Contents

Formaliz. Math. 20 (**4**)

FORMALIZED MATHEMATICS
Vol. 20, No. 4, Pages 257–263, 2012
DOI: 10.2478/v10037-012-0030-0

VERSITA
versita.com/fm/

Posterior Probability on Finite Set[1]

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. In [14] we formalized probability and probability distribution on a finite sample space. In this article first we propose a formalization of the class of finite sample spaces whose element's probability distributions are equivalent with each other. Next, we formalize the probability measure of the class of sample spaces we have formalized above. Finally, we formalize the sampling and posterior probability.

MML identifier: DIST_2, version: 8.0.01 5.3.1162

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

1. Equivalent Distributed Finite and Distributed Sample Spaces

The following propositions are true:

(1) Let Y be a non empty finite set and s be a finite sequence of elements of Y. If $Y = \{1\}$ and $s = \langle 1 \rangle$, then FDprobSEQ $s = \langle 1 \rangle$.

(2) Let S be a non empty finite set, p be a probability distribution finite sequence on S, and s be a finite sequence of elements of S. If FDprobSEQ $s = p$, then $\mathrm{distribution}(p, S) =$ the equivalence class of s and $s \in \mathrm{distribution}(p, S)$.

(3) Let S be a non empty finite set and x be an element of S. Then $x \in \mathrm{rng}\,\mathrm{CFS}(S)$ and there exists a natural number n such that $n \in \mathrm{dom}\,\mathrm{CFS}(S)$ and $x = (\mathrm{CFS}(S))(n)$ and $n \in \mathrm{Seg}\,\overline{\overline{S}}$.

[1]This work is supported by JSPS KAKENHI 21240001.

ISSN 1426–2630(p), 1898-9934(e)

Let S be a non empty finite set. One can check that every non empty finite set is non empty.

Let S be a non empty finite set and let D be an element of the distribution family of S. We see that the element of D is a finite sequence of elements of S.

One can prove the following proposition

(4) Let S be a non empty finite set, D be an element of the distribution family of S, and s, t be elements of D. Then s and t are probability equivalent.

Let S be a non empty finite set and let D be an element of the distribution family of S. We introduce D is well distributed as a synonym of D has non empty elements.

We now state the proposition

(5) Let S be a non empty finite set and s be a finite sequence of elements of S. Then for every set x holds $\mathrm{Prob}_{\mathrm{D}}(x, s) = 0$ if and only if s is empty.

Let S be a non empty finite set. Observe that every non empty finite set which is well distributed

We now state the proposition

(6) Let S be a non empty finite set and D be an element of the distribution family of S. Then D is not well distributed if and only if $D = \{\varepsilon_S\}$.

Let S be a non empty finite set. An equivalent distributed sample spaces family of S is a well distributed element of the distribution family of S.

Let S be a non empty finite set. One can verify that the uniform distribution S is well distributed.

One can prove the following proposition

(7) Let S be a non empty finite set and D be an equivalent distributed sample spaces family of S. Then $(\mathrm{GenProbSEQ}\, S)(D)$ is a probability distribution finite sequence on S.

2. Probability Measure of Equivalent Distributed Finite and Distributed Sample Spaces

Let S be a non empty finite set and let a be an element of S. The functor $|\bullet : a|_{\mathbb{N}}$ yielding an element of $\mathbb{N}$ is defined by:

(Def. 1) $|\bullet : a|_{\mathbb{N}} = a \hookleftarrow \mathrm{CFS}(S)$.

Let S be a non empty finite set and let D be an equivalent distributed sample spaces family of S. The probability finite sequence of D yields a probability distribution finite sequence on S and is defined by:

(Def. 2) The probability finite sequence of $D = (\mathrm{GenProbSEQ}\, S)(D)$.

Let j_1 be a *Boolean*-valued function. The true event of j_1 yielding an event of $\mathrm{dom}\, j_1$ is defined as follows:

(Def. 3) The true event of $j_1 = {j_1}^{-1}(\{true\})$.

The following proposition is true

(8) Let S be a non empty finite set, f be an S-valued function, and j_1 be a function from S into *Boolean*. Then the true event of $j_1 \cdot f$ is an event of $\operatorname{dom} f$.

Let S be a non empty finite set, let D be an equivalent distributed sample spaces family of S, let s be an element of D, and let j_1 be a function from S into *Boolean*. The functor $\operatorname{Prob}(j_1, s)$ yielding a real number is defined as follows:

(Def. 4) $\operatorname{Prob}(j_1, s) = \frac{\overline{\overline{\text{the true event of } j_1 \cdot s}}}{\operatorname{len} s}$.

The following propositions are true:

(9) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, s be an element of D, j_1 be a function from S into *Boolean*, F be a non empty finite set, and E be an event of F. If $F = \operatorname{dom} s$ and $E =$ the true event of $j_1 \cdot s$, then $\operatorname{Prob}(j_1, s) = \mathrm{P}(E)$.

(10) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, a be an element of S, s be an element of D, and j_1 be a function from S into *Boolean*. If for every set x holds $x = a$ iff $j_1(x) = true$, then $\operatorname{Prob}(j_1, s) = \operatorname{Prob}_{\mathrm{D}}(a, s)$.

Let S be a set, let s be a finite sequence of elements of S, and let A be a subset of $\operatorname{dom} s$. The functor $\operatorname{extract}(s, A)$ yielding a finite sequence of elements of S is defined by:

(Def. 5) $\operatorname{extract}(s, A) = s \cdot \operatorname{CFS}(A)$.

We now state several propositions:

(11) Let S be a set, s be a finite sequence of elements of S, and A be a subset of $\operatorname{dom} s$. Then $\operatorname{len} \operatorname{extract}(s, A) = \overline{\overline{A}}$ and for every natural number i such that $i \in \operatorname{dom} \operatorname{extract}(s, A)$ holds $(\operatorname{extract}(s, A))(i) = s((\operatorname{CFS}(A))(i))$.

(12) Let S be a non empty finite set, s be a finite sequence of elements of S, A be a subset of $\operatorname{dom} s$, and f be a function. If $f = \operatorname{CFS}(A)$, then $\operatorname{extract}(s, A) \cdot f^{-1} = s \restriction A$.

(13) Let S be a non empty finite set, f be an S-valued function, j_1 be a function from S into *Boolean*, and n be a set. Suppose $n \in \operatorname{dom} f$. Then $n \in$ the true event of $j_1 \cdot f$ if and only if $f(n) \in$ the true event of j_1.

(14) Let S be a non empty finite set, f be an S-valued function, and j_1 be a function from S into *Boolean*. Then the true event of $j_1 \cdot f = f^{-1}$(the true event of j_1).

(15) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, s be an element of D, and j_1 be a function from S into *Boolean*. Then there exists a subset A of $\operatorname{dom} \operatorname{freqSEQ} s$ such that $A =$ the true event of $j_1 \cdot \operatorname{CFS}(S)$ and $\overline{\overline{\text{the true event of } j_1 \cdot s}} =$

$\sum$ extract(freqSEQ s, A).

(16) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, and s be an element of D. Then freqSEQ $s = \operatorname{len} s \cdot$ FDprobSEQ s.

(17) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, s, t be elements of D, and j_1 be a function from S into *Boolean*. Then $\operatorname{Prob}(j_1, s) = \operatorname{Prob}(j_1, t)$.

Let S be a non empty finite set, let D be an equivalent distributed sample spaces family of S, and let j_1 be a function from S into *Boolean*. The functor $\operatorname{Prob}(j_1, D)$ yielding a real number is defined by:

(Def. 6) For every element s of D holds $\operatorname{Prob}(j_1, D) = \operatorname{Prob}(j_1, s)$.

Next we state the proposition

(18) For every non empty finite set S and for every element s of S^* and for every function j_1 from S into *Boolean* holds $\operatorname{Coim}(j_1 \cdot s, \mathit{true}) \in 2^{\operatorname{dom} s}$.

Let S be a set and let S_1 be a subset of S. The membership decision of S_1 yielding a function from S into *Boolean* is defined as follows:

(Def. 7) The membership decision of $S_1 = \chi_{(S_1), S}$.

The following propositions are true:

(19) For every non empty finite set S and for every subset B_1 of S there exists a function j_1 from S into *Boolean* such that $\operatorname{Coim}(j_1, \mathit{true}) = B_1$.

(20) Let S be a non empty finite set, s be an element of S^*, f be a function from S into *Boolean*, and F be a σ-field of subsets of dom s. If $F = 2^{\operatorname{dom} s}$, then $\operatorname{Coim}(f \cdot s, \mathit{true})$ is an event of F.

(21) Let S be a non empty finite set, s be an element of S^*, and f, g be functions from S into *Boolean*. Then $\operatorname{Coim}((f \vee g) \cdot s, \mathit{true}) = \operatorname{Coim}(f \cdot s, \mathit{true}) \cup \operatorname{Coim}(g \cdot s, \mathit{true})$.

(22) Let S be a non empty finite set, s be an element of S^*, and f, g be functions from S into *Boolean*. Then $\operatorname{Coim}((f \wedge g) \cdot s, \mathit{true}) = \operatorname{Coim}(f \cdot s, \mathit{true}) \cap \operatorname{Coim}(g \cdot s, \mathit{true})$.

(23) Let S be a non empty finite set, s be an element of S^*, and f be a function from S into *Boolean*. Then $\operatorname{Coim}(\neg f \cdot s, \mathit{true}) = \operatorname{dom} s \setminus \operatorname{Coim}(f \cdot s, \mathit{true})$.

(24) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, s be an element of D, and f, g be functions from S into *Boolean*. Then $\operatorname{Prob}(f \vee g, s) = \frac{\overline{\overline{(\text{the true event of } f \cdot s) \cup (\text{the true event of } g \cdot s)}}}{\operatorname{len} s}$.

(25) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, s be an element of D, and f, g be functions from S into *Boolean*. Then $\operatorname{Prob}(f \wedge g, s) = \frac{\overline{\overline{(\text{the true event of } f \cdot s) \cap (\text{the true event of } g \cdot s)}}}{\operatorname{len} s}$.

(26) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, s be an element of D, and f be a function from S into

Boolean. Then $\text{Prob}(\neg f, s) = 1 - \text{Prob}(f, s)$.

(27) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, and f, g be functions from S into *Boolean*. Then $\text{Prob}(f \vee g, D) = (\text{Prob}(f, D) + \text{Prob}(g, D)) - \text{Prob}(f \wedge g, D)$.

(28) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, and f be a function from S into *Boolean*. Then $\text{Prob}(\neg f, D) = 1 - \text{Prob}(f, D)$.

(29) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, and f be a function from S into *Boolean*. If $f = \chi_{S,S}$, then $\text{Prob}(f, D) = 1$.

(30) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, and f be a function from S into *Boolean*. Then $0 \leq \text{Prob}(f, D)$.

(31) Let S be a non empty finite set, A, B be sets, and f, g be functions from S into *Boolean*. If $A \subseteq S$ and $B \subseteq S$ and $f = \chi_{A,S}$ and $g = \chi_{B,S}$, then $\chi_{A \cup B,S} = f \vee g$.

(32) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, A, B be sets, and f, g be functions from S into *Boolean*. If $A \subseteq S$ and $B \subseteq S$ and A misses B and $f = \chi_{A,S}$ and $g = \chi_{B,S}$, then $\text{Prob}(f \wedge g, D) = 0$.

Let S be a non empty finite set and let D be an equivalent distributed sample spaces family of S. A function from $\textit{Boolean}^S$ into $\mathbb{R}$ is said to be a probability on D if:

(Def. 8) For every element j_1 of $\textit{Boolean}^S$ holds $\text{it}(j_1) = \text{Prob}(j_1, D)$.

Let S be a non empty finite set and let D be an equivalent distributed sample spaces family of S. The trivial probability of D yields a probability on the trivial σ-field of S and is defined by the condition (Def. 9).

(Def. 9) Let x be a set. Suppose $x \in$ the trivial σ-field of S. Then there exists a function c_1 from S into *Boolean* such that $c_1 = \chi_{x,S}$ and (the trivial probability of D)$(x) = \text{Prob}(c_1, D)$.

3. Sampling and Posterior Probability

Let S be a non empty finite set and let D be an equivalent distributed sample spaces family of S. An element of S is called a sample of D if:

(Def. 10) There exists an element s of D such that it $\in \text{rng}\, s$.

Let S be a non empty finite set, let D be an equivalent distributed sample spaces family of S, and let x be a sample of D. The functor $\text{Prob}\, x$ yielding a real number is defined as follows:

(Def. 11) $\text{Prob}\, x = \text{Prob}(\text{the membership decision of } \{x\}, D)$.

One can prove the following proposition

(33) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, and x be a sample of D. Then $\mathrm{Prob}\, x =$ (the probability finite sequence of D)$(|\bullet : x|_{\mathbb{N}})$.

A non empty subset of S is said to be a sampling RNG of D if:

(Def. 12) There exists a sample x of D such that $x \in$ it.

Let S be a non empty finite set, let D be an equivalent distributed sample spaces family of S, and let X be a sampling RNG of D. The functor $\mathrm{Prob}\, X$ yielding a real number is defined as follows:

(Def. 13) $\mathrm{Prob}\, X = \mathrm{Prob}$(the membership decision of X, D).

We now state several propositions:

(34) Let S be a non empty finite set, X be a subset of S, s, t be finite sequences of elements of S, S_2 be a subset of $\mathrm{dom}\, s$, and x be a subset of X. If $S_2 = s^{-1}(X)$ and $t = \mathrm{extract}(s, S_2)$, then $\overline{\overline{s^{-1}(x)}} = \overline{\overline{t^{-1}(x)}}$.

