-algebra with condition (S) which is strict and BCK-5.

A BCK-algebra with condition (S) is BCK-5 BCI-algebra with condition (S).

We now state four propositions:

(38) For every BCK-algebra $\mathfrak{X}$ with condition (S) and for all elements x, y of $\mathfrak{X}$ holds $x \leq x \cdot y$ and $y \leq x \cdot y$.

(39) For every BCK-algebra $\mathfrak{X}$ with condition (S) and for all elements x, y, z of $\mathfrak{X}$ holds $x \cdot y \setminus y \cdot z \setminus z \cdot x = 0_{\mathfrak{X}}$.

(40) For every BCK-algebra $\mathfrak{X}$ with condition (S) and for all elements x, y of $\mathfrak{X}$ holds $(x \setminus y) \cdot (y \setminus x) \leq x \cdot y$.

(41) For every BCK-algebra $\mathfrak{X}$ with condition (S) and for every element x of $\mathfrak{X}$ holds $(x \setminus 0_{\mathfrak{X}}) \cdot (0_{\mathfrak{X}} \setminus x) = x$.

Let $\mathfrak{B}$ be a BCK-algebra with condition (S). We say that $\mathfrak{B}$ is commutative if and only if:

(Def. 9) For all elements x, y of $\mathfrak{B}$ holds $x \setminus (x \setminus y) = y \setminus (y \setminus x)$.

One can verify that there exists a BCK-algebra with condition (S) which is commutative.

Next we state two propositions:

(42) Let $\mathfrak{X}$ be a non empty BCI structure with complements. Then $\mathfrak{X}$ is a commutative BCK-algebra with condition (S) if and only if for all elements x, y, z of $\mathfrak{X}$ holds $x \setminus (0_{\mathfrak{X}} \setminus y) = x$ and $(x \setminus z) \setminus (x \setminus y) = y \setminus z \setminus (y \setminus x)$ and $x \setminus y \setminus z = x \setminus y \cdot z$.

(43) Let $\mathfrak{X}$ be a commutative BCK-algebra with condition (S) and a be an element of $\mathfrak{X}$. If a is greatest, then for all elements x, y of $\mathfrak{X}$ holds $x \cdot y = a \setminus (a \setminus x \setminus y)$.

Let $\mathfrak{X}$ be a BCI-algebra and let a be an element of $\mathfrak{X}$. The initial section of a yields a non empty subset of $\mathfrak{X}$ and is defined by:

(Def. 10) The initial section of $a = \{t \in \mathfrak{X}\colon t \leq a\}$.

The following proposition is true

(44) Let $\mathfrak{X}$ be a commutative BCK-algebra with condition (S) and a, b, c be elements of $\mathfrak{X}$. Suppose $\mathrm{ConditionS}(a, b) \subseteq$ the initial section of c. Let x be an element of $\mathrm{ConditionS}(a, b)$. Then $x \leq c \setminus (c \setminus a \setminus b)$.

Let $\mathfrak{B}$ be a BCK-algebra with condition (S). We say that $\mathfrak{B}$ is positive-implicative if and only if:

(Def. 11) For all elements x, y of $\mathfrak{B}$ holds $x \setminus y \setminus y = x \setminus y$.

Let us note that there exists a BCK-algebra with condition (S) which is positive-implicative.

The following propositions are true:

(45) Let $\mathfrak{X}$ be a BCK-algebra with condition (S). Then $\mathfrak{X}$ is positive-implicative if and only if for every element x of $\mathfrak{X}$ holds $x \cdot x = x$.

(46) Let $\mathfrak{X}$ be a BCK-algebra with condition (S). Then $\mathfrak{X}$ is positive-implicative if and only if for all elements x, y of $\mathfrak{X}$ such that $x \leq y$ holds $x \cdot y = y$.

(47) Let $\mathfrak{X}$ be a BCK-algebra with condition (S). Then $\mathfrak{X}$ is positive-implicative if and only if for all elements x, y, z of $\mathfrak{X}$ holds $x \cdot y \setminus z = (x \setminus z) \cdot (y \setminus z)$.

(48) Let $\mathfrak{X}$ be a BCK-algebra with condition (S). Then $\mathfrak{X}$ is positive-implicative if and only if for all elements x, y of $\mathfrak{X}$ holds $x \cdot y = x \cdot (y \setminus x)$.

(49) Let $\mathfrak{X}$ be a positive-implicative BCK-algebra with condition (S) and x, y be elements of $\mathfrak{X}$. Then $x = (x \setminus y) \cdot (x \setminus (x \setminus y))$.

Let $\mathfrak{B}$ be a non empty BCI structure with complements. We say that $\mathfrak{B}$ is SB-1 if and only if:

(Def. 12) For every element x of $\mathfrak{B}$ holds $x \cdot x = x$.

We say that $\mathfrak{B}$ is SB-2 if and only if:

(Def. 13) For all elements x, y of $\mathfrak{B}$ holds $x \cdot y = y \cdot x$.

We say that $\mathfrak{B}$ is SB-4 if and only if:

(Def. 14) For all elements x, y of $\mathfrak{B}$ holds $(x \setminus y) \cdot y = x \cdot y$.

Let us note that the BCI S-example is SB-1, SB-2, SB-4, and I and satisfies condition (S).

Let us note that there exists a non empty BCI structure with complements which is strict, SB-1, SB-2, SB-4, and I and satisfies condition (S).

A semi-Brouwerian algebra is SB-1 SB-2 SB-4 I non empty BCI structure with complements satisfying condition (S).

One can prove the following proposition

(50) Let $\mathfrak{X}$ be a non empty BCI structure with complements. Then $\mathfrak{X}$ is a positive-implicative BCK-algebra with condition (S) if and only if $\mathfrak{X}$ is a semi-Brouwerian algebra.

Let $\mathfrak{B}$ be a BCK-algebra with condition (S). We say that $\mathfrak{B}$ is implicative if and only if:

(Def. 15) For all elements x, y of $\mathfrak{B}$ holds $x \setminus (y \setminus x) = x$.

Let us observe that there exists a BCK-algebra with condition (S) which is implicative.

Next we state two propositions:

(51) Let $\mathfrak{X}$ be a BCK-algebra with condition (S). Then $\mathfrak{X}$ is implicative if and only if $\mathfrak{X}$ is commutative and positive-implicative.

(52) Let $\mathfrak{X}$ be a BCK-algebra with condition (S). Then $\mathfrak{X}$ is implicative if and only if for all elements x, y, z of $\mathfrak{X}$ holds $x \setminus (y \setminus z) = (x \setminus y \setminus z) \cdot (z \setminus (z \setminus x))$.

References

[1] Grzegorz Bancerek. Curried and uncurried functions. *Formalized Mathematics*, 1(**3**):537–541, 1990.

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

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

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

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

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

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

[8] Jie Meng and YoungLin Liu. *An Introduction to BCI-algebras.* Shaanxi Scientific and Technological Press, 2001.

[9] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.

[10] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.

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

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

Received November 24, 2007

FORMALIZED MATHEMATICS
Vol. **16**, No. **1**, Pages 73–80, **2008**

Stability of n-Bit Generalized Full Adder Circuits (GFAs). Part II

Katsumi Wasaki
Shinshu University
Nagano, Japan

Summary. We continue to formalize the concept of the Generalized Full Addition and Subtraction circuits (GFAs), define the structures of calculation units for the Redundant Signed Digit (RSD) operations, then prove its stability of the calculations. Generally, one-bit binary full adder assumes positive weights to all of its three binary inputs and two outputs. We define the circuit structure of two-types n-bit GFAs using the recursive construction to use the RSD arithmetic logical units that we generalize full adder to have both positive and negative weights to inputs and outputs. The motivation for this research is to establish a technique based on formalized mathematics and its applications for calculation circuits with high reliability.

MML identifier: `GFACIRC2`, version: `7.8.09 4.97.1001`

The notation and terminology used in this paper have been introduced in the following articles: [15], [2], [12], [17], [1], [7], [8], [3], [6], [13], [16], [14], [11], [10], [9], [4], [5], and [18]. For simplicity the following abbreviations are introduced

$$\eta_0 = \mathit{Boolean}^0 \longmapsto \mathit{false}$$
$$\eta_1 = \mathit{Boolean}^0 \longmapsto \mathit{true}$$
$$\Sigma_0 = \text{1GateCircStr}(\varepsilon, \eta_0)$$
$$\Sigma_1 = \text{1GateCircStr}(\varepsilon, \eta_1)$$
$$\mathfrak{C}_0 = \text{1GateCircuit}(\varepsilon, \eta_0)$$
$$\mathfrak{C}_1 = \text{1GateCircuit}(\varepsilon, \eta_1)$$

ISSN 1426–2630(p), 1898-9934(e)

1. n-Bit Generalized Full Adder Circuit (TYPE-0)

Let n be a natural number and let x, y be finite sequences. The functor n-BitGFA0Str(x, y) yielding an unsplit non void strict non empty many sorted signature with arity held in gates and Boolean denotation held in gates is defined by the condition (Def. 1).