(35) Let S be a non empty finite set, X be a subset of S, s, t be finite sequences of elements of S, S_2 be a subset of $\mathrm{dom}\, s$, and x be a set. If $S_2 = s^{-1}(X)$ and $t = \mathrm{extract}(s, S_2)$ and $x \in X$, then $\mathrm{frequency}(x, s) = \mathrm{frequency}(x, t)$.

(36) Let S be a non empty finite set, D be an element of the distribution family of S, and s be a finite sequence of elements of S. If $s \in D$, then $D =$ the equivalence class of s.

(37) Let S be a non empty finite set, X be a subset of S, and s be a finite sequence of elements of S. Then $s^{-1}(X) =$ the true event of (the membership decision of X) $\cdot\, s$.

(38) Let S be a non empty finite set, X be a non empty subset of S, D be an equivalent distributed sample spaces family of S, s_1, s_2 be elements of D, t_1, t_2 be finite sequences of elements of S, S_3 be a subset of $\mathrm{dom}\, s_1$, and S_4 be a subset of $\mathrm{dom}\, s_2$. Suppose $S_3 = {s_1}^{-1}(X)$ and $t_1 = \mathrm{extract}(s_1, S_3)$ and $S_4 = {s_2}^{-1}(X)$ and $t_2 = \mathrm{extract}(s_2, S_4)$. Then t_1 and t_2 are probability equivalent.

The conditional subset of X yields an equivalent distributed sample spaces family of S and is defined by the condition (Def. 14).

(Def. 14) There exists an element s of D and there exists a finite sequence t of elements of S and there exists a subset S_2 of $\mathrm{dom}\, s$ such that $S_2 = s^{-1}(X)$ and $t = \mathrm{extract}(s, S_2)$ and $t \in$ the conditional subset of X.

Let f be a function from S into *Boolean*. The functor $\mathrm{Prob}(f, X)$ yielding a real number is defined by:

(Def. 15) $\mathrm{Prob}(f, X) = \mathrm{Prob}(f,$ the conditional subset of $X)$.

One can prove the following proposition

(39) Let S be a non empty finite set, D be an equivalent distributed sample spaces family of S, X be a sampling RNG of D, and f be a function from S into *Boolean*. Then $\mathrm{Prob}(f, X) \cdot \mathrm{Prob}\, X = \mathrm{Prob}(f \wedge$ the membership decision of X, $D)$.

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 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] Shunichi Kobayashi and Kui Jia. A theory of Boolean valued functions and partitions. *Formalized Mathematics*, 7(**2**):249–254, 1998.
[12] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**):841–845, 1990.
[13] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.
[14] Hiroyuki Okazaki. Probability on finite and discrete set and uniform distribution. *Formalized Mathematics*, 17(**2**):173–178, 2009, doi: 10.2478/v10037-009-0020-z.
[15] Hiroyuki Okazaki and Yasunari Shidama. Probability on finite set and real-valued random variables. *Formalized Mathematics*, 17(**2**):129–136, 2009, doi: 10.2478/v10037-009-0014-x.
[16] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[17] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[18] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[19] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[20] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[22] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.
[23] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[24] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[25] Bo Zhang and Yatsuka Nakamura. The definition of finite sequences and matrices of probability, and addition of matrices of real elements. *Formalized Mathematics*, 14(**3**):101–108, 2006, doi:10.2478/v10037-006-0012-1.

Received July 4, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 4, Pages 265–269, 2012
DOI: 10.2478/v10037-012-0031-z

VERSITA
versita.com/fm/

Basic Properties of Primitive Root and Order Function[1]

Na Ma
Qingdao University of Science and Technology
China

Xiquan Liang
Qingdao University of Science and Technology
China

Summary. In this paper we defined the reduced residue system and proved its fundamental properties. Then we proved the basic properties of the order function. Finally, we defined the primitive root and proved its fundamental properties. Our work is based on [12], [8], and [11].

MML identifier: `INT_8`, version: `8.0.01 5.3.1162`

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

For simplicity, we adopt the following convention: i, s, t, m, n, k are natural numbers, d, e are elements of $\mathbb{N}$, f_1 is a finite sequence of elements of $\mathbb{N}$, and x is an integer.

Let m be a natural number. The functor $\mathrm{RelPrimes}\, m$ yields a set and is defined by:

(Def. 1) $\mathrm{RelPrimes}\, m = \{k \in \mathbb{N}: m$ and k are relative prime $\wedge\ 1 \leq k\ \wedge\ k \leq m\}$.

We now state the proposition

(1) $\mathrm{RelPrimes}\, m \subseteq \mathrm{Seg}\, m$.

Let m be a natural number. Then $\mathrm{RelPrimes}\, m$ is a subset of $\mathbb{N}$.

Let m be a natural number. Observe that $\mathrm{RelPrimes}\, m$ is finite.

Next we state several propositions:

(2) If $1 \leq m$, then $\mathrm{RelPrimes}\, m \neq \emptyset$.

[1] Authors thank Andrzej Trybulec and Yatsuka Nakamura for the help during writing this article.

(3) For every subset X of $\mathbb{Z}$ and for every integer a holds $x \in a \circ X$ iff there exists an integer y such that $y \in X$ and $x = a \cdot y$.

(4) There exists a natural number r such that $(1+s)^t = 1+t\cdot s+\binom{t}{2}\cdot s^{\mathbf{2}}+r\cdot s^3$.

(5) If $n > 1$ and i and n are relative prime, then $i \neq 0$.

(6) For all integers a, b and for every natural number m such that $a \cdot b \bmod m = 1$ and $a \bmod m = 1$ holds $b \bmod m = 1$.

(7) For every odd integer x and for every natural number k such that $k \geq 3$ holds $x^{2^{k -' 2}} \bmod 2^k = 1$.

In the sequel p is a prime number.

We now state a number of propositions:

(8) If $m \geq 1$, then $\mathrm{Euler}\, p^m = p^m - p^{m -' 1}$.

(9) If $n > 1$ and i and n are relative prime, then $\mathrm{order}(i, n) \mid \mathrm{Euler}\, n$.

(10) For all i, n such that $n > 1$ and i and n are relative prime holds $i^s \equiv i^t \pmod{n}$ iff $s \equiv t \pmod{\mathrm{order}(i, n)}$.

(11) For all i, n such that $n > 1$ and i and n are relative prime holds $i^s \equiv 1 \pmod{n}$ iff $\mathrm{order}(i, n) \mid s$.

(12) Suppose $n > 1$ and i and n are relative prime and $\mathrm{len}\, f_1 = \mathrm{order}(i, n)$ and for every d such that $d \in \mathrm{dom}\, f_1$ holds $f_1(d) = i^{d -' 1}$. Let given d, e. If d, $e \in \mathrm{dom}\, f_1$ and $d \neq e$, then $f_1(d) \not\equiv f_1(e) \pmod{n}$.

(13) Suppose $n > 1$ and i and n are relative prime and $\mathrm{len}\, f_1 = \mathrm{order}(i, n)$ and for every d such that $d \in \mathrm{dom}\, f_1$ holds $f_1(d) = i^{d -' 1}$. Let given d. If $d \in \mathrm{dom}\, f_1$, then $f_1(d)^{\mathrm{order}(i,n)} \bmod n = 1$.

(14) If $n > 1$ and i and n are relative prime, then $\mathrm{order}(i^s, n) = \mathrm{order}(i, n) \operatorname{div} (\mathrm{order}(i, n) \gcd s)$.

(15) Let given i, n. Suppose $n > 1$ and i and n are relative prime. Then $\mathrm{order}(i, n)$ and s are relative prime if and only if $\mathrm{order}(i^s, n) = \mathrm{order}(i, n)$.

(16) If $n > 1$ and i and n are relative prime and $\mathrm{order}(i, n) = s \cdot t$, then $\mathrm{order}(i^s, n) = t$.

(17) Suppose that

(i) $n > 1$,

(ii) s and n are relative prime,

(iii) t and n are relative prime, and

(iv) $\mathrm{order}(s, n)$ and $\mathrm{order}(t, n)$ are relative prime.

Then $\mathrm{order}(s \cdot t, n) = \mathrm{order}(s, n) \cdot \mathrm{order}(t, n)$.

In the sequel f_2, f_3 are finite sequences of elements of $\mathbb{N}$.

We now state four propositions:

(18) Suppose $n > 1$ and s and n are relative prime and t and n are relative prime and $\mathrm{order}(s \cdot t, n) = \mathrm{order}(s, n) \cdot \mathrm{order}(t, n)$. Then $\mathrm{order}(s, n)$ and $\mathrm{order}(t, n)$ are relative prime.

(19) If $n > 1$ and s and n are relative prime and $s \cdot t \bmod n = 1$, then $\mathrm{order}(s, n) = \mathrm{order}(t, n)$.

(20) If $n > 1$ and $m > 1$ and i and n are relative prime and $m \mid n$, then $\mathrm{order}(i, m) \mid \mathrm{order}(i, n)$.

(21) If $n > 1$ and $m > 1$ and m and n are relative prime and i and $m \cdot n$ are relative prime, then $\mathrm{order}(i, m \cdot n) = \mathrm{lcm}(\mathrm{order}(i, m), \mathrm{order}(i, n))$.

Let X be a set and let m be a natural number. We say that X is primitive root of m if and only if the condition (Def. 2) is satisfied.

(Def. 2) There exists a finite sequence f_2 of elements of $\mathbb{Z}$ such that $\mathrm{len}\, f_2 = \mathrm{len}\, \mathrm{Sgm}\, \mathrm{RelPrimes}\, m$ and for every d such that $d \in \mathrm{dom}\, f_2$ holds $f_2(d) \in [(\mathrm{Sgm}\, \mathrm{RelPrimes}\, m)(d)]_{\mathrm{Cong}\, m}$ and $X = \mathrm{rng}\, f_2$.

We now state several propositions:

(22) RelPrimes m is primitive root of m.

(23) If $d, e \in \mathrm{dom}\, \mathrm{Sgm}\, \mathrm{RelPrimes}\, m$ and $d \neq e$, then $(\mathrm{Sgm}\, \mathrm{RelPrimes}\, m)(d) \not\equiv (\mathrm{Sgm}\, \mathrm{RelPrimes}\, m)(e) \pmod{m}$.

(24) Let X be a finite set. Suppose X is primitive root of m. Then
  (i) $\overline{\overline{X}} = \mathrm{Euler}\, m$,
  (ii) for all integers x, y such that $x, y \in X$ and $x \neq y$ holds $x \not\equiv y \pmod{m}$, and
  (iii) for every integer x such that $x \in X$ holds x and m are relative prime.

(25) $\emptyset$ is primitive root of m iff $m = 0$.

(26) Let X be a finite subset of $\mathbb{Z}$. Suppose that
  (i) $1 < m$,
  (ii) $\overline{\overline{X}} = \mathrm{Euler}\, m$,
  (iii) for all integers x, y such that $x, y \in X$ and $x \neq y$ holds $x \not\equiv y \pmod{m}$, and
  (iv) for every integer x such that $x \in X$ holds x and m are relative prime.

  Then X is primitive root of m.

(27) Let X be a finite subset of $\mathbb{Z}$ and a be an integer. Suppose $m > 1$ and a and m are relative prime and X is primitive root of m. Then $a \circ X$ is primitive root of m.

Let us consider i, n. We say that i is RRS of n if and only if:

(Def. 3) $\mathrm{order}(i, n) = \mathrm{Euler}\, n$.

Next we state several propositions:

(28) Suppose $n > 1$ and i and n are relative prime. Then i is RRS of n if and only if for every f_1 such that $\mathrm{len}\, f_1 = \mathrm{Euler}\, n$ and for every natural number d such that $d \in \mathrm{dom}\, f_1$ holds $f_1(d) = i^d$ holds $\mathrm{rng}\, f_1$ is primitive root of n.

(29) Suppose $p > 2$ and i and p are relative prime and i is RRS of p. Let k be a natural number. Then $i^{2 \cdot k+1}$ is not quadratic residue mod p.

(30) Let k be a natural number. Suppose $k \geq 3$. Let given m. If m and 2^k are relative prime, then m is not RRS of 2^k.

(31) If $p > 2$ and $k \geq 2$ and i and p are relative prime and i is RRS of p and $i^{p -' 1} \bmod p^{\mathbf{2}} \neq 1$, then $i^{\mathrm{Euler}\, p^{k -' 1}} \bmod p^k \neq 1$.

(32) Suppose $n > 1$ and $\mathrm{len}\, f_2 \geq 2$ and for every d such that $d \in \mathrm{dom}\, f_2$ holds $f_2(d)$ and n are relative prime. Let given f_3. Suppose that

(i) $\mathrm{len}\, f_3 = \mathrm{len}\, f_2$,

(ii) for every d such that $d \in \mathrm{dom}\, f_3$ holds $f_3(d) = \mathrm{order}(f_2(d), n)$, and

(iii) for all d, e such that $d, e \in \mathrm{dom}\, f_3$ and $d \neq e$ holds $f_3(d)$ and $f_3(e)$ are relative prime.

Then $\mathrm{order}(\prod f_2, n) = \prod f_3$.

References

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

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

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

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

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

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

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

[8] Zhang Dexin. *Integer Theory.* Science Publication, China, 1965.

[9] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6(**4**):549–551, 1997.

[10] 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.

[11] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Posts and Telecom Press, China, 2007.

[12] Hua Loo Keng. *Introduction to Number Theory.* Beijing Science Publication, China, 1957.

[13] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**):841–845, 1990.

[14] Artur Korniłowicz. Collective operations on number-membered sets. *Formalized Mathematics*, 17(**2**):99–115, 2009, doi: 10.2478/v10037-009-0011-0.

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

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

[17] Xiquan Liang, Li Yan, and Junjie Zhao. Linear congruence relation and complete residue systems. *Formalized Mathematics*, 15(**4**):181–187, 2007, doi:10.2478/v10037-007-0022-7.

[18] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.

[19] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.

[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 and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[23] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received August 6, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 4, Pages 271–274, 2012
DOI: 10.2478/v10037-012-0032-y

VERSITA
versita.com/fm/

Banach's Continuous Inverse Theorem and Closed Graph Theorem[1]

Hideki Sakurai
406-3, Haneo, Naganohara
Agatuma, Gunma, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article we formalize one of the most important theorems of linear operator theory – the Closed Graph Theorem commonly used in a standard text book such as [10] in Chapter 24.3. It states that a surjective closed linear operator between Banach spaces is bounded.

MML identifier: `LOPBAN_7`, version: `8.0.01 5.3.1162`

The terminology and notation used here have been introduced in the following articles: [3], [4], [2], [15], [11], [14], [1], [5], [13], [12], [19], [20], [16], [7], [17], [8], [18], [9], and [6].

Let X, Y be non empty normed structures, let x be a point of X, and let y be a point of Y. Then $\langle x, y\rangle$ is a point of $X \times Y$.

Let X, Y be non empty normed structures, let s_1 be a sequence of X, and let s_2 be a sequence of Y. Then $\langle s_1, s_2\rangle$ is a sequence of $X \times Y$.

We now state several propositions:

(1) Let X, Y be real linear spaces and T be a linear operator from X into Y. Suppose T is bijective. Then T^{-1} is a linear operator from Y into X and $\mathrm{rng}(T^{-1}) =$ the carrier of X.

(2) Let X, Y be non empty linear topological spaces, T be a linear operator from X into Y, and S be a function from Y into X. Suppose T is bijective

[1]This work was supported by JSPS KAKENHI 22300285.

ISSN 1426–2630(p), 1898-9934(e)

and open and $S = T^{-1}$. Then S is a linear operator from Y into X, onto, and continuous.

(3) For all real normed spaces X, Y and for every linear operator f from X into Y holds $0_Y = f(0_X)$.

(4) Let X, Y be real normed spaces, f be a linear operator from X into Y, and x be a point of X. Then f is continuous in x if and only if f is continuous in 0_X.

(5) Let X, Y be real normed spaces and f be a linear operator from X into Y. Then f is continuous on the carrier of X if and only if f is continuous in 0_X.

(6) Let X, Y be real normed spaces and f be a linear operator from X into Y. Then f is Lipschitzian if and only if f is continuous on the carrier of X.

(7) Let X, Y be real Banach spaces and T be a Lipschitzian linear operator from X into Y. Suppose T is bijective. Then T^{-1} is a Lipschitzian linear operator from Y into X.

(8) Let X, Y be real normed spaces, s_1 be a sequence of X, s_2 be a sequence of Y, x be a point of X, and y be a point of Y. Then s_1 is convergent and $\lim s_1 = x$ and s_2 is convergent and $\lim s_2 = y$ if and only if $\langle s_1, s_2 \rangle$ is convergent and $\lim \langle s_1, s_2 \rangle = \langle x, y \rangle$.

Let X, Y be real normed spaces and let T be a partial function from X to Y. The functor graph(T) yields a subset of $X \times Y$ and is defined as follows:

(Def. 1) graph(T) $= T$.

Let X, Y be real normed spaces and let T be a non empty partial function from X to Y. Observe that graph(T) is non empty.

Let X, Y be real normed spaces and let T be a linear operator from X into Y. Note that graph(T) is linearly closed.

Let X, Y be real normed spaces and let T be a linear operator from X into Y. The functor graphNrm(T) yielding a function from graph(T) into $\mathbb{R}$ is defined as follows:

(Def. 2) graphNrm(T) = (the norm of $X \times Y$)$\restriction$graph(T).

Let X, Y be real normed spaces and let T be a partial function from X to Y. We say that T is closed if and only if:

(Def. 3) graph(T) is closed.

Let X, Y be real normed spaces and let T be a linear operator from X into Y. The functor graphNSP(T) yields a non empty normed structure and is defined by:

(Def. 4) $\mathrm{graphNSP}(T) = \langle \mathrm{graph}(T), \mathrm{Zero}(\mathrm{graph}(T), X \times Y), \mathrm{Add}(\mathrm{graph}(T), X \times Y), \mathrm{Mult}(\mathrm{graph}(T), X \times Y), \mathrm{graphNrm}(T) \rangle$.

Let X, Y be real normed spaces and let T be a linear operator from X into Y. One can check that graphNSP(T) is Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, and scalar unital.

One can prove the following proposition

(9) For all real normed spaces X, Y and for every linear operator T from X into Y holds graphNSP(T) is a subspace of $X \times Y$.

Let X, Y be real normed spaces and let T be a linear operator from X into Y. Note that graphNSP(T) is reflexive, discernible, and real normed space-like.

We now state several propositions:

(10) Let X be a real normed space, Y be a real Banach space, and X_0 be a subset of Y. Suppose that

(i) X is a subspace of Y,

(ii) the carrier of $X = X_0$,

(iii) the norm of $X =$ (the norm of Y)↾(the carrier of X), and

(iv) X_0 is closed.

Then X is complete.

(11) Let X, Y be real Banach spaces and T be a linear operator from X into Y. If T is closed, then graphNSP(T) is complete.

(12) Let X, Y be real normed spaces and T be a non empty partial function from X to Y. Then T is closed if and only if for every sequence s_3 of X such that $\operatorname{rng} s_3 \subseteq \operatorname{dom} T$ and s_3 is convergent and $T_* s_3$ is convergent holds $\lim s_3 \in \operatorname{dom} T$ and $\lim(T_* s_3) = T(\lim s_3)$.

(13) Let X, Y be real normed spaces, T be a non empty partial function from X to Y, and T_0 be a linear operator from X into Y. If T_0 is Lipschitzian and $\operatorname{dom} T$ is closed and $T = T_0$, then T is closed.

(14) Let X, Y be real normed spaces, T be a non empty partial function from X to Y, and S be a non empty partial function from Y to X. If T is closed and one-to-one and $S = T^{-1}$, then S is closed.

(15) For all real normed spaces X, Y and for every point x of X and for every point y of Y holds $\|x\| \leq \|\langle x, y\rangle\|$ and $\|y\| \leq \|\langle x, y\rangle\|$.

Let X, Y be real Banach spaces. Note that every linear operator from X into Y which is closed is also Lipschitzian.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[2] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.
[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[4] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[5] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[6] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[7] Czesław Byliński. Introduction to real linear topological spaces. *Formalized Mathematics*, 13(**1**):99–107, 2005.
[8] Noboru Endou, Yasumasa Suzuki, and Yasunari Shidama. Real linear space of real sequences. *Formalized Mathematics*, 11(**3**):249–253, 2003.
[9] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[10] Isao Miyadera. *Functional Analysis*. Riko-Gaku-Sya, 1972.
[11] Takaya Nishiyama, Keiji Ohkubo, and Yasunari Shidama. The continuous functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):269–275, 2004.
[12] Hiroyuki Okazaki, Noboru Endou, and Yasunari Shidama. Cartesian products of family of real linear spaces. *Formalized Mathematics*, 19(**1**):51–59, 2011, doi: 10.2478/v10037-011-0009-2.
[13] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[14] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[15] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.
[16] Wojciech A. Trybulec. Subspaces and cosets of subspaces in real linear space. *Formalized Mathematics*, 1(**2**):297–301, 1990.
[17] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[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.

Received August 6, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 4, Pages 275–280, 2012
DOI: 10.2478/v10037-012-0033-x

VERSITA
versita.com/fm/

Free $\mathbb{Z}$-module[1]

Yuichi Futa
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article we formalize a free $\mathbb{Z}$-module and its rank. We formally prove that for a free finite rank $\mathbb{Z}$-module V, the number of elements in its basis, that is a rank of the $\mathbb{Z}$-module, is constant regardless of the selection of its basis. $\mathbb{Z}$-module is necessary for lattice problems, LLL(Lenstra, Lenstra and Lovász) base reduction algorithm and cryptographic systems with lattice [15]. Some theorems in this article are described by translating theorems in [21] and [8] into theorems of $\mathbb{Z}$-module.

MML identifier: ZMODUL03, version: 8.0.01 5.3.1162

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

1. Free $\mathbb{Z}$-module

In this paper V is a $\mathbb{Z}$-module, v is a vector of V, and W is a submodule of V.

Let us note that there exists a $\mathbb{Z}$-module which is non trivial.

Let V be a $\mathbb{Z}$-module. One can verify that there exists a finite subset of V which is linearly independent.

Let K be a field, let V be a non empty vector space structure over K, let L be a linear combination of V, and let v be a vector of V. Then $L(v)$ is an element of K.

Next we state two propositions:

(1) Let u be a vector of V. Then there exists a z linear combination l of V such that $l(u) = 1$ and for every vector v of V such that $v \neq u$ holds $l(v) = 0$.

[1]This work was supported by JSPS KAKENHI 21240001 and 22300285.

ISSN 1426–2630(p), 1898-9934(e)

(2) Let G be a $\mathbb{Z}$-module, i be an element of $\mathbb{Z}$, w be an element of $\mathbb{Z}$, and v be an element of G. Suppose $G = \langle$the carrier of $(\mathbb{Z}^{\rm R})$, the zero of $(\mathbb{Z}^{\rm R})$, the addition of $(\mathbb{Z}^{\rm R})$, the left integer multiplication of $(\mathbb{Z}^{\rm R})\rangle$ and $v = w$. Then $i \cdot v = i \cdot w$.

Let I_1 be a $\mathbb{Z}$-module. We say that I_1 is free if and only if:

(Def. 1) There exists a subset A of I_1 such that A is linearly independent and $\mathrm{Lin}(A) =$ the $\mathbb{Z}$-module structure of I_1.

Let us consider V. One can check that $\mathbf{0}_V$ is free.

One can verify that there exists a $\mathbb{Z}$-module which is strict and free.

Let V be a $\mathbb{Z}$-module. One can verify that there exists a submodule of V which is strict and free.

Let V be a free $\mathbb{Z}$-module. A subset of V is called a basis of V if:

(Def. 2) It is linearly independent and $\mathrm{Lin}(\mathrm{it}) =$ the $\mathbb{Z}$-module structure of V.

One can verify that every free $\mathbb{Z}$-module inherits cancelable on multiplication.

Let us observe that there exists a non trivial $\mathbb{Z}$-module which is free.

In the sequel K_1, K_2 denote z linear combinations of V and X denotes a subset of V.

We now state a number of propositions:

(3) If X is linearly independent and the support of $K_1 \subseteq X$ and the support of $K_2 \subseteq X$ and $\sum K_1 = \sum K_2$, then $K_1 = K_2$.

(4) Let V be a free $\mathbb{Z}$-module and A be a subset of V. Suppose A is linearly independent. Then there exists a subset B of V such that $A \subseteq B$ and B is linearly independent and for every vector v of V there exists an integer a such that $a \cdot v \in \mathrm{Lin}(B)$.

(5) Let L be a z linear combination of V, F, G be finite sequences of elements of V, and P be a permutation of $\mathrm{dom}\, F$. If $G = F \cdot P$, then $\sum(L \cdot F) = \sum(L \cdot G)$.

(6) Let L be a z linear combination of V and F be a finite sequence of elements of V. If the support of L misses $\mathrm{rng}\, F$, then $\sum(L \cdot F) = 0_V$.

(7) Let F be a finite sequence of elements of V. Suppose F is one-to-one. Let L be a z linear combination of V. If the support of $L \subseteq \mathrm{rng}\, F$, then $\sum(L \cdot F) = \sum L$.

(8) Let L be a z linear combination of V and F be a finite sequence of elements of V. Then there exists a z linear combination K of V such that the support of $K = \mathrm{rng}\, F \cap$ (the support of L) and $L \cdot F = K \cdot F$.

(9) Let L be a z linear combination of V, A be a subset of V, and F be a finite sequence of elements of V. Suppose $\mathrm{rng}\, F \subseteq$ the carrier of $\mathrm{Lin}(A)$. Then there exists a z linear combination K of A such that $\sum(L \cdot F) = \sum K$.

(10) Let L be a z linear combination of V and A be a subset of V. Suppose the support of $L \subseteq$ the carrier of $\mathrm{Lin}(A)$. Then there exists a z linear combination K of A such that $\sum L = \sum K$.

(11) Let L be a z linear combination of V. Suppose the support of $L \subseteq$ the carrier of W. Let K be a z linear combination of W. Suppose $K = L{\restriction}$the carrier of W. Then the support of $L =$ the support of K and $\sum L = \sum K$.

(12) Let K be a z linear combination of W. Then there exists a z linear combination L of V such that the support of $K =$ the support of L and $\sum K = \sum L$.

(13) Let L be a z linear combination of V. Suppose the support of $L \subseteq$ the carrier of W. Then there exists a z linear combination K of W such that the support of $K =$ the support of L and $\sum K = \sum L$.

(14) For every free $\mathbb{Z}$-module V and for every basis I of V and for every vector v of V holds $v \in \mathrm{Lin}(I)$.