(Def. 1) There exist many sorted sets f, h indexed by $\mathbb{N}$ such that

(i) n-BitGFA0Str$(x, y) = f(n)$,

(ii) $f(0) = \Sigma_0$,

(iii) $h(0) = \langle \varepsilon, \eta_0 \rangle$, and

(iv) for every element n of $\mathbb{N}$ and for every non empty many sorted signature S and for every set z such that $S = f(n)$ and $z = h(n)$ holds $f(n+1) = S{+\cdot}\,$BitGFA0Str$(x(n+1), y(n+1), z)$ and $h(n+1) =$ GFA0CarryOutput$(x(n+1), y(n+1), z)$.

Let n be an element of $\mathbb{N}$ and let x, y be finite sequences. The functor n-BitGFA0Circ(x, y) yields a Boolean strict circuit of n-BitGFA0Str(x, y) with denotation held in gates and is defined by the condition (Def. 2).

(Def. 2) There exist many sorted sets f, g, h indexed by $\mathbb{N}$ such that

(i) n-BitGFA0Str$(x, y) = f(n)$,

(ii) n-BitGFA0Circ$(x, y) = g(n)$,

(iii) $f(0) = \Sigma_0$,

(iv) $g(0) = \mathfrak{C}_0$,

(v) $h(0) = \langle \varepsilon, \eta_0 \rangle$, and

(vi) for every element n of $\mathbb{N}$ and for every non empty many sorted signature S and for every non-empty algebra A over S and for every set z such that $S = f(n)$ and $A = g(n)$ and $z = h(n)$ holds $f(n+1) = S{+\cdot}\,$BitGFA0Str$(x(n+1), y(n+1), z)$ and $g(n+1) = A{+\cdot}\,$BitGFA0Circ$(x(n+1), y(n+1), z)$ and $h(n+1) =$ GFA0CarryOutput$(x(n+1), y(n+1), z)$.

Let n be an element of $\mathbb{N}$ and let x, y be finite sequences. The functor n-BitGFA0CarryOutput(x, y) yields an element of InnerVertices(n-BitGFA0Str(x, y)) and is defined by the condition (Def. 3).

(Def. 3) There exists a many sorted set h indexed by $\mathbb{N}$ such that n-BitGFA0CarryOutput$(x, y) = h(n)$ and $h(0) = \langle \varepsilon, \eta_0 \rangle$ and for every element n of $\mathbb{N}$ holds $h(n+1) =$ GFA0CarryOutput$(x(n+1), y(n+1), h(n))$.

The following propositions are true:

(1) Let x, y be finite sequences and f, g, h be many sorted sets indexed by $\mathbb{N}$. Suppose that

(i) $f(0) = \Sigma_0$,

(ii) $g(0) = \mathfrak{C}_0$,

(iii) $h(0) = \langle \varepsilon, \eta_0 \rangle$, and

(iv) for every element n of $\mathbb{N}$ and for every non empty many sorted signature S and for every non-empty algebra A over S and for every set z such that $S = f(n)$ and $A = g(n)$ and $z = h(n)$ holds $f(n+1) = S +\cdot \mathrm{BitGFA0Str}(x(n+1), y(n+1), z)$ and $g(n+1) = A +\cdot \mathrm{BitGFA0Circ}(x(n+1), y(n+1), z)$ and $h(n+1) = \mathrm{GFA0CarryOutput}(x(n+1), y(n+1), z)$.

Let n be an element of $\mathbb{N}$. Then n-BitGFA0Str$(x, y) = f(n)$ and n-BitGFA0Circ$(x, y) = g(n)$ and n-BitGFA0CarryOutput$(x, y) = h(n)$.

(2) For all finite sequences a, b holds 0-BitGFA0Str$(a, b) = \Sigma_0$ and 0-BitGFA0Circ$(a, b) = \mathfrak{C}_0$ and 0-BitGFA0CarryOutput$(a, b) = \langle \varepsilon, \eta_0 \rangle$.

(3) Let a, b be finite sequences and c be a set. Suppose $c = \langle \varepsilon, \eta_0 \rangle$. Then 1-BitGFA0Str$(a, b) = \Sigma_0 +\cdot \mathrm{BitGFA0Str}(a(1), b(1), c)$ and 1-BitGFA0Circ$(a, b) = \mathfrak{C}_0 +\cdot \mathrm{BitGFA0Circ}(a(1), b(1), c)$ and 1-BitGFA0CarryOutput$(a, b) = \mathrm{GFA0CarryOutput}(a(1), b(1), c)$.

(4) For all sets a, b, c such that $c = \langle \varepsilon, \eta_0 \rangle$ holds 1-BitGFA0Str$(\langle a \rangle, \langle b \rangle) = \Sigma_0 +\cdot \mathrm{BitGFA0Str}(a, b, c)$ and 1-BitGFA0Circ$(\langle a \rangle, \langle b \rangle) = \mathfrak{C}_0 +\cdot \mathrm{BitGFA0Circ}(a, b, c)$ and 1-BitGFA0CarryOutput$(\langle a \rangle, \langle b \rangle) = \mathrm{GFA0CarryOutput}(a, b, c)$.

(5) Let n be an element of $\mathbb{N}$, p, q be finite sequences with length n, and p_1, p_2, q_1, q_2 be finite sequences. Then n-BitGFA0Str$(p \frown p_1, q \frown q_1) = n$-BitGFA0Str$(p \frown p_2, q \frown q_2)$ and n-BitGFA0Circ$(p \frown p_1, q \frown q_1) = n$-BitGFA0Circ$(p \frown p_2, q \frown q_2)$ and n-BitGFA0CarryOutput$(p \frown p_1, q \frown q_1) = n$-BitGFA0CarryOutput$(p \frown p_2, q \frown q_2)$.

(6) Let n be an element of $\mathbb{N}$, x, y be finite sequences with length n, and a, b be sets. Then $(n+1)$-BitGFA0Str$(x \frown \langle a \rangle, y \frown \langle b \rangle) = (n$-BitGFA0Str$(x, y)) +\cdot \mathrm{BitGFA0Str}(a, b, n$-BitGFA0CarryOutput$(x, y))$ and
$(n+1)$-BitGFA0Circ$(x \frown \langle a \rangle, y \frown \langle b \rangle) = (n$-BitGFA0Circ$(x, y)) +\cdot$ BitGFA0Circ$(a, b, n$-BitGFA0CarryOutput$(x, y))$ and
$(n+1)$-BitGFA0CarryOutput$(x \frown \langle a \rangle, y \frown \langle b \rangle) = \mathrm{GFA0CarryOutput}(a, b, n$-BitGFA0CarryOutput$(x, y))$.

(7) Let n be an element of $\mathbb{N}$ and x, y be finite sequences. Then $(n+1)$-BitGFA0Str$(x, y) = (n$-BitGFA0Str$(x, y)) +\cdot \mathrm{BitGFA0Str}(x(n+1), y(n+1), n$-BitGFA0CarryOutput$(x, y))$ and $(n+1)$-BitGFA0Circ$(x, y) = (n$-BitGFA0Circ$(x, y)) +\cdot \mathrm{BitGFA0Circ}(x(n+1), y(n+1), n$-BitGFA0CarryOutput$(x, y))$ and $(n+1)$-BitGFA0CarryOutput$(x, y) = \mathrm{GFA0CarryOutput}(x(n+1), y(n+1), n$-BitGFA0CarryOutput$(x, y))$.

(8) For all elements n, m of $\mathbb{N}$ such that $n \leq m$ and for all finite sequences x, y holds InnerVertices$(n$-BitGFA0Str$(x, y)) \subseteq$ InnerVertices$(m$-BitGFA0Str$(x, y))$.

(9) For every element n of $\mathbb{N}$ and for all finite sequences x, y holds

InnerVertices((n+1)-BitGFA0Str(x, y)) = InnerVertices(n-BitGFA0Str(x, y))$\cup$InnerVertices(BitGFA0Str(x(n+1), y(n+1), n-BitGFA0CarryOutput (x, y))).

Let k, n be elements of $\mathbb{N}$. Let us assume that $k \geq 1$ and $k \leq n$. Let x, y be finite sequences. The functor (k, n)-BitGFA0AdderOutput(x, y) yielding an element of InnerVertices(n-BitGFA0Str(x, y)) is defined as follows:

(Def. 4) There exists an element i of $\mathbb{N}$ such that $k = i + 1$ and (k, n)-BitGFA0AdderOutput(x, y) = GFA0AdderOutput(x(k), y(k), i-BitGFA0CarryOutput(x, y)).