(15) For every subset A of W such that A is linearly independent holds A is a linearly independent subset of V.

(16) Let A be a subset of V. Suppose A is linearly independent and $A \subseteq$ the carrier of W. Then A is a linearly independent subset of W.

(17) Let V be a $\mathbb{Z}$-module and A be a subset of V. Suppose A is linearly independent. Let v be a vector of V. If $v \in A$, then for every subset B of V such that $B = A \setminus \{v\}$ holds $v \notin \mathrm{Lin}(B)$.

(18) Let V be a free $\mathbb{Z}$-module, I be a basis of V, and A be a non empty subset of V. Suppose A misses I. Let B be a subset of V. If $B = I \cup A$, then B is linearly dependent.

(19) For every subset A of V such that $A \subseteq$ the carrier of W holds $\mathrm{Lin}(A)$ is a submodule of W.

(20) For every subset A of V and for every subset B of W such that $A = B$ holds $\mathrm{Lin}(A) = \mathrm{Lin}(B)$.

Let V be a $\mathbb{Z}$-module and let A be a linearly independent subset of V. One can check that $\mathrm{Lin}(A)$ is free.

Let V be a free $\mathbb{Z}$-module. Observe that Ω_V is strict and free.

2. FINITE RANK FREE $\mathbb{Z}$-MODULE

Let I_1 be a free $\mathbb{Z}$-module. We say that I_1 is finite-rank if and only if:

(Def. 3) There exists a finite subset of I_1 which is a basis of I_1.

Let us consider V. Note that $\mathbf{0}_V$ is finite-rank.

Let us note that there exists a free $\mathbb{Z}$-module which is strict and finite-rank.

Let V be a $\mathbb{Z}$-module. Note that there exists a free submodule of V which is strict and finite-rank.

Let V be a $\mathbb{Z}$-module and let A be a finite linearly independent subset of V. One can check that $\operatorname{Lin}(A)$ is finite-rank.

Let V be a $\mathbb{Z}$-module. We say that V is finitely-generated if and only if:

(Def. 4) There exists a finite subset A of V such that $\operatorname{Lin}(A) =$ the $\mathbb{Z}$-module structure of V.

Let us consider V. One can verify that $\mathbf{0}_V$ is finitely-generated.

Let us mention that there exists a $\mathbb{Z}$-module which is strict, finitely-generated, and free.

Let V be a finite-rank free $\mathbb{Z}$-module. Observe that every basis of V is finite.

3. Rank of a Finite Rank Free $\mathbb{Z}$-module

The following propositions are true:

(21) Let p be a prime number, V be a free $\mathbb{Z}$-module, I be a basis of V, and u_1, u_2 be vectors of V. If $u_1 \neq u_2$ and $u_1, u_2 \in I$, then $\mathrm{ZMtoMQV}(V, p, u_1) \neq \mathrm{ZMtoMQV}(V, p, u_2)$.

(22) Let p be a prime number, V be a $\mathbb{Z}$-module, Z_1 be a vector space over $\mathrm{GF}(p)$, and v_1 be a vector of Z_1. If $Z_1 = \mathrm{Z_MQ_VectSp}(V, p)$, then there exists a vector v of V such that $v_1 = \mathrm{ZMtoMQV}(V, p, v)$.

(23) Let p be a prime number, V be a $\mathbb{Z}$-module, I be a subset of V, and l_1 be a linear combination of $\mathrm{Z_MQ_VectSp}(V, p)$. Then there exists a z linear combination l of I such that for every vector v of V if $v \in I$, then there exists a vector w of V such that $w \in I$ and $w \in \mathrm{ZMtoMQV}(V, p, v)$ and $l(w) = l_1(\mathrm{ZMtoMQV}(V, p, v))$.

(24) Let p be a prime number, V be a free $\mathbb{Z}$-module, I be a basis of V, and l_1 be a linear combination of $\mathrm{Z_MQ_VectSp}(V, p)$. Then there exists a z linear combination l of I such that for every vector v of V if $v \in I$, then $l(v) = l_1(\mathrm{ZMtoMQV}(V, p, v))$.

(25) Let p be a prime number, V be a free $\mathbb{Z}$-module, I be a basis of V, and X be a non empty subset of $\mathrm{Z_MQ_VectSp}(V, p)$. Suppose $X = \{\mathrm{ZMtoMQV}(V, p, u); u$ ranges over vectors of $V \colon u \in I\}$. Then there exists a function F from X into the carrier of V such that for every vector u of V such that $u \in I$ holds $F(\mathrm{ZMtoMQV}(V, p, u)) = u$ and F is one-to-one and $\operatorname{dom} F = X$ and $\operatorname{rng} F = I$.

(26) Let p be a prime number, V be a free $\mathbb{Z}$-module, and I be a basis of V. Then $\overline{\overline{\{\mathrm{ZMtoMQV}(V, p, u); u \text{ ranges over vectors of } V \colon u \in I\}}} = \overline{\overline{I}}$.

(27) For every prime number p and for every free $\mathbb{Z}$-module V holds $\mathrm{ZMtoMQV}(V, p, 0_V) = 0_{\mathrm{Z_MQ_VectSp}(V,p)}$.

(28) Let p be a prime number, V be a free $\mathbb{Z}$-module, and s, t be elements of V. Then $\mathrm{ZMtoMQV}(V, p, s) + \mathrm{ZMtoMQV}(V, p, t) = \mathrm{ZMtoMQV}(V, p, s+t)$.

(29) Let p be a prime number, V be a free $\mathbb{Z}$-module, s be a finite sequence of elements of V, and t be a finite sequence of elements of $\mathrm{Z_MQ_VectSp}(V, p)$. Suppose $\mathrm{len}\, s = \mathrm{len}\, t$ and for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, s$ there exists a vector s_1 of V such that $s_1 = s(i)$ and $t(i) = \mathrm{ZMtoMQV}(V, p, s_1)$. Then $\sum t = \mathrm{ZMtoMQV}(V, p, \sum s)$.

(30) Let p be a prime number, V be a free $\mathbb{Z}$-module, s be an element of V, a be an integer, and b be an element of $\mathrm{GF}(p)$. If $a = b$, then $b \cdot \mathrm{ZMtoMQV}(V, p, s) = \mathrm{ZMtoMQV}(V, p, a \cdot s)$.

(31) Let p be a prime number, V be a free $\mathbb{Z}$-module, I be a basis of V, l be a z linear combination of I, I_2 be a subset of $\mathrm{Z_MQ_VectSp}(V, p)$, and l_1 be a linear combination of I_2. Suppose $I_2 = \{\mathrm{ZMtoMQV}(V, p, u); u$ ranges over vectors of V: $u \in I\}$ and for every vector v of V such that $v \in I$ holds $l(v) = l_1(\mathrm{ZMtoMQV}(V, p, v))$. Then $\sum l_1 = \mathrm{ZMtoMQV}(V, p, \sum l)$.

(32) Let p be a prime number, V be a free $\mathbb{Z}$-module, I be a basis of V, and I_2 be a subset of $\mathrm{Z_MQ_VectSp}(V, p)$. If $I_2 = \{\mathrm{ZMtoMQV}(V, p, u); u$ ranges over vectors of V: $u \in I\}$, then I_2 is linearly independent.

(33) Let p be a prime number, V be a free $\mathbb{Z}$-module, I be a subset of V, and I_2 be a subset of $\mathrm{Z_MQ_VectSp}(V, p)$. Suppose $I_2 = \{\mathrm{ZMtoMQV}(V, p, u); u$ ranges over vectors of V: $u \in I\}$. Let s be a finite sequence of elements of V. Suppose that for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, s$ there exists a vector s_1 of V such that $s_1 = s(i)$ and $\mathrm{ZMtoMQV}(V, p, s_1) \in \mathrm{Lin}(I_2)$. Then $\mathrm{ZMtoMQV}(V, p, \sum s) \in \mathrm{Lin}(I_2)$.

(34) Let p be a prime number, V be a free $\mathbb{Z}$-module, I be a basis of V, I_2 be a subset of $\mathrm{Z_MQ_VectSp}(V, p)$, and l be a z linear combination of I. If $I_2 = \{\mathrm{ZMtoMQV}(V, p, u); u$ ranges over vectors of V: $u \in I\}$, then $\mathrm{ZMtoMQV}(V, p, \sum l) \in \mathrm{Lin}(I_2)$.

(35) Let p be a prime number, V be a free $\mathbb{Z}$-module, I be a basis of V, and I_2 be a subset of $\mathrm{Z_MQ_VectSp}(V, p)$. If $I_2 = \{\mathrm{ZMtoMQV}(V, p, u); u$ ranges over vectors of V: $u \in I\}$, then I_2 is a basis of $\mathrm{Z_MQ_VectSp}(V, p)$.

Let p be a prime number and let V be a finite-rank free $\mathbb{Z}$-module. Observe that $\mathrm{Z_MQ_VectSp}(V, p)$ is finite dimensional.

Next we state the proposition

(36) For every finite-rank free $\mathbb{Z}$-module V and for all bases A, B of V holds $\overline{\overline{A}} = \overline{\overline{B}}$.

Let V be a finite-rank free $\mathbb{Z}$-module. The functor $\mathrm{rank}\, V$ yields a natural number and is defined as follows:

(Def. 5) For every basis I of V holds $\mathrm{rank}\, V = \overline{\overline{I}}$.

The following proposition is true

(37) For every prime number p and for every finite-rank free $\mathbb{Z}$-module V holds $\mathrm{rank}\, V = \dim(\mathrm{Z_MQ_VectSp}(V, p))$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[8] Jing-Chao Chen. The Steinitz theorem and the dimension of a real linear space. *Formalized Mathematics*, 6(**3**):411–415, 1997.
[9] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[10] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012, doi: 10.2478/v10037-012-0007-z.
[11] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Quotient module of $\mathbb{Z}$-module. *Formalized Mathematics*, 20(**3**):205–214, 2012, doi: 10.2478/v10037-012-0024-y.
[12] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**):841–845, 1990.
[13] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[14] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[15] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: A cryptographic perspective (the international series in engineering and computer science). 2002.
[16] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(**3**):339–345, 1996.
[17] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.
[18] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[19] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[20] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[21] Wojciech A. Trybulec. Basis of real linear space. *Formalized Mathematics*, 1(**5**):847–850, 1990.
[22] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 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. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[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.

Received August 6, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 4, Pages 281–290, 2012
DOI: 10.2478/v10037-012-0034-9

VERSITA
versita.com/fm/

Cayley-Dickson Construction[1]

Artur Korniłowicz
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

Summary. Cayley-Dickson construction produces a sequence of normed algebras over real numbers. Its consequent applications result in complex numbers, quaternions, octonions, etc. In this paper we formalize the construction and prove its basic properties.

MML identifier: CAYLDICK, version: 8.0.01 5.3.1162

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

1. Preliminaries

We use the following convention: u, v, x, y, z, X, Y are sets and r, s are real numbers.

One can prove the following proposition

(1) For all real numbers a, b, c, d holds $(a+b)^{\mathbf{2}} + (c+d)^{\mathbf{2}} \leq (\sqrt{a^{\mathbf{2}} + c^{\mathbf{2}}} + \sqrt{b^{\mathbf{2}} + d^{\mathbf{2}}})^{\mathbf{2}}$.

Let X be a non trivial real normed space and let x be a non zero element of X. One can verify that $\|x\|$ is positive.

Let c be a non zero complex number. Note that $c^{\mathbf{2}}$ is non zero.

[1]This work has been supported by the Polish Ministry of Science and Higher Education project "Managing a Large Repository of Computer-verified Mathematical Knowledge" (N N519 385136).

ISSN 1426–2630(p), 1898-9934(e)

Let x be a non empty set. Observe that $\langle x \rangle$ is non-empty.

Let us note that there exists a finite 0-sequence which is non-empty.

Let f, g be non-empty finite 0-sequences. Observe that $f \frown g$ is non-empty.

Let x, y be non empty sets. One can verify that $\langle x, y \rangle$ is non-empty.

The following propositions are true:

(2) If $\langle u \rangle = \langle x \rangle$, then $u = x$.

(3) If $\langle u, v \rangle = \langle x, y \rangle$, then $u = x$ and $v = y$.

(4) If $x \in X$, then $\langle x \rangle \in \prod \langle X \rangle$.

(5) If $z \in \prod \langle X \rangle$, then there exists x such that $x \in X$ and $z = \langle x \rangle$.

(6) If $x \in X$ and $y \in Y$, then $\langle x, y \rangle \in \prod \langle X, Y \rangle$.

(7) If $z \in \prod \langle X, Y \rangle$, then there exist x, y such that $x \in X$ and $y \in Y$ and $z = \langle x, y \rangle$.

Let D be a set. The functor binop D yielding a binary operation on D is defined by:

(Def. 1) $\operatorname{binop} D = D \times D \longmapsto$ the element of D.

Let D be a set. Observe that binop D is associative and commutative.

Let D be a set. One can verify that there exists a binary operation on D which is associative and commutative.

2. Conjunctive Normed Spaces

We introduce conjunctive normed algebra structures which are extensions of normed algebra structures and are systems

⟨ a carrier, a multiplication, an addition, an external multiplication, a one, a zero, a norm, a conjugate ⟩,

where the carrier is a set, the multiplication and the addition are binary operations on the carrier, the external multiplication is a function from $\mathbb{R} \times$ the carrier into the carrier, the one and the zero are elements of the carrier, the norm is a function from the carrier into $\mathbb{R}$, and the conjugate is a function from the carrier into the carrier.