Next we state two propositions:

(10) For all elements n, k of $\mathbb{N}$ such that $k < n$ and for all finite sequences x, y holds ($k+1$, n)-BitGFA0AdderOutput(x, y) = GFA0AdderOutput(x($k+1$), y($k+1$), k-BitGFA0CarryOutput(x, y)).

(11) For every element n of $\mathbb{N}$ and for all finite sequences x, y holds InnerVertices(n-BitGFA0Str(x, y)) is a binary relation.

Let n be an element of $\mathbb{N}$ and let x, y be finite sequences. Observe that n-BitGFA0CarryOutput(x, y) is pair.

One can prove the following three propositions:

(12) Let f, g be nonpair yielding finite sequences and n be an element of $\mathbb{N}$. Then InputVertices((n + 1)-BitGFA0Str(f, g)) = InputVertices(n-BitGFA0Str(f, g))$\cup$(InputVertices(BitGFA0Str(f(n+1), g(n + 1), n-BitGFA0CarryOutput(f, g))) $\setminus$ {n-BitGFA0CarryOutput(f, g)}) and InnerVertices(n-BitGFA0Str(f, g)) is a binary relation and InputVertices(n-BitGFA0Str(f, g)) has no pairs.

(13) For every element n of $\mathbb{N}$ and for all nonpair yielding finite sequences x, y with length n holds InputVertices(n-BitGFA0Str(x, y)) = $\operatorname{rng} x \cup \operatorname{rng} y$.

(14) Let n be an element of $\mathbb{N}$, x, y be nonpair yielding finite sequences with length n, and s be a state of n-BitGFA0Circ(x, y). Then Following($s, 1 + 2 \cdot n$) is stable.

2. n-Bit Generalized Full Adder Circuit (TYPE-1)

Let n be a natural number and let x, y be finite sequences. The functor n-BitGFA1Str(x, y) yielding an unsplit non void strict non empty many sorted signature with arity held in gates and Boolean denotation held in gates is defined by the condition (Def. 5).

(Def. 5) There exist many sorted sets f, h indexed by $\mathbb{N}$ such that

(i) n-BitGFA1Str(x, y) = $f(n)$,

(ii) $f(0) = \Sigma_1$,

(iii) $h(0) = \langle \varepsilon, \eta_1 \rangle$, and

(iv) for every element n of $\mathbb{N}$ and for every non empty many sorted signature S and for every set z such that $S = f(n)$ and $z = h(n)$ holds $f(n+1) = S{+\cdot}\,\mathrm{BitGFA1Str}(x(n+1), y(n+1), z)$ and $h(n+1) = \mathrm{GFA1CarryOutput}(x(n+1), y(n+1), z)$.

Let n be an element of $\mathbb{N}$ and let x, y be finite sequences. The functor n-BitGFA1Circ(x, y) yielding a Boolean strict circuit of n-BitGFA1Str(x, y) with denotation held in gates is defined by the condition (Def. 6).

(Def. 6) There exist many sorted sets f, g, h indexed by $\mathbb{N}$ such that

(i) n-BitGFA1Str$(x, y) = f(n)$,

(ii) n-BitGFA1Circ$(x, y) = g(n)$,

(iii) $f(0) = \Sigma_1$,

(iv) $g(0) = \mathfrak{C}_1$,

(v) $h(0) = \langle \varepsilon, \eta_1 \rangle$, and

(vi) for every element n of $\mathbb{N}$ and for every non empty many sorted signature S and for every non-empty algebra A over S and for every set z such that $S = f(n)$ and $A = g(n)$ and $z = h(n)$ holds $f(n+1) = S{+\cdot}\,\mathrm{BitGFA1Str}(x(n+1), y(n+1), z)$ and $g(n+1) = A{+\cdot}\,\mathrm{BitGFA1Circ}(x(n+1), y(n+1), z)$ and $h(n+1) = \mathrm{GFA1CarryOutput}(x(n+1), y(n+1), z)$.

Let n be an element of $\mathbb{N}$ and let x, y be finite sequences. The functor n-BitGFA1CarryOutput(x, y) yields an element of InnerVertices(n-BitGFA1Str(x, y)) and is defined by the condition (Def. 7).

(Def. 7) There exists a many sorted set h indexed by $\mathbb{N}$ such that n-BitGFA1CarryOutput$(x, y) = h(n)$ and $h(0) = \langle \varepsilon, \eta_1 \rangle$ and for every element n of $\mathbb{N}$ holds $h(n+1) = \mathrm{GFA1CarryOutput}(x(n+1), y(n+1), h(n))$.

One can prove the following propositions:

(15) Let x, y be finite sequences and f, g, h be many sorted sets indexed by $\mathbb{N}$. Suppose that

(i) $f(0) = \Sigma_1$,

(ii) $g(0) = \mathfrak{C}_1$,

(iii) $h(0) = \langle \varepsilon, \eta_1 \rangle$, and

(iv) for every element n of $\mathbb{N}$ and for every non empty many sorted signature S and for every non-empty algebra A over S and for every set z such that $S = f(n)$ and $A = g(n)$ and $z = h(n)$ holds $f(n+1) = S{+\cdot}\,\mathrm{BitGFA1Str}(x(n+1), y(n+1), z)$ and $g(n+1) = A{+\cdot}\,\mathrm{BitGFA1Circ}(x(n+1), y(n+1), z)$ and $h(n+1) = \mathrm{GFA1CarryOutput}(x(n+1), y(n+1), z)$.

Let n be an element of $\mathbb{N}$. Then n-BitGFA1Str$(x, y) = f(n)$ and n-BitGFA1Circ$(x, y) = g(n)$ and n-BitGFA1CarryOutput$(x, y) = h(n)$.

(16) For all finite sequences a, b holds 0-BitGFA1Str(a, b) $= \Sigma_1$ and 0-BitGFA1Circ(a, b) $= \mathfrak{C}_1$ and 0-BitGFA1CarryOutput(a, b) $= \langle\varepsilon, \eta_1\rangle$.

(17) Let a, b be finite sequences and c be a set. Suppose $c = \langle\varepsilon, \eta_1\rangle$. Then 1-BitGFA1Str($a$, b) $= \Sigma_1 +\cdot$ BitGFA1Str($a(1)$, $b(1)$, c) and 1-BitGFA1Circ(a, b) $= \mathfrak{C}_1 +\cdot$ BitGFA1Circ($a(1)$, $b(1)$, c) and 1-BitGFA1CarryOutput(a, b) = GFA1CarryOutput($a(1)$, $b(1)$, c).

(18) For all sets a, b, c such that $c = \langle\varepsilon, \eta_1\rangle$ holds 1-BitGFA1Str($\langle a\rangle$, $\langle b\rangle$) $= \Sigma_1 +\cdot$ BitGFA1Str(a, b, c) and 1-BitGFA1Circ($\langle a\rangle$, $\langle b\rangle$) $= \mathfrak{C}_1 +\cdot$ BitGFA1Circ(a, b, c) and 1-BitGFA1CarryOutput($\langle a\rangle$, $\langle b\rangle$) = GFA1CarryOutput(a, b, c).

(19) Let n be an element of $\mathbb{N}$, p, q be finite sequences with length n, and p_1, p_2, q_1, q_2 be finite sequences. Then n-BitGFA1Str($p \frown p_1$, $q \frown q_1$) $=$ n-BitGFA1Str($p \frown p_2$, $q \frown q_2$) and n-BitGFA1Circ($p \frown p_1$, $q \frown q_1$) $=$ n-BitGFA1Circ($p \frown p_2$, $q \frown q_2$) and n-BitGFA1CarryOutput($p \frown p_1$, $q \frown q_1$) $=$ n-BitGFA1CarryOutput($p \frown p_2$, $q \frown q_2$).

(20) Let n be an element of $\mathbb{N}$, x, y be finite sequences with length n, and a, b be sets. Then $(n+1)$-BitGFA1Str($x \frown \langle a\rangle$, $y \frown \langle b\rangle$) $=$ (n-BitGFA1Str(x, y))$+\cdot$ BitGFA1Str(a, b, n-BitGFA1CarryOutput(x, y)) and $(n+1)$-BitGFA1Circ($x \frown \langle a\rangle$, $y \frown \langle b\rangle$) $=$ (n-BitGFA1Circ(x, y))$+\cdot$ BitGFA1Circ(a, b, n-BitGFA1CarryOutput(x, y)) and $(n+1)$-BitGFA1CarryOutput($x \frown \langle a\rangle$, $y \frown \langle b\rangle$) = GFA1CarryOutput($a$, b, n-BitGFA1CarryOutput(x, y)).