Let us observe that there exists a conjunctive normed algebra structure which is non trivial and strict.

We use the following convention: N is a non empty conjunctive normed algebra structure and a, a_1, a_2, b, b_1, b_2 are elements of N.

Let N be a non empty conjunctive normed algebra structure and let a be an element of N. The functor $\overline{a}$ yields an element of N and is defined as follows:

(Def. 2) $\overline{a} = (\text{the conjugate of } N)(a)$.

Let N be a non empty conjunctive normed algebra structure and let a be an element of N. We say that a is properly conjugated if and only if:

(Def. 3)(i) $\overline{a} \cdot a = \|a\|^{\mathbf{2}} \cdot 1_N$ if a is non zero,

(ii) $\overline{a}$ is zero, otherwise.

Let N be a non empty conjunctive normed algebra structure. We say that N is properly conjugated if and only if:

(Def. 4) Every element of N is properly conjugated.

We say that N is additively conjugative if and only if:

(Def. 5) For all elements a, b of N holds $\overline{a+b} = \overline{a} + \overline{b}$.

We say that N is norm-wise conjugative if and only if:

(Def. 6) For every element a of N holds $\|\overline{a}\| = \|a\|$.

We say that N is scalar-wise conjugative if and only if:

(Def. 7) For every real number r and for every element a of N holds $r \cdot \overline{a} = \overline{r \cdot a}$.

Let D be a real-membered set, let a, m be binary operations on D, let M be a function from $\mathbb{R} \times D$ into D, let O, Z be elements of D, let n be a function from D into $\mathbb{R}$, and let c be a function from D into D. Observe that $\langle D, m, a, M, O, Z, n, c \rangle$ is real-membered.

Let D be a set, let a be an associative binary operation on D, let m be a binary operation on D, let M be a function from $\mathbb{R} \times D$ into D, let O, Z be elements of D, let n be a function from D into $\mathbb{R}$, and let c be a function from D into D. Observe that $\langle D, m, a, M, O, Z, n, c \rangle$ is add-associative.

Let D be a set, let a be a commutative binary operation on D, let m be a binary operation on D, let M be a function from $\mathbb{R} \times D$ into D, let O, Z be elements of D, let n be a function from D into $\mathbb{R}$, and let c be a function from D into D. Observe that $\langle D, m, a, M, O, Z, n, c \rangle$ is Abelian.

Let D be a set, let a be a binary operation on D, let m be an associative binary operation on D, let M be a function from $\mathbb{R} \times D$ into D, let O, Z be elements of D, let n be a function from D into $\mathbb{R}$, and let c be a function from D into D. One can verify that $\langle D, m, a, M, O, Z, n, c \rangle$ is associative.

Let D be a set, let a be a binary operation on D, let m be a commutative binary operation on D, let M be a function from $\mathbb{R} \times D$ into D, let O, Z be elements of D, let n be a function from D into $\mathbb{R}$, and let c be a function from D into D. One can check that $\langle D, m, a, M, O, Z, n, c \rangle$ is commutative.

The strict conjunctive normed algebra structure N-Real is defined by:

(Def. 8) N-Real $= \langle \mathbb{R}, \cdot_{\mathbb{R}}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, 1(\in \mathbb{R}), 0(\in \mathbb{R}), |\Box|_{\mathbb{R}}, \mathrm{id}_{\mathbb{R}} \rangle$.

Let us observe that N-Real is non degenerated, real-membered, add-associative, Abelian, associative, and commutative. Let a, b be elements of N-Real and r, s be real numbers. We identify $r+s$ with $a+b$ where $a = r$ and $b = s$. We identify $r \cdot s$ with $a \cdot b$ where $a = r$ and $b = s$.

One can check the following observations:

* every Abelian non empty additive magma which is right add-cancelable is also left add-cancelable,

* every Abelian non empty additive magma which is left add-cancelable is also right add-cancelable,
* every Abelian non empty additive loop structure which is left complementable is also right complementable,
* every Abelian commutative non empty double loop structure which is left distributive is also right distributive,
* every Abelian commutative non empty double loop structure which is right distributive is also left distributive,
* every commutative non empty multiplicative loop with zero structure which is almost left invertible is also almost right invertible,
* every commutative non empty multiplicative loop with zero structure which is almost right invertible is also almost left invertible,
* every commutative non empty multiplicative loop with zero structure which is almost right cancelable is also almost left cancelable,
* every commutative non empty multiplicative loop with zero structure which is almost left cancelable is also almost right cancelable,
* every commutative non empty multiplicative magma which is right mult-cancelable is also left mult-cancelable, and
* every commutative non empty multiplicative magma which is left mult-cancelable is also right mult-cancelable.

One can verify that N-Real is right complementable and right add-cancelable.

We identify $-r$ with $-a$ where $a = r$.

We identify $r - s$ with $a - b$ where $a = r$ and $b = s$.

We identify $r \cdot s$ with $r \cdot a$ where $a = s$.

We identify $|a|$ with $\|a\|$.

The following proposition is true

(8) For every element a of N-Real holds $a \cdot a = \|a\|^{\mathbf{2}}$.

Let us observe that $\overline{a}$ reduces to a.

One can verify that N-Real is reflexive, discernible, well unital, real normed space-like, right zeroed, right distributive, vector associative, vector distributive, scalar distributive, scalar associative, scalar unital, Banach Algebra-like1, Banach Algebra-like2, Banach Algebra-like3, almost left invertible, almost left cancelable, properly conjugated, additively conjugative, norm-wise conjugative, and scalar-wise conjugative.

One can verify that there exists a non empty conjunctive normed algebra structure which is strict, non degenerated, real-membered, reflexive, discernible, zeroed, complementable, add-associative, Abelian, associative, commutative, distributive, well unital, add-cancelable, vector associative, vector distributive, scalar distributive, scalar associative, scalar unital, Banach Algebra-like1, Banach Algebra-like2, Banach Algebra-like3, properly conjugated, additively conjugative, norm-wise conjugative, scalar-wise conjugative, almost left invertible, almost left cancelable, and real normed space-like.

One can check that $0_{\text{N-Real}}$ is non left invertible and non right invertible.

We identify r^{-1} with a^{-1} where $a = r$.

Let X be a discernible non trivial conjunctive normed algebra structure and let x be a non zero element of X. One can check that $\|x\|$ is non zero.

Let us mention that every non zero element of N-Real is non empty.

Let us observe that every non zero element of N-Real is mult-cancelable.

Let N be a properly conjugated non empty conjunctive normed algebra structure. Observe that every element of N is properly conjugated.

Let N be a properly conjugated non empty conjunctive normed algebra structure and let a be a zero element of N. Observe that $\overline{a}$ is zero.

Let us observe that $\overline{0_N}$ reduces to 0_N.

Let N be a properly conjugated discernible add-associative right zeroed right complementable left distributive scalar distributive scalar associative scalar unital vector distributive non degenerated conjunctive normed algebra structure and let a be a non zero element of N. Note that $\overline{a}$ is non zero.

The following propositions are true:

(9) Suppose that N is add-associative, right zeroed, right complementable, properly conjugated, reflexive, scalar distributive, scalar unital, vector distributive, and left distributive. Let given a. Then $\overline{a} \cdot a = \|a\|^{\mathbf{2}} \cdot 1_N$.

Let N be left unital Banach Algebra-like2 almost right cancelable properly conjugated scalar unital nonempty conjunctive normed algebra structure. Let us observe that $\overline{\overline{a}}$ reduces to a.

Let N be right unital Banach Algebra-like2 almost right cancelable properly conjugated scalar unital nonempty conjunctive normed algebra structure. Let us observe that $\overline{1_N}$ reduces to 1_N.

(10) Suppose that N is properly conjugated, reflexive, discernible, real normed space-like, vector distributive, scalar distributive, scalar associative, scalar unital, Abelian, add-associative, right zeroed, right complementable, associative, distributive, well unital, non degenerated, and almost left invertible. Then $\overline{-a} = -\overline{a}$.

(11) Suppose that N is properly conjugated, reflexive, discernible, real normed space-like, vector distributive, scalar distributive, scalar associative, scalar unital, Abelian, add-associative, right zeroed, right complementable, associative, distributive, well unital, non degenerated, almost left invertible, and additively conjugative. Then $\overline{a - b} = \overline{a} - \overline{b}$.

3. Cayley-Dickson Construction

Let N be a non empty conjunctive normed algebra structure. The functor Cayley-Dickson N yielding a strict conjunctive normed algebra structure is defined by the conditions (Def. 9).

(Def. 9)(i) The carrier of Cayley-Dickson $N = \prod\langle$the carrier of N, the carrier of $N\rangle$,

(ii) the zero of Cayley-Dickson $N = \langle 0_N, 0_N\rangle$,

(iii) the one of Cayley-Dickson $N = \langle 1_N, 0_N\rangle$,

(iv) for all elements a_1, a_2, b_1, b_2 of N holds (the addition of Cayley-Dickson N)$(\langle a_1, b_1\rangle, \langle a_2, b_2\rangle) = \langle a_1 + a_2, b_1 + b_2\rangle$ and (the multiplication of Cayley-Dickson N)$(\langle a_1, b_1\rangle, \langle a_2, b_2\rangle) = \langle a_1 \cdot a_2 - \overline{b_2} \cdot b_1, b_2 \cdot a_1 + b_1 \cdot \overline{a_2}\rangle$,

(v) for every real number r and for all elements a, b of N holds (the external multiplication of Cayley-Dickson N)$(r, \langle a, b\rangle) = \langle r \cdot a, r \cdot b\rangle$, and

(vi) for all elements a, b of N holds (the norm of Cayley-Dickson N)$(\langle a, b\rangle) = \sqrt{\|a\|^{\mathbf{2}} + \|b\|^{\mathbf{2}}}$ and (the conjugate of Cayley-Dickson N)$(\langle a, b\rangle) = \langle \overline{a}, -b\rangle$.

In the sequel c, c_1, c_2 are elements of Cayley-Dickson N.

Let N be a non empty conjunctive normed algebra structure. Note that Cayley-Dickson N is non empty.

We now state two propositions:

(12) There exist elements a, b of N such that $c = \langle a, b\rangle$.

(13) For every element c of Cayley-Dickson Cayley-Dickson N there exist a_1, b_1, a_2, b_2 such that $c = \langle\langle a_1, b_1\rangle, \langle a_2, b_2\rangle\rangle$.

Let us consider N, a, b. Then $\langle a, b\rangle$ is an element of Cayley-Dickson N.

Let us consider N and let a, b be zero elements of N. Observe that $\langle a, b\rangle$ is zero.

Let N be a non degenerated non empty conjunctive normed algebra structure, let a be a non zero element of N, and let b be an element of N. One can check that $\langle a, b\rangle$ is non zero.

Let N be a reflexive non empty conjunctive normed algebra structure. Note that Cayley-Dickson N is reflexive.

Let N be a discernible non empty conjunctive normed algebra structure. Observe that Cayley-Dickson N is discernible.

We now state a number of propositions:

(14) If a is left complementable and b is left complementable, then $\langle a, b\rangle$ is left complementable.

(15) If $\langle a, b\rangle$ is left complementable, then a is left complementable and b is left complementable.

(16) If a is right complementable and b is right complementable, then $\langle a, b\rangle$ is right complementable.

(17) If $\langle a, b\rangle$ is right complementable, then a is right complementable and b is right complementable.

(18) If a is complementable and b is complementable, then $\langle a, b\rangle$ is complementable.

(19) If $\langle a, b\rangle$ is complementable, then a is complementable and b is complementable.

(20) If a is left add-cancelable and b is left add-cancelable, then $\langle a, b\rangle$ is left add-cancelable.

(21) If $\langle a, b\rangle$ is left add-cancelable, then a is left add-cancelable and b is left add-cancelable.

(22) If a is right add-cancelable and b is right add-cancelable, then $\langle a, b\rangle$ is right add-cancelable.

(23) If $\langle a, b\rangle$ is right add-cancelable, then a is right add-cancelable and b is right add-cancelable.

(24) If a is add-cancelable and b is add-cancelable, then $\langle a, b\rangle$ is add-cancelable.

(25) If $\langle a, b\rangle$ is add-cancelable, then a is add-cancelable and b is add-cancelable.

(26) If $\langle a, b\rangle$ is left complementable and right add-cancelable, then $-\langle a, b\rangle = \langle -a, -b\rangle$.

Let N be an add-associative non empty conjunctive normed algebra structure. Observe that Cayley-Dickson N is add-associative.

Let N be a right zeroed non empty conjunctive normed algebra structure. Observe that Cayley-Dickson N is right zeroed.

Let N be a left zeroed non empty conjunctive normed algebra structure. One can verify that Cayley-Dickson N is left zeroed.

Let N be a right complementable non empty conjunctive normed algebra structure. One can check that Cayley-Dickson N is right complementable.

Let N be a left complementable non empty conjunctive normed algebra structure. One can check that Cayley-Dickson N is left complementable.

Let N be an Abelian non empty conjunctive normed algebra structure. Observe that Cayley-Dickson N is Abelian.

One can prove the following propositions:

(27) If N is add-associative, right zeroed, and right complementable, then $-\langle a, b\rangle = \langle -a, -b\rangle$.

(28) If N is add-associative, right zeroed, and right complementable, then $\langle a_1, b_1\rangle - \langle a_2, b_2\rangle = \langle a_1 - a_2, b_1 - b_2\rangle$.