(21) Let n be an element of $\mathbb{N}$ and x, y be finite sequences. Then $(n+1)$-BitGFA1Str(x, y) $=$ (n-BitGFA1Str(x, y))$+\cdot$ BitGFA1Str($x(n+1)$, $y(n+1)$, n-BitGFA1CarryOutput(x, y)) and $(n+1)$-BitGFA1Circ(x, y) $=$ (n-BitGFA1Circ(x, y))$+\cdot$ BitGFA1Circ($x(n+1)$, $y(n+1)$, n-BitGFA1CarryOutput(x, y)) and $(n+1)$-BitGFA1CarryOutput(x, y) = GFA1CarryOutput($x(n+1)$, $y(n+1)$, n-BitGFA1CarryOutput(x, y)).

(22) For all elements n, m of $\mathbb{N}$ such that $n \leq m$ and for all finite sequences x, y holds InnerVertices(n-BitGFA1Str(x, y)) $\subseteq$ InnerVertices(m-BitGFA1Str(x, y)).

(23) For every element n of $\mathbb{N}$ and for all finite sequences x, y holds InnerVertices($(n+1)$-BitGFA1Str(x, y)) = InnerVertices(n-BitGFA1Str(x, y))$\cup$InnerVertices(BitGFA1Str($x(n+1)$, $y(n+1)$, n-BitGFA1CarryOutput(x, y))).

Let k, n be elements of $\mathbb{N}$. Let us assume that $k \geq 1$ and $k \leq n$. Let x, y be finite sequences. The functor (k, n)-BitGFA1AdderOutput(x, y) yielding an element of InnerVertices(n-BitGFA1Str(x, y)) is defined by:

(Def. 8) There exists an element i of $\mathbb{N}$ such that $k = i + 1$ and (k, n)-BitGFA1AdderOutput(x, y) $=$ GFA1AdderOutput($x(k)$, $y(k)$,

i-BitGFA1CarryOutput(x, y)).

Next we state two propositions:

(24) For all elements n, k of $\mathbb{N}$ such that $k < n$ and for all finite sequences x, y holds $(k+1, n)$-BitGFA1AdderOutput(x, y) = GFA1AdderOutput$(x(k+1), y(k+1), k$-BitGFA1CarryOutput$(x, y))$.

(25) For every element n of $\mathbb{N}$ and for all finite sequences x, y holds InnerVertices(n-BitGFA1Str(x, y)) is a binary relation.

Let n be an element of $\mathbb{N}$ and let x, y be finite sequences. One can check that n-BitGFA1CarryOutput(x, y) is pair.

We now state three propositions:

(26) Let f, g be nonpair yielding finite sequences and n be an element of $\mathbb{N}$. Then InputVertices(($n+1$)-BitGFA1Str(f, g)) = InputVertices(n-BitGFA1Str(f, g))$\cup$(InputVertices(BitGFA1Str$(f(n+1), g(n+1), n$-BitGFA1CarryOutput(f, g)))) $\setminus$ $\{n$-BitGFA1CarryOutput$(f, g)\}$) and InnerVertices(n-BitGFA1Str(f, g)) is a binary relation and InputVertices(n-BitGFA1Str(f, g)) has no pairs.

(27) For every element n of $\mathbb{N}$ and for all nonpair yielding finite sequences x, y with length n holds InputVertices(n-BitGFA1Str(x, y)) $= \operatorname{rng} x \cup \operatorname{rng} y$.

(28) Let n be an element of $\mathbb{N}$, x, y be nonpair yielding finite sequences with length n, and s be a state of n-BitGFA1Circ(x, y). Then Following$(s, 1 + 2 \cdot n)$ is stable.

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 and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Grzegorz Bancerek and Yatsuka Nakamura. Full adder circuit. Part I. *Formalized Mathematics*, 5(**3**):367–380, 1996.
[5] Grzegorz Bancerek, Shin'nosuke Yamaguchi, and Katsumi Wasaki. Full adder circuit. Part II. *Formalized Mathematics*, 10(**1**):65–71, 2002.
[6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 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] Yatsuka Nakamura and Grzegorz Bancerek. Combining of circuits. *Formalized Mathematics*, 5(**2**):283–295, 1996.
[10] Yatsuka Nakamura, Piotr Rudnicki, Andrzej Trybulec, and Pauline N. Kawamoto. Introduction to circuits, I. *Formalized Mathematics*, 5(**2**):227–232, 1996.
[11] Yatsuka Nakamura, Piotr Rudnicki, Andrzej Trybulec, and Pauline N. Kawamoto. Preliminaries to circuits, II. *Formalized Mathematics*, 5(**2**):215–220, 1996.
[12] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[13] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[14] Andrzej Trybulec. Many sorted algebras. *Formalized Mathematics*, 5(**1**):37–42, 1996.

[15] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[16] Edmund Woronowicz. Many–argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.
[17] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[18] Shin'nosuke Yamaguchi, Katsumi Wasaki, and Nobuhiro Shimoi. Generalized full adder circuits (GFAs). Part I. *Formalized Mathematics*, 13(**4**):549–571, 2005.

Received December 18, 2007

FORMALIZED MATHEMATICS
Vol. **16**, No. **1**, Pages 81–90, **2008**

Solutions of Linear Equations

Karol Pąk
Institute of Computer Science
University of Białystok
Poland

Summary. In this paper I present the Kronecker-Capelli theorem which states that a system of linear equations has a solution if and only if the rank of its coefficient matrix is equal to the rank of its augmented matrix.

MML identifier: `MATRIX15`, version: `7.8.09 4.97.1001`

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

1. Preliminaries

For simplicity, we follow the rules: x denotes a set, i, j, k, l, m, n denote natural numbers, K denotes a field, N denotes a without zero finite subset of $\mathbb{N}$, a, b denote elements of K, A, B, B_1, B_2, X, X_1, X_2 denote matrices over K, A' denotes a matrix over K of dimension $m \times n$, B' denotes a matrix over K of dimension $m \times k$, and M denotes a square matrix over K of dimension n.

We now state a number of propositions:

(1) If $\operatorname{width} A = \operatorname{len} B$, then $(a \cdot A) \cdot B = a \cdot (A \cdot B)$.

(2) $\mathbf{1}_K \cdot A = A$ and $a \cdot (b \cdot A) = (a \cdot b) \cdot A$.

(3) Let K be a non empty additive loop structure and f, g, h, w be finite sequences of elements of K. If $\operatorname{len} f = \operatorname{len} g$ and $\operatorname{len} h = \operatorname{len} w$, then $f \frown h + g \frown w = (f+g) \frown (h+w)$.

(4) Let K be a non empty multiplicative magma, f, g be finite sequences of elements of K, and a be an element of K. Then $a \cdot (f \frown g) = (a \cdot f) \frown (a \cdot g)$.

ISSN 1426–2630(p), 1898-9934(e)

(5) Let f be a function and p_1, p_2, f_1, f_2 be finite sequences. If $\operatorname{rng} p_1 \subseteq \operatorname{dom} f$ and $\operatorname{rng} p_2 \subseteq \operatorname{dom} f$ and $f_1 = f \cdot p_1$ and $f_2 = f \cdot p_2$, then $f \cdot (p_1 \frown p_2) = f_1 \frown f_2$.

(6) Let f be a finite sequence of elements of $\mathbb{N}$ and given n. Suppose f is one-to-one and $\operatorname{rng} f \subseteq \operatorname{Seg} n$ and for all i, j such that i, $j \in \operatorname{dom} f$ and $i < j$ holds $f(i) < f(j)$. Then $\operatorname{Sgm} \operatorname{rng} f = f$.

(7) Let K be an Abelian add-associative right zeroed right complementable non empty additive loop structure, p be a finite sequence of elements of K, and given i, j. Suppose i, $j \in \operatorname{dom} p$ and $i \neq j$ and for every k such that $k \in \operatorname{dom} p$ and $k \neq i$ and $k \neq j$ holds $p(k) = 0_K$. Then $\sum p = p_i + p_j$.

(8) If $i \in \operatorname{Seg} m$, then $(\operatorname{Sgm}(\operatorname{Seg}(n+m) \setminus \operatorname{Seg} n))(i) = n + i$.

(9) Let D be a non empty set, A be a matrix over D, and B_3, B_4, C_1, C_2 be without zero finite subsets of $\mathbb{N}$. Suppose $B_3 \times B_4 \subseteq$ the indices of A and $C_1 \times C_2 \subseteq$ the indices of A. Let B be a matrix over D of dimension $\operatorname{card} B_3 \times \operatorname{card} B_4$ and C be a matrix over D of dimension $\operatorname{card} C_1 \times \operatorname{card} C_2$. Suppose that for all natural numbers i, j, b_1, b_2, c_1, c_2 such that $\langle i, j \rangle \in (B_3 \times B_4) \cap (C_1 \times C_2)$ and $b_1 = (\operatorname{Sgm} B_3)^{-1}(i)$ and $b_2 = (\operatorname{Sgm} B_4)^{-1}(j)$ and $c_1 = (\operatorname{Sgm} C_1)^{-1}(i)$ and $c_2 = (\operatorname{Sgm} C_2)^{-1}(j)$ holds $B_{b_1,b_2} = C_{c_1,c_2}$. Then there exists a matrix M over D of dimension $\operatorname{len} A \times \operatorname{width} A$ such that $\operatorname{Segm}(M, B_3, B_4) = B$ and $\operatorname{Segm}(M, C_1, C_2) = C$ and for all i, j such that $\langle i, j \rangle \in (\text{the indices of } M) \setminus (B_3 \times B_4 \cup C_1 \times C_2)$ holds $M_{i,j} = A_{i,j}$.

(10) Let P, Q, Q' be without zero finite subsets of $\mathbb{N}$. Suppose $P \times Q' \subseteq$ the indices of A. Let given i, j. Suppose $i \in \operatorname{dom} A \setminus P$ and $j \in \operatorname{Seg} \operatorname{width} A \setminus Q$ and $A_{i,j} \neq 0_K$ and $Q \subseteq Q'$ and $\operatorname{Line}(A, i) \cdot \operatorname{Sgm} Q' = \operatorname{card} Q' \mapsto 0_K$. Then $\operatorname{rk}(A) > \operatorname{rk}(\operatorname{Segm}(A, P, Q))$.

(11) For every N such that $N \subseteq \operatorname{dom} A$ and for every i such that $i \in \operatorname{dom} A \setminus N$ holds $\operatorname{Line}(A, i) = \operatorname{width} A \mapsto 0_K$ holds $\operatorname{rk}(A) = \operatorname{rk}(\operatorname{Segm}(A, N, \operatorname{Seg} \operatorname{width} A))$.

(12) For every N such that $N \subseteq \operatorname{Seg} \operatorname{width} A$ and for every i such that $i \in \operatorname{Seg} \operatorname{width} A \setminus N$ holds $A_{\square,i} = \operatorname{len} A \mapsto 0_K$ holds $\operatorname{rk}(A) = \operatorname{rk}(\operatorname{Segm}(A, \operatorname{Seg} \operatorname{len} A, N))$.

(13) Let V be a vector space over K, U be a finite subset of V, u, v be vectors of V, and given a. If u, $v \in U$, then $\operatorname{Lin}((U \setminus \{u\}) \cup \{u + a \cdot v\})$ is a subspace of $\operatorname{Lin}(U)$.

(14) Let V be a vector space over K, U be a finite subset of V, u, v be vectors of V, and given a. Suppose u, $v \in U$ and if $u = v$, then $a \neq -\mathbf{1}_K$ or $u = 0_V$. Then $\operatorname{Lin}((U \setminus \{u\}) \cup \{u + a \cdot v\}) = \operatorname{Lin}(U)$.

2. Selected Properties of Joining Operation of two Matrices

Let D be a non empty set, let n, m, k be natural numbers, let A be a matrix over D of dimension $n \times m$, and let B be a matrix over D of dimension $n \times k$. Then $A \frown B$ is a matrix over D of dimension $n \times (\mathrm{width}\, A + \mathrm{width}\, B)$.

We now state a number of propositions:

(15) Let D be a non empty set, A be a matrix over D of dimension $n \times m$, B be a matrix over D of dimension $n \times k$, and given i. If $i \in \mathrm{Seg}\, n$, then $\mathrm{Line}(A \frown B, i) = \mathrm{Line}(A, i) \frown \mathrm{Line}(B, i)$.

(16) Let D be a non empty set, A be a matrix over D of dimension $n \times m$, B be a matrix over D of dimension $n \times k$, and given i. If $i \in \mathrm{Seg}\,\mathrm{width}\, A$, then $(A \frown B)_{\square, i} = A_{\square, i}$.

(17) Let D be a non empty set, A be a matrix over D of dimension $n \times m$, B be a matrix over D of dimension $n \times k$, and given i. If $i \in \mathrm{Seg}\,\mathrm{width}\, B$, then $(A \frown B)_{\square, \mathrm{width}\, A + i} = B_{\square, i}$.

(18) Let D be a non empty set, A be a matrix over D of dimension $n \times m$, B be a matrix over D of dimension $n \times k$, and p_3, p_4 be finite sequences of elements of D. If $\mathrm{len}\, p_3 = \mathrm{width}\, A$ and $\mathrm{len}\, p_4 = \mathrm{width}\, B$, then $\mathrm{ReplaceLine}(A \frown B, i, p_3 \frown p_4) = (\mathrm{ReplaceLine}(A, i, p_3)) \frown \mathrm{ReplaceLine}(B, i, p_4)$.

(19) Let D be a non empty set, A be a matrix over D of dimension $n \times m$, and B be a matrix over D of dimension $n \times k$. Then $\mathrm{Segm}(A \frown B, \mathrm{Seg}\, n, \mathrm{Seg}\,\mathrm{width}\, A) = A$ and $\mathrm{Segm}(A \frown B, \mathrm{Seg}\, n, \mathrm{Seg}(\mathrm{width}\, A + \mathrm{width}\, B) \setminus \mathrm{Seg}\,\mathrm{width}\, A) = B$.

(20) For all matrices A, B over K such that $\mathrm{len}\, A = \mathrm{len}\, B$ holds $\mathrm{rk}(A) \leq \mathrm{rk}(A \frown B)$ and $\mathrm{rk}(B) \leq \mathrm{rk}(A \frown B)$.

(21) For all matrices A, B over K such that $\mathrm{len}\, A = \mathrm{len}\, B$ and $\mathrm{len}\, A = \mathrm{rk}(A)$ holds $\mathrm{rk}(A) = \mathrm{rk}(A \frown B)$.

(22) For all matrices A, B over K such that $\mathrm{len}\, A = \mathrm{len}\, B$ and $\mathrm{width}\, A = 0$ holds $A \frown B = B$ and $B \frown A = B$.

(23) For all matrices A, B over K such that $B = 0_K^{(\mathrm{len}\, A) \times m}$ holds $\mathrm{rk}(A) = \mathrm{rk}(A \frown B)$.

(24) Let A, B be matrices over K. Suppose $\mathrm{rk}(A) = \mathrm{rk}(A \frown B)$ and $\mathrm{len}\, A = \mathrm{len}\, B$. Let given N. Suppose $N \subseteq \mathrm{dom}\, A$ and for every i such that $i \in N$ holds $\mathrm{Line}(A, i) = \mathrm{width}\, A \mapsto 0_K$. Let given i. If $i \in N$, then $\mathrm{Line}(B, i) = \mathrm{width}\, B \mapsto 0_K$.

3. Basic Properties of two Transformations which Transform Finite Sequences to Matrices

For simplicity, we follow the rules: D is a non empty set, b_3 is a finite sequence of elements of D, b, f, g are finite sequences of elements of K, and M_1 is a matrix over D.

Let D be a non empty set and let b be a finite sequence of elements of D. The functor $\mathrm{LineVec2Mx}\, b$ yielding a matrix over D of dimension $1 \times \mathrm{len}\, b$ is defined by:

(Def. 1) $\mathrm{LineVec2Mx}\, b = \langle b \rangle$.

The functor $\mathrm{ColVec2Mx}\, b$ yielding a matrix over D of dimension $\mathrm{len}\, b \times 1$ is defined by:

(Def. 2) $\mathrm{ColVec2Mx}\, b = \langle b \rangle^{\mathrm{T}}$.

One can prove the following propositions:

(25) $M_1 = \mathrm{LineVec2Mx}\, b_3$ iff $\mathrm{Line}(M_1, 1) = b_3$ and $\mathrm{len}\, M_1 = 1$.

(26) If $\mathrm{len}\, M_1 \neq 0$ or $\mathrm{len}\, b_3 \neq 0$, then $M_1 = \mathrm{ColVec2Mx}\, b_3$ iff $(M_1)_{\square,1} = b_3$ and $\mathrm{width}\, M_1 = 1$.

(27) If $\mathrm{len}\, f = \mathrm{len}\, g$, then $\mathrm{LineVec2Mx}\, f + \mathrm{LineVec2Mx}\, g = \mathrm{LineVec2Mx}(f + g)$.

(28) If $\mathrm{len}\, f = \mathrm{len}\, g$, then $\mathrm{ColVec2Mx}\, f + \mathrm{ColVec2Mx}\, g = \mathrm{ColVec2Mx}(f + g)$.