Let N be a well unital add-associative right zeroed right complementable distributive Banach Algebra-like2 properly conjugated scalar unital almost right cancelable non empty conjunctive normed algebra structure. Observe that

Cayley-Dickson N is well unital.

Let N be a non degenerated non empty conjunctive normed algebra structure. One can check that Cayley-Dickson N is non degenerated.

Let N be an additively conjugative add-associative right zeroed right complementable Abelian non empty conjunctive normed algebra structure. One can verify that Cayley-Dickson N is additively conjugative.

Let N be a norm-wise conjugative reflexive discernible real normed space-like vector distributive scalar distributive scalar associative scalar unital Abelian add-associative right zeroed right complementable non empty conjunctive normed algebra structure. Observe that Cayley-Dickson N is norm-wise conjugative.

Let N be a scalar-wise conjugative add-associative right zeroed right complementable Abelian scalar distributive scalar associative scalar unital vector distributive non empty conjunctive normed algebra structure. One can check that Cayley-Dickson N is scalar-wise conjugative.

Let N be a distributive add-associative right zeroed right complementable Abelian non empty conjunctive normed algebra structure.

Note that Cayley-Dickson N is left distributive.

Let N be a distributive add-associative right zeroed right complementable additively conjugative Abelian non empty conjunctive normed algebra structure. Note that Cayley-Dickson N is right distributive.

Let N be a reflexive discernible real normed space-like vector distributive scalar distributive scalar associative scalar unital Abelian add-associative right zeroed right complementable non empty conjunctive normed algebra structure. One can check that Cayley-Dickson N is real normed space-like.

Let N be a vector distributive non empty conjunctive normed algebra structure. Observe that Cayley-Dickson N is vector distributive.

Let N be a vector associative Banach Algebra-like3 add-associative right zeroed right complementable Abelian scalar distributive scalar associative scalar unital vector distributive non empty conjunctive normed algebra structure. Observe that Cayley-Dickson N is vector associative.

Let N be a scalar distributive non empty conjunctive normed algebra structure. One can verify that Cayley-Dickson N is scalar distributive.

Let N be a scalar associative non empty conjunctive normed algebra structure. Note that Cayley-Dickson N is scalar associative.

Let N be a scalar unital non empty conjunctive normed algebra structure. One can check that Cayley-Dickson N is scalar unital.

Let N be a reflexive Banach Algebra-like2 non empty conjunctive normed algebra structure. Observe that Cayley-Dickson N is Banach Algebra-like2.

Let N be a Banach Algebra-like3 add-associative right zeroed right complementable Abelian scalar distributive scalar associative scalar unital vector distributive vector associative scalar-wise conjugative non empty conjunctive normed algebra structure. Observe that Cayley-Dickson N is Banach Algebra-like3.

Next we state the proposition

(29) Let N be an almost left invertible associative add-associative right zeroed right complementable well unital distributive Abelian scalar distributive scalar associative scalar unital vector distributive vector associative reflexive discernible real normed space-like almost right cancelable properly conjugated additively conjugative Banach Algebra-like2 Banach Algebra-like3 non degenerated conjunctive normed algebra structure and a, b be elements of N. Suppose a is non zero or b is non zero but $\langle a, b\rangle$ is right mult-cancelable and left invertible. Then $\langle a, b\rangle^{-1} = \langle \frac{1}{\|a\|^2+\|b\|^2} \cdot \overline{a}, \frac{1}{\|a\|^2+\|b\|^2} \cdot -b\rangle$.

Let N be an add-associative right zeroed right complementable distributive scalar distributive scalar unital vector distributive discernible reflexive properly conjugated non empty conjunctive normed algebra structure. Note that Cayley-Dickson N is properly conjugated.

Let us mention that Cayley-Dickson N-Real is associative and commutative.

The following propositions are true:

(30) $\langle\langle 0_{\text{N-Real}}, 1_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle \cdot \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 1_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle = \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 1_{\text{N-Real}}\rangle\rangle$.

(31) $\langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 1_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle \cdot \langle\langle 0_{\text{N-Real}}, 1_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle = \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, -1_{\text{N-Real}}\rangle\rangle$.

One can verify that Cayley-Dickson Cayley-Dickson N-Real is associative and non commutative.

We now state four propositions:

(32) $\langle\langle\langle 0_{\text{N-Real}}, 1_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle \cdot \langle\langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 1_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle = \langle\langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 1_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle$.

(33) $\langle\langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 1_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle \cdot \langle\langle\langle 0_{\text{N-Real}}, 1_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle = \langle\langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, -1_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle$.

(34) $\langle\langle\langle 0_{\text{N-Real}}, 1_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle \cdot \langle\langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 1_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle \cdot \langle\langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 1_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle = \langle\langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle -1_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle$.

(35) $\langle\langle\langle 0_{\text{N-Real}}, 1_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle \cdot (\langle\langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 1_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle \cdot \langle\langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 1_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle) = \langle\langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle, \langle\langle 0_{\text{N-Real}}, 0_{\text{N-Real}}\rangle, \langle 1_{\text{N-Real}}, 0_{\text{N-Real}}\rangle\rangle\rangle$.

One can check that Cayley-Dickson Cayley-Dickson Cayley-Dickson N-Real is non associative and non commutative.

References

[1] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[8] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[9] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[10] Agata Darmochwał and Yatsuka Nakamura. Metric spaces as topological spaces – fundamental concepts. *Formalized Mathematics*, 2(**4**):605–608, 1991.
[11] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[12] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.
[13] Henryk Oryszczyszyn and Krzysztof Prażmowski. Real functions spaces. *Formalized Mathematics*, 1(**3**):555–561, 1990.
[14] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[15] Yasunari Shidama. The Banach algebra of bounded linear operators. *Formalized Mathematics*, 12(**2**):103–108, 2004.
[16] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[17] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[18] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[19] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[20] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[22] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.
[23] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received August 6, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 4, Pages 291–301, 2012
DOI: 10.2478/v10037-012-0035-8

VERSITA
versita.com/fm/

Contracting Mapping on Normed Linear Space[1]

Keiichi Miyajima
Ibaraki University
Faculty of Engineering
Hitachi, Japan

Artur Korniłowicz[2]
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

Yasunari Shidama[3]
Shinshu University
Nagano, Japan

Summary. In this article, we described the contracting mapping on normed linear space. Furthermore, we applied that mapping to ordinary differential equations on real normed space. Our method is based on the one presented by Schwarz [29].

MML identifier: ORDEQ_01, version: 8.0.01 5.3.1162

The papers [28], [3], [20], [8], [26], [32], [4], [5], [18], [16], [17], [12], [34], [30], [2], [33], [23], [15], [22], [21], [24], [19], [25], [1], [6], [10], [13], [27], [9], [38], [39], [35], [36], [11], [31], [37], [14], and [7] provide the notation and terminology for this paper.

1. The Principle of Contracting Mapping on Normed Linear Space

We use the following convention: n denotes a non empty element of $\mathbb{N}$ and a, b, r, t denote real numbers.

[1]We would like to express our gratitude to Prof. Yatsuka Nakamura.
[2]My work has been supported by the Polish Ministry of Science and Higher Education project “Managing a Large Repository of Computer-verified Mathematical Knowledge” (N N519 385136).
[3]My work has been supported by JSPS KAKENHI 22300285.

ISSN 1426–2630(p), 1898-9934(e)

Let f be a function. We say that f has unique fixpoint if and only if:

(Def. 1) There exists a set x such that x is a fixpoint of f and for every set y such that y is a fixpoint of f holds $x = y$.

Next we state two propositions:

(1) Every set x is a fixpoint of $\{\langle x, x\rangle\}$.

(2) For all sets x, y, z such that x is a fixpoint of $\{\langle y, z\rangle\}$ holds $x = y$.

Let x be a set. Observe that $\{\langle x, x\rangle\}$ has unique fixpoint.

Next we state three propositions:

(3) Let X be a real normed space and x be a point of X. If for every real number e such that $e > 0$ holds $\|x\| < e$, then $x = 0_X$.

(4) Let X be a real normed space and x, y be points of X. If for every real number e such that $e > 0$ holds $\|x - y\| < e$, then $x = y$.

(5) For all real numbers K, L, e such that $0 < K < 1$ and $0 < e$ there exists a natural number n such that $|L \cdot K^n| < e$.

Let X be a real normed space. Note that every function from X into X which is constant is also contraction.

Let X be a real Banach space. One can verify that every function from X into X which is contraction also has unique fixpoint.

One can prove the following three propositions:

(6) Let X be a real Banach space and f be a function from X into X. Suppose f is contraction. Then there exists a point x_1 of X such that $f(x_1) = x_1$ and for every point x of X such that $f(x) = x$ holds $x_1 = x$.

(7) Let X be a real Banach space and f be a function from X into X such that there exists a natural number n_0 such that f^{n_0} is contraction. Then f has unique fixpoint.

(8) Let X be a real Banach space and f be a function from X into X. Given an element n_0 of $\mathbb{N}$ such that f^{n_0} is contraction. Then there exists a point x_1 of X such that $f(x_1) = x_1$ and for every point x of X such that $f(x) = x$ holds $x_1 = x$.

2. The Real Banach Space C([a,b],X)

We now state the proposition

(9) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, and f be a continuous partial function from $\mathbb{R}$ to Y. If $\operatorname{dom} f = X$, then f is a bounded function from X into Y.

Let X be a non empty closed interval subset of $\mathbb{R}$ and let Y be a real normed space. The continuous functions of X and Y yields a subset of the set of bounded real sequences from X into Y and is defined by the condition (Def. 2).

(Def. 2) Let x be a set. Then $x \in$ the continuous functions of X and Y if and only if there exists a continuous partial function f from $\mathbb{R}$ to Y such that $x = f$ and $\operatorname{dom} f = X$.

Let X be a non empty closed interval subset of $\mathbb{R}$ and let Y be a real normed space. Note that the continuous functions of X and Y is non empty.

Let X be a non empty closed interval subset of $\mathbb{R}$ and let Y be a real normed space. Observe that the continuous functions of X and Y is linearly closed.

Let X be a non empty closed interval subset of $\mathbb{R}$ and let Y be a real normed space. The $\mathbb{R}$-vector space of continuous functions of X and Y yielding a strict real linear space is defined by the condition (Def. 3).

(Def. 3) The $\mathbb{R}$-vector space of continuous functions of X and Y = $\langle$the continuous functions of X and Y, Zero(the continuous functions of X and Y, the set of bounded real sequences from X into Y), Add(the continuous functions of X and Y, the set of bounded real sequences from X into Y), Mult(the continuous functions of X and Y, the set of bounded real sequences from X into Y)$\rangle$.

Let X be a non empty closed interval subset of $\mathbb{R}$ and let Y be a real normed space. Observe that the $\mathbb{R}$-vector space of continuous functions of X and Y is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

One can prove the following three propositions:

(10) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, f, g, h be vectors of the $\mathbb{R}$-vector space of continuous functions of X and Y, and f_9, g_9, h_9 be continuous partial functions from $\mathbb{R}$ to Y. Suppose $f_9 = f$ and $g_9 = g$ and $h_9 = h$ and $\operatorname{dom} f_9 = X$ and $\operatorname{dom} g_9 = X$ and $\operatorname{dom} h_9 = X$. Then $h = f + g$ if and only if for every element x of X holds $(h_9)_x = (f_9)_x + (g_9)_x$.

(11) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, f, h be vectors of the $\mathbb{R}$-vector space of continuous functions of X and Y, and f_9, h_9 be continuous partial functions from $\mathbb{R}$ to Y. Suppose $f_9 = f$ and $h_9 = h$ and $\operatorname{dom} f_9 = X$ and $\operatorname{dom} h_9 = X$. Then $h = a \cdot f$ if and only if for every element x of X holds $(h_9)_x = a \cdot (f_9)_x$.

(12) Let X be a non empty closed interval subset of $\mathbb{R}$ and Y be a real normed space. Then $0_{\text{the } \mathbb{R}\text{-vector space of continuous functions of } X \text{ and } Y} = X \longmapsto 0_Y$.

Let X be a non empty closed interval subset of $\mathbb{R}$ and let Y be a real normed space. The continuous functions norm of X and Y yields a function from the continuous functions of X and Y into $\mathbb{R}$ and is defined as follows:

(Def. 4) The continuous functions norm of X and $Y = \mathrm{BdFuncsNorm}(X, Y) \restriction$the continuous functions of X and Y.

Let X be a non empty closed interval subset of $\mathbb{R}$, let Y be a real normed space, and let f be a set. Let us assume that $f \in$ the continuous functions of X and Y. The functor modetrans(f, X, Y) yielding a continuous partial function from $\mathbb{R}$ to Y is defined by:

(Def. 5) modetrans$(f, X, Y) = f$ and dom modetrans$(f, X, Y) = X$.

Let X be a non empty closed interval subset of $\mathbb{R}$ and let Y be a real normed space. The $\mathbb{R}$-norm space of continuous functions of X and Y yields a strict non empty normed structure and is defined by the condition (Def. 6).

(Def. 6) The $\mathbb{R}$-norm space of continuous functions of X and $Y = \langle$the continuous functions of X and Y, Zero(the continuous functions of X and Y, the set of bounded real sequences from X into Y), Add(the continuous functions of X and Y, the set of bounded real sequences from X into Y), Mult(the continuous functions of X and Y, the set of bounded real sequences from X into Y), the continuous functions norm of X and $Y\rangle$.

We now state several propositions:

(13) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, and f be a continuous partial function from $\mathbb{R}$ to Y. If dom $f = X$, then modetrans$(f, X, Y) = f$.