(29) $a \cdot \mathrm{LineVec2Mx}\, f = \mathrm{LineVec2Mx}(a \cdot f)$.

(30) $a \cdot \mathrm{ColVec2Mx}\, f = \mathrm{ColVec2Mx}(a \cdot f)$.

(31) $\mathrm{LineVec2Mx}(k \mapsto 0_K) = 0_K^{1 \times k}$.

(32) $\mathrm{ColVec2Mx}(k \mapsto 0_K) = 0_K^{k \times 1}$.

4. Basis Properties of the Solution of Linear Equations

Let us consider K and let us consider A, B. The set of solutions of A and B is a set and is defined as follows:

(Def. 3) The set of solutions of A and $B = \{X : \mathrm{len}\, X = \mathrm{width}\, A \ \wedge\ \mathrm{width}\, X = \mathrm{width}\, B \ \wedge\ A \cdot X = B\}$.

We now state a number of propositions:

(33) If the set of solutions of A and B is non empty, then $\mathrm{len}\, A = \mathrm{len}\, B$.

(34) If $X \in$ the set of solutions of A and B and $i \in \mathrm{Seg}\,\mathrm{width}\, X$ and $X_{\square,i} = \mathrm{len}\, X \mapsto 0_K$, then $B_{\square,i} = \mathrm{len}\, B \mapsto 0_K$.

(35) Suppose $X \in$ the set of solutions of A and B. Then $a \cdot X \in$ the set of solutions of A and $a \cdot B$ and $X \in$ the set of solutions of $a \cdot A$ and $a \cdot B$.

(36) If $a \neq 0_K$, then the set of solutions of A and $B =$ the set of solutions of $a \cdot A$ and $a \cdot B$.

(37) Suppose $X_1 \in$ the set of solutions of A and B_1 and $X_2 \in$ the set of solutions of A and B_2 and width $B_1 =$ width B_2. Then $X_1 + X_2 \in$ the set of solutions of A and $B_1 + B_2$.

(38) If $X \in$ the set of solutions of A' and B', then $X \in$ the set of solutions of $\mathrm{RLine}(A', i, a \cdot \mathrm{Line}(A', i))$ and $\mathrm{RLine}(B', i, a \cdot \mathrm{Line}(B', i))$.

(39) Suppose $X \in$ the set of solutions of A' and B' and $j \in \mathrm{Seg}\, m$ and $i \neq j$. Then $X \in$ the set of solutions of $\mathrm{RLine}(A', i, \mathrm{Line}(A', i) + a \cdot \mathrm{Line}(A', j))$ and $\mathrm{RLine}(B', i, \mathrm{Line}(B', i) + a \cdot \mathrm{Line}(B', j))$.

(40) Suppose $j \in \mathrm{Seg}\, m$ and if $i = j$, then $a \neq -\mathbf{1}_K$. Then the set of solutions of A' and $B' =$ the set of solutions of $\mathrm{RLine}(A', i, \mathrm{Line}(A', i) + a \cdot \mathrm{Line}(A', j))$ and $\mathrm{RLine}(B', i, \mathrm{Line}(B', i) + a \cdot \mathrm{Line}(B', j))$.

(41) If $X \in$ the set of solutions of A and B and $i \in \mathrm{dom}\, A$ and $\mathrm{Line}(A, i) = \mathrm{width}\, A \mapsto 0_K$, then $\mathrm{Line}(B, i) = \mathrm{width}\, B \mapsto 0_K$.

(42) Let n_1 be an element of $\mathbb{N}^n$. Suppose $\mathrm{rng}\, n_1 \subseteq \mathrm{dom}\, A$ and $n > 0$. Then the set of solutions of A and $B \subseteq$ the set of solutions of $\mathrm{Segm}(A, n_1, \mathrm{Sgm}\,\mathrm{Seg}\,\mathrm{width}\, A)$ and $\mathrm{Segm}(B, n_1, \mathrm{Sgm}\,\mathrm{Seg}\,\mathrm{width}\, B)$.

(43) Let n_1 be an element of $\mathbb{N}^n$. Suppose $\mathrm{rng}\, n_1 \subseteq \mathrm{dom}\, A = \mathrm{dom}\, B$ and $n > 0$ and for every i such that $i \in \mathrm{dom}\, A \setminus \mathrm{rng}\, n_1$ holds $\mathrm{Line}(A, i) = \mathrm{width}\, A \mapsto 0_K$ and $\mathrm{Line}(B, i) = \mathrm{width}\, B \mapsto 0_K$. Then the set of solutions of A and $B =$ the set of solutions of $\mathrm{Segm}(A, n_1, \mathrm{Sgm}\,\mathrm{Seg}\,\mathrm{width}\, A)$ and $\mathrm{Segm}(B, n_1, \mathrm{Sgm}\,\mathrm{Seg}\,\mathrm{width}\, B)$.

(44) Let given N. Suppose $N \subseteq \mathrm{dom}\, A$ and N is non empty. Then the set of solutions of A and $B \subseteq$ the set of solutions of $\mathrm{Segm}(A, N, \mathrm{Seg}\,\mathrm{width}\, A)$ and $\mathrm{Segm}(B, N, \mathrm{Seg}\,\mathrm{width}\, B)$.

(45) Let given N. Suppose $N \subseteq \mathrm{dom}\, A$ and N is non empty and $\mathrm{dom}\, A = \mathrm{dom}\, B$ and for every i such that $i \in \mathrm{dom}\, A \setminus N$ holds $\mathrm{Line}(A, i) = \mathrm{width}\, A \mapsto 0_K$ and $\mathrm{Line}(B, i) = \mathrm{width}\, B \mapsto 0_K$. Then the set of solutions of A and $B =$ the set of solutions of $\mathrm{Segm}(A, N, \mathrm{Seg}\,\mathrm{width}\, A)$ and $\mathrm{Segm}(B, N, \mathrm{Seg}\,\mathrm{width}\, B)$.

(46) Suppose $i \in \mathrm{dom}\, A$ and $\mathrm{len}\, A > 1$. Then the set of solutions of A and $B \subseteq$ the set of solutions of the deleting of i-row in A and the deleting of i -row in B.

(47) Let given A, B, i. Suppose $i \in \mathrm{dom}\, A$ and $\mathrm{len}\, A > 1$ and $\mathrm{Line}(A, i) = \mathrm{width}\, A \mapsto 0_K$ and $i \in \mathrm{dom}\, B$ and $\mathrm{Line}(B, i) = \mathrm{width}\, B \mapsto 0_K$. Then the set of solutions of A and $B =$ the set of solutions of the deleting of i-row in A and the deleting of i -row in B.

(48) Let A be a matrix over K of dimension $n \times m$, B be a matrix over K of dimension $n \times k$, and P be a function from $\mathrm{Seg}\, n$ into $\mathrm{Seg}\, n$. Then

(i) the set of solutions of A and $B \subseteq$ the set of solutions of $A \cdot P$ and $B \cdot P$, and

(ii) if P is one-to-one, then the set of solutions of A and B = the set of solutions of $A \cdot P$ and $B \cdot P$.

(49) Let A be a matrix over K of dimension $n \times m$ and given N. Suppose $\operatorname{card} N = n$ and $N \subseteq \operatorname{Seg} m$ and $\operatorname{Segm}(A, \operatorname{Seg} n, N) = I_K^{n \times n}$ and $n > 0$. Then there exists a matrix M_2 over K of dimension $m -' n \times m$ such that

(i) $\operatorname{Segm}(M_2, \operatorname{Seg}(m -' n), \operatorname{Seg} m \setminus N) = I_K^{(m-'n)\times(m-'n)}$,

(ii) $\operatorname{Segm}(M_2, \operatorname{Seg}(m -' n), N) = -(\operatorname{Segm}(A, \operatorname{Seg} n, \operatorname{Seg} m \setminus N))^{\mathrm{T}}$, and

(iii) for every l and for every matrix M over K of dimension $m \times l$ such that for every i such that $i \in \operatorname{Seg} l$ holds there exists j such that $j \in \operatorname{Seg}(m -' n)$ and $M_{\square,i} = \operatorname{Line}(M_2, j)$ or $M_{\square,i} = m \mapsto 0_K$ holds $M \in$ the set of solutions of A and $0_K^{n \times l}$.

(50) Let A be a matrix over K of dimension $n \times m$, B be a matrix over K of dimension $n \times l$, and given N. Suppose $\operatorname{card} N = n$ and $N \subseteq \operatorname{Seg} m$ and $n > 0$ and $\operatorname{Segm}(A, \operatorname{Seg} n, N) = I_K^{n \times n}$. Then there exists a matrix X over K of dimension $m \times l$ such that $\operatorname{Segm}(X, \operatorname{Seg} m \setminus N, \operatorname{Seg} l) = 0_K^{(m-'n)\times l}$ and $\operatorname{Segm}(X, N, \operatorname{Seg} l) = B$ and $X \in$ the set of solutions of A and B.

(51) Let A be a matrix over K of dimension $0 \times n$ and B be a matrix over K of dimension $0 \times m$. Then the set of solutions of A and $B = \{\emptyset\}$.

(52) For every matrix B over K such that the set of solutions of $0_K^{n \times k}$ and B is non empty holds $B = 0_K^{n \times (\operatorname{width} B)}$.

(53) Let A be a matrix over K of dimension $n \times k$ and B be a matrix over K of dimension $n \times m$. Suppose $n > 0$. Suppose $x \in$ the set of solutions of A and B. Then x is a matrix over K of dimension $k \times m$.

(54) Suppose $n > 0$ and $k > 0$. Then the set of solutions of $0_K^{n \times k}$ and $0_K^{n \times m} = \{X : X$ ranges over matrices over K of dimension $k \times m\}$.

(55) If $n > 0$ and the set of solutions of $0_K^{n \times 0}$ and $0_K^{n \times m}$ is non empty, then $m = 0$.

(56) The set of solutions of $0_K^{n \times 0}$ and $0_K^{n \times 0} = \{\emptyset\}$.

5. Gaussian Eliminations

In this article we present several logical schemes. The scheme *GAUSS1* deals with a field $\mathcal{A}$, natural numbers $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, a matrix $\mathcal{E}$ over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{C}$, a matrix $\mathcal{F}$ over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{D}$, a 4-ary functor $\mathcal{F}$ yielding a matrix over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{D}$, and a binary predicate $\mathcal{P}$, and states that:

> There exists a matrix A' over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{C}$ and there exists a matrix B' over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{D}$ and there exists a without zero finite subset N of $\mathbb{N}$ such that
>
> $N \subseteq \operatorname{Seg} \mathcal{C}$ and $\operatorname{rk}(\mathcal{E}) = \operatorname{rk}(A')$ and $\operatorname{rk}(\mathcal{E}) = \operatorname{card} N$ and $\mathcal{P}[A', B']$ and $\operatorname{Segm}(A', \operatorname{Seg} \operatorname{card} N, N)$ is diagonal and for every i

such that $i \in \operatorname{Seg}\operatorname{card} N$ holds $A'_{i,(\operatorname{Sgm} N)_i} \neq 0_{\mathcal{A}}$ and for every i such that $i \in \operatorname{dom} A'$ and $i > \operatorname{card} N$ holds $\operatorname{Line}(A', i) = \mathcal{C} \mapsto 0_{\mathcal{A}}$ and for all i, j such that $i \in \operatorname{Seg}\operatorname{card} N$ and $j \in \operatorname{Seg}\operatorname{width} A'$ and $j < (\operatorname{Sgm} N)(i)$ holds $A'_{i,j} = 0_{\mathcal{A}}$

provided the parameters meet the following requirements:

- $\mathcal{P}[\mathcal{E}, \mathcal{F}]$, and
- Let A' be a matrix over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{C}$ and B' be a matrix over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{D}$. Suppose $\mathcal{P}[A', B']$. Let given i, j. Suppose $i \neq j$ and $j \in \operatorname{dom} A'$. Let a be an element of $\mathcal{A}$. Then $\mathcal{P}[\operatorname{RLine}(A', i, \operatorname{Line}(A', i) + a \cdot \operatorname{Line}(A', j)), \mathcal{F}(B', i, j, a)]$.

The scheme *GAUSS2* deals with a field $\mathcal{A}$, natural numbers $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, a matrix $\mathcal{E}$ over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{C}$, a matrix $\mathcal{F}$ over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{D}$, a 4-ary functor $\mathcal{F}$ yielding a matrix over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{D}$, and a binary predicate $\mathcal{P}$, and states that:

There exists a matrix A' over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{C}$ and there exists a matrix B' over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{D}$ and there exists a without zero finite subset N of $\mathbb{N}$ such that

$N \subseteq \operatorname{Seg}\mathcal{C}$ and $\operatorname{rk}(\mathcal{E}) = \operatorname{rk}(A')$ and $\operatorname{rk}(\mathcal{E}) = \operatorname{card} N$ and $\mathcal{P}[A', B']$ and $\operatorname{Segm}(A', \operatorname{Seg}\operatorname{card} N, N) = I_{\mathcal{A}}^{\operatorname{card} N \times \operatorname{card} N}$ and for every i such that $i \in \operatorname{dom} A'$ and $i > \operatorname{card} N$ holds $\operatorname{Line}(A', i) = \mathcal{C} \mapsto 0_{\mathcal{A}}$ and for all i, j such that $i \in \operatorname{Seg}\operatorname{card} N$ and $j \in \operatorname{Seg}\operatorname{width} A'$ and $j < (\operatorname{Sgm} N)(i)$ holds $A'_{i,j} = 0_{\mathcal{A}}$

provided the parameters satisfy the following conditions:

- $\mathcal{P}[\mathcal{E}, \mathcal{F}]$, and
- Let A' be a matrix over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{C}$ and B' be a matrix over $\mathcal{A}$ of dimension $\mathcal{B} \times \mathcal{D}$. Suppose $\mathcal{P}[A', B']$. Let a be an element of $\mathcal{A}$ and given i, j. If $j \in \operatorname{dom} A'$ and if $i = j$, then $a \neq -\mathbf{1}_{\mathcal{A}}$, then $\mathcal{P}[\operatorname{RLine}(A', i, \operatorname{Line}(A', i) + a \cdot \operatorname{Line}(A', j)), \mathcal{F}(B', i, j, a)]$.

6. The Main Theorem

We now state the proposition

(57) Let A, B be matrices over K. Suppose $\operatorname{len} A = \operatorname{len} B$ and if $\operatorname{width} A = 0$, then $\operatorname{width} B = 0$. Then $\operatorname{rk}(A) = \operatorname{rk}(A \frown B)$ if and only if the set of solutions of A and B is non empty.

7. Space of Solutions of Linear Equations

Let us consider K, let A be a matrix over K, and let b be a finite sequence of elements of K. The set of solutions of A and b is defined by:

(Def. 4) The set of solutions of A and $b = \{f : \mathrm{ColVec2Mx}\, f \in$ the set of solutions of A and $\mathrm{ColVec2Mx}\, b\}$.

We now state two propositions:

(58) For every x such that $x \in$ the set of solutions of A and $\mathrm{ColVec2Mx}\, b$ there exists f such that $x = \mathrm{ColVec2Mx}\, f$ and $\mathrm{len}\, f = \mathrm{width}\, A$.

(59) For every f such that $\mathrm{ColVec2Mx}\, f \in$ the set of solutions of A and $\mathrm{ColVec2Mx}\, b$ holds $\mathrm{len}\, f = \mathrm{width}\, A$.

Let us consider K, let A be a matrix over K, and let b be a finite sequence of elements of K. Then the set of solutions of A and b is a subset of the width A-dimension vector space over K.

Let us consider K, let A be a matrix over K, and let k be an element of $\mathbb{N}$. Note that the set of solutions of A and $k \mapsto 0_K$ is linearly closed.

We now state two propositions:

(60) If the set of solutions of A and b is non empty and $\mathrm{width}\, A = 0$, then $\mathrm{len}\, A = 0$.

(61) If $\mathrm{width}\, A \neq 0$ or $\mathrm{len}\, A = 0$, then the set of solutions of A and $\mathrm{len}\, A \mapsto 0_K$ is non empty.

Let us consider K and let A be a matrix over K. Let us assume that if $\mathrm{width}\, A = 0$, then $\mathrm{len}\, A = 0$. The space of solutions of A is a strict subspace of the width A-dimension vector space over K and is defined by:

(Def. 5) The carrier of the space of solutions of $A =$ the set of solutions of A and $\mathrm{len}\, A \mapsto 0_K$.

The following propositions are true:

(62) Let A be a matrix over K and b be a finite sequence of elements of K. Suppose the set of solutions of A and b is non empty. Then the set of solutions of A and b is a coset of the space of solutions of A.

(63) Let given A. Suppose if $\mathrm{width}\, A = 0$, then $\mathrm{len}\, A = 0$ and $\mathrm{rk}(A) = 0$. Then the space of solutions of $A =$ the width A-dimension vector space over K.

(64) For every A such that the space of solutions of $A =$ the width A-dimension vector space over K holds $\mathrm{rk}(A) = 0$.