(14) Let X be a non empty closed interval subset of $\mathbb{R}$ and Y be a real normed space. Then $X \longmapsto 0_Y = 0_{\text{the } \mathbb{R}\text{-norm space of continuous functions of } X \text{ and } Y}$.

(15) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, f, g, h be points of the $\mathbb{R}$-norm space of continuous functions of X and Y, and f_9, g_9, h_9 be continuous partial functions from $\mathbb{R}$ to Y. Suppose $f_9 = f$ and $g_9 = g$ and $h_9 = h$ and dom $f_9 = X$ and dom $g_9 = X$ and dom $h_9 = X$. Then $h = f + g$ if and only if for every element x of X holds $(h_9)_x = (f_9)_x + (g_9)_x$.

(16) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, f, h be points of the $\mathbb{R}$-norm space of continuous functions of X and Y, and f_9, h_9 be continuous partial functions from $\mathbb{R}$ to Y. Suppose $f_9 = f$ and $h_9 = h$ and dom $f_9 = X$ and dom $h_9 = X$. Then $h = a \cdot f$ if and only if for every element x of X holds $(h_9)_x = a \cdot (f_9)_x$.

(17) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, f be a point of the $\mathbb{R}$-norm space of continuous functions of X and Y, and g be a point of the real normed space of bounded functions from X into Y. If $f = g$, then $\|f\| = \|g\|$.

(18) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, f, g be points of the $\mathbb{R}$-norm space of continuous functions of X and Y, and f_1, g_1 be points of the real normed space of bounded functions from X into Y. If $f_1 = f$ and $g_1 = g$, then $f + g = f_1 + g_1$.

(19) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, f be a point of the $\mathbb{R}$-norm space of continuous functions of X and

Y, and f_1 be a point of the real normed space of bounded functions from X into Y. If $f_1 = f$, then $a \cdot f = a \cdot f_1$.

Let X be a non empty closed interval subset of $\mathbb{R}$ and let Y be a real normed space. Observe that the $\mathbb{R}$-norm space of continuous functions of X and Y is reflexive, discernible, real normed space-like, vector distributive, scalar distributive, scalar associative, scalar unital, Abelian, add-associative, right zeroed, and right complementable.

One can prove the following propositions:

(20) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, f, g, h be points of the $\mathbb{R}$-norm space of continuous functions of X and Y, and f_9, g_9, h_9 be continuous partial functions from $\mathbb{R}$ to Y. Suppose $f_9 = f$ and $g_9 = g$ and $h_9 = h$ and $\operatorname{dom} f_9 = X$ and $\operatorname{dom} g_9 = X$ and $\operatorname{dom} h_9 = X$. Then $h = f - g$ if and only if for every element x of X holds $(h_9)_x = (f_9)_x - (g_9)_x$.

(21) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, f, g be points of the $\mathbb{R}$-norm space of continuous functions of X and Y, and f_1, g_1 be points of the real normed space of bounded functions from X into Y. If $f_1 = f$ and $g_1 = g$, then $f - g = f_1 - g_1$.

Let X be a non empty closed interval subset of $\mathbb{R}$ and let Y be a real normed space. Note that there exists a subset of the real normed space of bounded functions from X into Y which is closed.

The following two propositions are true:

(22) Let X be a non empty closed interval subset of $\mathbb{R}$ and Y be a real normed space. Then the continuous functions of X and Y is a closed subset of the real normed space of bounded functions from X into Y.

(23) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, and s_1 be a sequence of the $\mathbb{R}$-norm space of continuous functions of X and Y. Suppose Y is complete and s_1 is Cauchy sequence by norm. Then s_1 is convergent.

Let X be a non empty closed interval subset of $\mathbb{R}$ and let Y be a real Banach space. One can check that the $\mathbb{R}$-norm space of continuous functions of X and Y is complete.

We now state four propositions:

(24) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, v be a point of the $\mathbb{R}$-norm space of continuous functions of X and Y, and g be a partial function from $\mathbb{R}$ to Y. If $g = v$, then for every real number t such that $t \in X$ holds $\|g_t\| \leq \|v\|$.

(25) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, K be a real number, v be a point of the $\mathbb{R}$-norm space of continuous functions of X and Y, and g be a partial function from $\mathbb{R}$ to Y. Suppose

$g = v$ and for every real number t such that $t \in X$ holds $\|g_t\| \leq K$. Then $\|v\| \leq K$.

(26) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, v_1, v_2 be points of the $\mathbb{R}$-norm space of continuous functions of X and Y, and g_1, g_2 be partial functions from $\mathbb{R}$ to Y. Suppose $g_1 = v_1$ and $g_2 = v_2$. Let t be a real number. If $t \in X$, then $\|(g_1)_t - (g_2)_t\| \leq \|v_1 - v_2\|$.

(27) Let X be a non empty closed interval subset of $\mathbb{R}$, Y be a real normed space, K be a real number, v_1, v_2 be points of the $\mathbb{R}$-norm space of continuous functions of X and Y, and g_1, g_2 be partial functions from $\mathbb{R}$ to Y. Suppose $g_1 = v_1$ and $g_2 = v_2$ and for every real number t such that $t \in X$ holds $\|(g_1)_t - (g_2)_t\| \leq K$. Then $\|v_1 - v_2\| \leq K$.

3. Differential Equations

The following propositions are true:

(28) Let n, i be natural numbers, f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$, and A be a subset of $\mathbb{R}$. Then $\mathrm{proj}(i,n) \cdot (f{\restriction}A) = (\mathrm{proj}(i,n) \cdot f){\restriction}A$.

(29) For every continuous partial function g from $\mathbb{R}$ to $\mathcal{R}^n$ such that $\mathrm{dom}\, g = [a,b]$ holds $g{\restriction}[a,b]$ is bounded.

(30) For every continuous partial function g from $\mathbb{R}$ to $\mathcal{R}^n$ such that $\mathrm{dom}\, g = [a,b]$ holds g is integrable on $[a,b]$.

(31) Let f, F be partial functions from $\mathbb{R}$ to $\mathcal{R}^n$. Suppose $a \leq b$ and $\mathrm{dom}\, f = [a,b]$ and $\mathrm{dom}\, F = [a,b]$ and f is continuous and for every real number t such that $t \in [a,b]$ holds $F(t) = \int\limits_a^t f(x)dx$. Let x be a real number. If $x \in [a,b]$, then F is continuous in x.

(32) For every continuous partial function f from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ such that $\mathrm{dom}\, f = [a,b]$ holds $f{\restriction}[a,b]$ is bounded.

(33) For every continuous partial function f from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ such that $\mathrm{dom}\, f = [a,b]$ holds f is integrable on $[a,b]$.

(34) Let f be a continuous partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and F be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $a \leq b$ and $\mathrm{dom}\, f = [a,b]$ and $\mathrm{dom}\, F = [a,b]$ and for every real number t such that $t \in [a,b]$ holds $F(t) = \int\limits_a^t f(x)dx$. Let x be a real number. If $x \in [a,b]$, then F is continuous in x.

(35) Let R be a partial function from $\mathbb{R}$ to $\mathbb{R}$. Suppose R is total. Then R is rest-like if and only if for every real number r such that $r > 0$ there exists

a real number d such that $d > 0$ and for every real number z such that $z \neq 0$ and $|z| < d$ holds $|z|^{-1} \cdot |R_z| < r$.

In the sequel Z denotes an open subset of $\mathbb{R}$, y_0 denotes a vector of $\langle \mathcal{E}^n, \|\cdot\| \rangle$, and G denotes a function from $\langle \mathcal{E}^n, \|\cdot\| \rangle$ into $\langle \mathcal{E}^n, \|\cdot\| \rangle$.

One can prove the following propositions:

(36) Let f be a continuous partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $a \leq b$ and $\operatorname{dom} f = [a, b]$ and $\operatorname{dom} g = [a, b]$ and $Z =]a, b[$ and for every real number t such that $t \in [a, b]$ holds $g(t) = y_0 + \int\limits_a^t f(x)dx$. Then g is continuous and $g_a = y_0$ and g is differentiable on Z and for every real number t such that $t \in Z$ holds $g'(t) = f_t$.

(37) For every natural number i and for all points y_1, y_2 of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ holds $(\operatorname{proj}(i, n))(y_1 + y_2) = (\operatorname{proj}(i, n))(y_1) + (\operatorname{proj}(i, n))(y_2)$.

(38) For every natural number i and for every point y_1 of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and for every real number r holds $(\operatorname{proj}(i, n))(r \cdot y_1) = r \cdot (\operatorname{proj}(i, n))(y_1)$.

(39) Let g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, x_0 be a real number, and i be a natural number. Suppose $1 \leq i \leq n$ and g is differentiable in x_0. Then $\operatorname{proj}(i, n) \cdot g$ is differentiable in x_0 and $(\operatorname{proj}(i, n))(g'(x_0)) = (\operatorname{proj}(i, n) \cdot g)'(x_0)$.

(40) Let f be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and X be a set. Suppose that for every natural number i such that $1 \leq i \leq n$ holds $(\operatorname{proj}(i, n) \cdot f) \restriction X$ is constant. Then $f \restriction X$ is constant.

(41) Let f be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $]a, b[\subseteq \operatorname{dom} f$ and f is differentiable on $]a, b[$ and for every real number x such that $x \in]a, b[$ holds $f'(x) = 0_{\langle \mathcal{E}^n, \|\cdot\| \rangle}$. Then $f \restriction]a, b[$ is constant.

(42) Let f be a continuous partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $a < b$ and $[a, b] = \operatorname{dom} f$ and $f \restriction]a, b[$ is constant. Let x be a real number. If $x \in [a, b]$, then $f(x) = f(a)$.

(43) Let y, G_1 be continuous partial functions from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and g be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose that $a < b$ and $Z =]a, b[$ and $\operatorname{dom} y = [a, b]$ and $\operatorname{dom} g = [a, b]$ and $\operatorname{dom} G_1 = [a, b]$ and y is differentiable on Z and $y_a = y_0$ and for every real number t such that $t \in Z$ holds $y'(t) = (G_1)_t$ and for every real number t such that $t \in [a, b]$ holds $g(t) = y_0 + \int\limits_a^t G_1(x)dx$. Then $y = g$.

(44) Let a, b, c, d be real numbers and f be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose that $a \leq b$ and f is integrable on $[a, b]$ and $\|f\|$ is integrable on $[a, b]$ and $f \restriction [a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$ and c, $d \in [a, b]$. Then

$\|f\|$ is integrable on $[\min(c,d), \max(c,d)]$ and $\|f\|\restriction[\min(c,d), \max(c,d)]$ is bounded and $\|\int\limits_c^d f(x)dx\| \leq \int\limits_{\min(c,d)}^{\max(c,d)} \|f\|(x)dx$.

(45) Let a, b, c, d, e be real numbers and f be a partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose that $a \leq b$ and $c \leq d$ and f is integrable on $[a,b]$ and $\|f\|$ is integrable on $[a,b]$ and $f\restriction[a,b]$ is bounded and $[a,b] \subseteq \operatorname{dom} f$ and c, $d \in [a,b]$ and for every real number x such that $x \in [c,d]$ holds $\|f_x\| \leq e$. Then $\|\int\limits_c^d f(x)dx\| \leq e \cdot (d-c)$ and $\|\int\limits_d^c f(x)dx\| \leq e \cdot (d-c)$.

(46) Let n be a natural number and g be a function from $\mathbb{R}$ into $\mathbb{R}$. Suppose that for every real number x holds $g(x) = (x-a)^{n+1}$. Let x be a real number. Then g is differentiable in x and $g'(x) = (n+1) \cdot (x-a)^n$.

(47) Let n be a natural number and g be a function from $\mathbb{R}$ into $\mathbb{R}$. Suppose that for every real number x holds $g(x) = \frac{(x-a)^{n+1}}{(n+1)!}$. Let x be a real number. Then g is differentiable in x and $g'(x) = \frac{(x-a)^n}{n!}$.

(48) Let f, g be partial functions from $\mathbb{R}$ to $\mathbb{R}$. Suppose that $a \leq t$ and $[a,t] \subseteq \operatorname{dom} f$ and f is integrable on $[a,t]$ and $f\restriction[a,t]$ is bounded and $[a,t] \subseteq \operatorname{dom} g$ and g is integrable on $[a,t]$ and $g\restriction[a,t]$ is bounded and for every real number x such that $x \in [a,t]$ holds $f(x) \leq g(x)$. Then $\int\limits_a^t f(x)dx \leq \int\limits_a^t g(x)dx$.

Let n be a non empty element of $\mathbb{N}$, let y_0 be a vector of $\langle \mathcal{E}^n, \|\cdot\| \rangle$, let G be a function from $\langle \mathcal{E}^n, \|\cdot\| \rangle$ into $\langle \mathcal{E}^n, \|\cdot\| \rangle$, and let a, b be real numbers. Let us assume that $a \leq b$ and G is continuous on $\operatorname{dom} G$. The functor $\operatorname{Fredholm}(G, a, b, y_0)$ yielding a function from the $\mathbb{R}$-norm space of continuous functions of $[a,b]$ and $\langle \mathcal{E}^n, \|\cdot\| \rangle$ into the $\mathbb{R}$-norm space of continuous functions of $[a,b]$ and $\langle \mathcal{E}^n, \|\cdot\| \rangle$ is defined by the condition (Def. 7).