(65) Let given i, j. Suppose $j \in \mathrm{Seg}\, m$ and $n > 0$ and if $i = j$, then $a \neq -\mathbf{1}_K$. Then the space of solutions of $A' =$ the space of solutions of $\mathrm{RLine}(A', i, \mathrm{Line}(A', i) + a \cdot \mathrm{Line}(A', j))$.

(66) Let given N. Suppose $N \subseteq \mathrm{dom}\, A$ and N is non empty and $\mathrm{width}\, A > 0$ and for every i such that $i \in \mathrm{dom}\, A \setminus N$ holds $\mathrm{Line}(A, i) = \mathrm{width}\, A \mapsto 0_K$. Then the space of solutions of $A =$ the space of solutions of $\mathrm{Segm}(A, N, \mathrm{Seg}\,\mathrm{width}\, A)$.

(67) Let A be a matrix over K of dimension $n \times m$ and given N. Suppose $\mathrm{card}\, N = n$ and $N \subseteq \mathrm{Seg}\, m$ and $\mathrm{Segm}(A, \mathrm{Seg}\, n, N) = I_K^{n \times n}$ and $n > 0$

and $m -' n > 0$. Then there exists a matrix M_2 over K of dimension $m -' n \times m$ such that $\mathrm{Segm}(M_2, \mathrm{Seg}(m -' n), \mathrm{Seg}\, m \setminus N) = I_K^{(m-'n)\times(m-'n)}$ and $\mathrm{Segm}(M_2, \mathrm{Seg}(m -' n), N) = -(\mathrm{Segm}(A, \mathrm{Seg}\, n, \mathrm{Seg}\, m \setminus N))^{\mathrm{T}}$ and $\mathrm{Lin}(\mathrm{lines}(M_2)) =$ the space of solutions of A.

(68) For every A such that if $\mathrm{width}\, A = 0$, then $\mathrm{len}\, A = 0$ holds dim(the space of solutions of A) $= \mathrm{width}\, A - \mathrm{rk}(A)$.

(69) Let M be a matrix over K of dimension $n \times m$ and given i, j, a. Suppose M is without repeated line and $j \in \mathrm{dom}\, M$ and if $i = j$, then $a \neq -\mathbf{1}_K$. Then $\mathrm{Lin}(\mathrm{lines}(M)) = \mathrm{Lin}(\mathrm{lines}(\mathrm{RLine}(M, i, \mathrm{Line}(M, i) + a \cdot \mathrm{Line}(M, j))))$.

(70) Let W be a subspace of the m-dimension vector space over K. Then there exists a matrix A over K of dimension $\dim(W) \times m$ and there exists a without zero finite subset N of $\mathbb{N}$ such that $N \subseteq \mathrm{Seg}\, m$ and $\dim(W) = \mathrm{card}\, N$ and $\mathrm{Segm}(A, \mathrm{Seg}\dim(W), N) = I_K^{\dim(W)\times\dim(W)}$ and $\mathrm{rk}(A) = \dim(W)$ and $\mathrm{lines}(A)$ is a basis of W.

(71) Let W be a strict subspace of the m-dimension vector space over K. Suppose $\dim(W) < m$. Then there exists a matrix A over K of dimension $m -' \dim(W) \times m$ and there exists a without zero finite subset N of $\mathbb{N}$ such that $\mathrm{card}\, N = m -' \dim(W)$ and $N \subseteq \mathrm{Seg}\, m$ and $\mathrm{Segm}(A, \mathrm{Seg}(m -' \dim(W)), N) = I_K^{(m-'\dim(W))\times(m-'\dim(W))}$ and $W =$ the space of solutions of A.

(72) Let A, B be matrices over K. Suppose $\mathrm{width}\, A = \mathrm{len}\, B$ and if $\mathrm{width}\, A = 0$, then $\mathrm{len}\, A = 0$ and if $\mathrm{width}\, B = 0$, then $\mathrm{len}\, B = 0$. Then the space of solutions of B is a subspace of the space of solutions of $A \cdot B$.

(73) For all matrices A, B over K such that $\mathrm{width}\, A = \mathrm{len}\, B$ holds $\mathrm{rk}(A \cdot B) \leq \mathrm{rk}(A)$ and $\mathrm{rk}(A \cdot B) \leq \mathrm{rk}(B)$.

(74) Let A be a matrix over K of dimension $n \times n$ and B be a matrix over K. Suppose $\mathrm{Det}\, A \neq 0_K$ and $\mathrm{width}\, A = \mathrm{len}\, B$ and if $\mathrm{width}\, B = 0$, then $\mathrm{len}\, B = 0$. Then the space of solutions of $B =$ the space of solutions of $A \cdot B$.

(75) Let A be a matrix over K of dimension $n \times n$ and B be a matrix over K. If $\mathrm{width}\, A = \mathrm{len}\, B$ and $\mathrm{Det}\, A \neq 0_K$, then $\mathrm{rk}(A \cdot B) = \mathrm{rk}(B)$.

(76) Let A be a matrix over K of dimension $n \times n$ and B be a matrix over K. If $\mathrm{len}\, A = \mathrm{width}\, B$ and $\mathrm{Det}\, A \neq 0_K$, then $\mathrm{rk}(B \cdot A) = \mathrm{rk}(B)$.

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

[4] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.

[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 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] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[11] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.
[12] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Formalized Mathematics*, 2(**5**):711–717, 1991.
[13] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[14] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(**3**):339–345, 1996.
[15] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[16] Karol Pąk. Basic properties of determinants of square matrices over a field. *Formalized Mathematics*, 15(**1**):17–25, 2007.
[17] Karol Pąk. Basic properties of the rank of matrices over a field. *Formalized Mathematics*, 15(**4**):199–211, 2007.
[18] Karol Pąk and Andrzej Trybulec. Laplace expansion. *Formalized Mathematics*, 15(**3**):143–150, 2007.
[19] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[20] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 1990.
[21] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[22] Wojciech A. Trybulec. Subspaces and cosets of subspaces in vector space. *Formalized Mathematics*, 1(**5**):865–870, 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 and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[26] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.
[27] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.
[28] Mariusz Żynel. The Steinitz theorem and the dimension of a vector space. *Formalized Mathematics*, 5(**3**):423–428, 1996.

Received December 18, 2007

FORMALIZED MATHEMATICS
Volume **16**, Number **1**, **2008**

Addenda

We have the pleasure of making a new volume of *Formalized Mathematics* available to a wider audience. This volume includes articles accepted to the Mizar Mathematical Library (MML) from October 2007 to September 2008 (with one exception – July 2007). The total number of articles published in the four issues of this volume is 48 (12, 15, 7, and 14). They were written by 40 authors from 6 countries: Japan (18 articles), China (13), Poland (12), Italy (2), USA (2), and Canada (1).

Each issue in addition to the previous issues includes an Addenda with a table of changes in notation, an index of authors, and an index of MML identifiers.

Grzegorz Bancerek
Scientific Editor

Changes in notation

Concept name	**old notation**	**new notation**
Cartesian product of two sets	$[\!: A, B :\!]$	$A \times B$
Cartesian product of three sets	$[\!: A, B, C :\!]$	$A \times B \times C$
Affine map	$\mathrm{AffineMap}(a, b)$	$a\square + b$
Forward difference	$\mathrm{fD}(f, h)$	$\Delta_h[f]$
Backward difference	$\mathrm{bD}(f, h)$	$\nabla_h[f]$
Central difference	$\mathrm{cD}(f, h)$	$\delta_h[f]$
Forward difference sequence	$\mathrm{fdif}(f, h)$	$\vec{\Delta}_h[f]$
Backward difference sequence	$\mathrm{bdif}(f, h)$	$\vec{\nabla}_h[f]$
Central difference sequence	$\mathrm{cdif}(f, h)$	$\vec{\delta}_h[f]$
Difference	$\Delta(f, x, y)$	$\Delta[f](x, y)$
Difference	$[!f, x, y, z!]$	$\Delta[f](x, y, z)$
Difference	$[!f, x, y, z, v!]$	$\Delta[f](x, y, z, v)$
Identity matrix of size n over K	$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n\times n}_{K}$	$I^{n\times n}_{K}$
Zero matrix of size $n \times m$ over K	$\begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}^{n\times m}_{K}$	$0^{n\times m}_{K}$

ISSN 1426–2630(p), 1898-9934(e)

Number sets

$\mathbb{N}$ - the set of natural numbers
$\omega = \mathbb{N}$ - the set of finite ordinal numbers
$\mathbb{Z}$ - the set of integer numbers
$\mathbb{Q}$ - the set of rational numbers
$\mathbb{R}$ - the set of real numbers
$\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ - the set of extended real numbers
$\mathbb{C}$ - the set of complex numbers

Authors

MML Identifiers