(Def. 7) Let x be a vector of the $\mathbb{R}$-norm space of continuous functions of $[a,b]$ and $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Then there exist continuous partial functions f, g, G_1 from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ such that $x = f$ and $(\operatorname{Fredholm}(G, a, b, y_0))(x) = g$ and $\operatorname{dom} f = [a,b]$ and $\operatorname{dom} g = [a,b]$ and $G_1 = G \cdot f$ and for every real number t such that $t \in [a,b]$ holds $g(t) = y_0 + \int\limits_a^t G_1(x)dx$.

We now state several propositions:

(49) Suppose $a \leq b$ and $0 < r$ and for all vectors y_1, y_2 of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ holds $\|G_{y_1} - G_{y_2}\| \leq r \cdot \|y_1 - y_2\|$. Let u, v be vectors of the $\mathbb{R}$-norm space of continuous functions of $[a,b]$ and $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and g, h be continuous partial

functions from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $g = (\mathrm{Fredholm}(G, a, b, y_0))(u)$ and $h = (\mathrm{Fredholm}(G, a, b, y_0))(v)$. Let t be a real number. If $t \in [a, b]$, then $\|g_t - h_t\| \leq r \cdot (t - a) \cdot \|u - v\|$.

(50) Suppose $a \leq b$ and $0 < r$ and for all vectors y_1, y_2 of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ holds $\|G_{y_1} - G_{y_2}\| \leq r \cdot \|y_1 - y_2\|$. Let u, v be vectors of the $\mathbb{R}$-norm space of continuous functions of $[a, b]$ and $\langle \mathcal{E}^n, \|\cdot\| \rangle$, m be an element of $\mathbb{N}$, and g, h be continuous partial functions from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $g = (\mathrm{Fredholm}(G, a, b, y_0))^{m+1}(u)$ and $h = (\mathrm{Fredholm}(G, a, b, y_0))^{m+1}(v)$. Let t be a real number. If $t \in [a, b]$, then $\|g_t - h_t\| \leq \frac{(r \cdot (t-a))^{m+1}}{(m+1)!} \cdot \|u - v\|$.

(51) Let m be a natural number. Suppose $a \leq b$ and $0 < r$ and for all vectors y_1, y_2 of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ holds $\|G_{y_1} - G_{y_2}\| \leq r \cdot \|y_1 - y_2\|$. Let u, v be vectors of the $\mathbb{R}$-norm space of continuous functions of $[a, b]$ and $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Then $\|(\mathrm{Fredholm}(G, a, b, y_0))^{m+1}(u) - (\mathrm{Fredholm}(G, a, b, y_0))^{m+1}(v)\| \leq \frac{(r \cdot (b-a))^{m+1}}{(m+1)!} \cdot \|u - v\|$.

(52) Suppose $a < b$ and G is Lipschitzian on the carrier of $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Then there exists a natural number m such that $(\mathrm{Fredholm}(G, a, b, y_0))^{m+1}$ is contraction.

(53) If $a < b$ and G is Lipschitzian on the carrier of $\langle \mathcal{E}^n, \|\cdot\| \rangle$, then $\mathrm{Fredholm}(G, a, b, y_0)$ has unique fixpoint.

(54) Let f, g be continuous partial functions from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose $\mathrm{dom}\, f = [a, b]$ and $\mathrm{dom}\, g = [a, b]$ and $Z =]a, b[$ and $a < b$ and G is Lipschitzian on the carrier of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and $g = (\mathrm{Fredholm}(G, a, b, y_0))(f)$. Then $g_a = y_0$ and g is differentiable on Z and for every real number t such that $t \in Z$ holds $g'(t) = (G \cdot f)_t$.

(55) Let y be a continuous partial function from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose that $a < b$ and $Z =]a, b[$ and G is Lipschitzian on the carrier of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and $\mathrm{dom}\, y = [a, b]$ and y is differentiable on Z and $y_a = y_0$ and for every real number t such that $t \in Z$ holds $y'(t) = G(y_t)$. Then y is a fixpoint of $\mathrm{Fredholm}(G, a, b, y_0)$.

(56) Let y_1, y_2 be continuous partial functions from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Suppose that $a < b$ and $Z =]a, b[$ and G is Lipschitzian on the carrier of $\langle \mathcal{E}^n, \|\cdot\| \rangle$ and $\mathrm{dom}\, y_1 = [a, b]$ and y_1 is differentiable on Z and $(y_1)_a = y_0$ and for every real number t such that $t \in Z$ holds ${y_1}'(t) = G((y_1)_t)$ and $\mathrm{dom}\, y_2 = [a, b]$ and y_2 is differentiable on Z and $(y_2)_a = y_0$ and for every real number t such that $t \in Z$ holds ${y_2}'(t) = G((y_2)_t)$. Then $y_1 = y_2$.

(57) Suppose $a < b$ and $Z =]a, b[$ and G is Lipschitzian on the carrier of $\langle \mathcal{E}^n, \|\cdot\| \rangle$. Then there exists a continuous partial function y from $\mathbb{R}$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$ such that $\mathrm{dom}\, y = [a, b]$ and y is differentiable on Z and $y_a = y_0$ and for every real number t such that $t \in Z$ holds $y'(t) = G(y_t)$.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[2] Józef Białas. Properties of the intervals of real numbers. *Formalized Mathematics*, 3(**2**):263–269, 1992.
[3] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[8] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[9] Noboru Endou and Yasunari Shidama. Completeness of the real Euclidean space. *Formalized Mathematics*, 13(**4**):577–580, 2005.
[10] Noboru Endou, Yasunari Shidama, and Keiichi Miyajima. Partial differentiation on normed linear spaces $\mathcal{R}^n$. *Formalized Mathematics*, 15(**2**):65–72, 2007, doi:10.2478/v10037-007-0008-5.
[11] Noboru Endou, Yasumasa Suzuki, and Yasunari Shidama. Real linear space of real sequences. *Formalized Mathematics*, 11(**3**):249–253, 2003.
[12] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definition of integrability for partial functions from $\mathbb{R}$ to $\mathbb{R}$ and integrability for continuous functions. *Formalized Mathematics*, 9(**2**):281–284, 2001.
[13] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**):841–845, 1990.
[14] Artur Korniłowicz. Arithmetic operations on functions from sets into functional sets. *Formalized Mathematics*, 17(**1**):43–60, 2009, doi:10.2478/v10037-009-0005-y.
[15] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[16] Keiichi Miyajima, Takahiro Kato, and Yasunari Shidama. Riemann integral of functions from $\mathbb{R}$ into real normed space. *Formalized Mathematics*, 19(**1**):17–22, 2011, doi: 10.2478/v10037-011-0003-8.
[17] Keiichi Miyajima, Artur Korniłowicz, and Yasunari Shidama. Riemann integral of functions from $\mathbb{R}$ into n-dimensional real normed space. *Formalized Mathematics*, 20(**1**):79–86, 2012, doi: 10.2478/v10037-012-0011-3.
[18] Keiichi Miyajima and Yasunari Shidama. Riemann integral of functions from $\mathbb{R}$ into $\mathcal{R}^n$. *Formalized Mathematics*, 17(**2**):179–185, 2009, doi: 10.2478/v10037-009-0021-y.
[19] Keiko Narita, Artur Kornilowicz, and Yasunari Shidama. More on the continuity of real functions. *Formalized Mathematics*, 19(**4**):233–239, 2011, doi: 10.2478/v10037-011-0032-3.
[20] Adam Naumowicz. Conjugate sequences, bounded complex sequences and convergent complex sequences. *Formalized Mathematics*, 6(**2**):265–268, 1997.
[21] Takaya Nishiyama, Artur Korniłowicz, and Yasunari Shidama. The uniform continuity of functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):277–279, 2004.
[22] Takaya Nishiyama, Keiji Ohkubo, and Yasunari Shidama. The continuous functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):269–275, 2004.
[23] Hiroyuki Okazaki, Noboru Endou, Keiko Narita, and Yasunari Shidama. Differentiable functions into real normed spaces. *Formalized Mathematics*, 19(**2**):69–72, 2011, doi: 10.2478/v10037-011-0012-7.
[24] Hiroyuki Okazaki, Noboru Endou, and Yasunari Shidama. More on continuous functions on normed linear spaces. *Formalized Mathematics*, 19(**1**):45–49, 2011, doi: 10.2478/v10037-011-0008-3.
[25] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[26] Konrad Raczkowski and Paweł Sadowski. Real function differentiability. *Formalized Mathematics*, 1(**4**):797–801, 1990.
[27] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.
[28] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.
[29] Laurent Schwartz. *Cours d'analyse II, Ch. 5.* HERMANN, Paris, 1967.

[30] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.
[31] Yasumasa Suzuki. Banach space of bounded real sequences. *Formalized Mathematics*, 12(**2**):77–83, 2004.
[32] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[33] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[34] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[35] Wojciech A. Trybulec. Subspaces and cosets of subspaces in real linear space. *Formalized Mathematics*, 1(**2**):297–301, 1990.
[36] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[37] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[38] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[39] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received August 19, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 4, Pages 303–307, 2012
DOI: 10.2478/v10037-012-0036-7

VERSITA
versita.com/fm/

Products in Categories without Uniqueness of cod and dom[1]

Artur Korniłowicz
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

Summary. The paper introduces Cartesian products in categories without uniqueness of **cod** and **dom**. It is proven that set-theoretical product is the product in the category Ens [7].

MML identifier: ALTCAT_5, version: 8.0.01 5.3.1162

The papers [10], [6], [1], [8], [2], [3], [4], [9], [12], [11], and [5] provide the terminology and notation for this paper.

In this paper I denotes a set and E denotes a non empty set.

Let us mention that every binary relation which is empty is also $\emptyset$-defined.

Let C be a graph. We say that C is functional if and only if:

(Def. 1) For all objects a, b of C holds $\langle a, b \rangle$ is functional.

Let us consider E. One can verify that Ens_E is functional.

Let us observe that there exists a category which is functional and strict.

Let C be a functional category structure. One can verify that the graph of C is functional.

Let us observe that there exists a graph which is functional and strict.

Let us note that there exists a category which is functional and strict.

Let C be a functional graph and let a, b be objects of C. Observe that $\langle a, b \rangle$ is functional.

[1]This work has been supported by the Polish Ministry of Science and Higher Education project "Managing a Large Repository of Computer-verified Mathematical Knowledge" (N N519 385136).

ISSN 1426–2630(p), 1898-9934(e)

Let C be a non empty category structure and let I be a set. An objects family of I and C is a function from I into C.

Let C be a non empty category structure, let o be an object of C, let I be a set, and let f be an objects family of I and C. A many sorted set indexed by I is said to be a morphisms family of o and f if:

(Def. 2) For every set i such that $i \in I$ there exists an object o_1 of C such that $o_1 = f(i)$ and $\mathrm{it}(i)$ is a morphism from o to o_1.

Let C be a non empty category structure, let o be an object of C, let I be a non empty set, and let f be an objects family of I and C. Let us note that the morphisms family of o and f can be characterized by the following (equivalent) condition:

(Def. 3) For every element i of I holds $\mathrm{it}(i)$ is a morphism from o to $f(i)$.

Let C be a non empty category structure, let o be an object of C, let I be a non empty set, let f be an objects family of I and C, let M be a morphisms family of o and f, and let i be an element of I. Then $M(i)$ is a morphism from o to $f(i)$.

Let C be a functional non empty category structure, let o be an object of C, let I be a set, and let f be an objects family of I and C. Observe that every morphisms family of o and f is function yielding.

Next we state the proposition

(1) Let C be a non empty category structure, o be an object of C, and f be an objects family of $\emptyset$ and C. Then $\emptyset$ is a morphisms family of o and f.

Let C be a non empty category structure, let I be a set, let A be an objects family of I and C, let B be an object of C, and let P be a morphisms family of B and A. We say that P is feasible if and only if:

(Def. 4) For every set i such that $i \in I$ there exists an object o of C such that $o = A(i)$ and $P(i) \in \langle B, o \rangle$.

Let C be a non empty category structure, let I be a non empty set, let A be an objects family of I and C, let B be an object of C, and let P be a morphisms family of B and A. Let us observe that P is feasible if and only if:

(Def. 5) For every element i of I holds $P(i) \in \langle B, A(i) \rangle$.

Let C be a category, let I be a set, let A be an objects family of I and C, let B be an object of C, and let P be a morphisms family of B and A. We say that P is projection morphisms family if and only if the condition (Def. 6) is satisfied.

(Def. 6) Let X be an object of C and F be a morphisms family of X and A. Suppose F is feasible. Then there exists a morphism f from X to B such that

(i) $f \in \langle X, B \rangle$,

(ii) for every set i such that $i \in I$ there exists an object s_1 of C and there exists a morphism P_1 from B to s_1 such that $s_1 = A(i)$ and $P_1 = P(i)$ and $F(i) = P_1 \cdot f$, and

(iii) for every morphism f_1 from X to B such that for every set i such that $i \in I$ there exists an object s_1 of C and there exists a morphism P_1 from B to s_1 such that $s_1 = A(i)$ and $P_1 = P(i)$ and $F(i) = P_1 \cdot f_1$ holds $f = f_1$.

Let C be a category, let I be a non empty set, let A be an objects family of I and C, let B be an object of C, and let P be a morphisms family of B and A. Let us observe that P is projection morphisms family if and only if the condition (Def. 7) is satisfied.

(Def. 7) Let X be an object of C and F be a morphisms family of X and A. Suppose F is feasible. Then there exists a morphism f from X to B such that

(i) $f \in \langle X, B \rangle$,

(ii) for every element i of I holds $F(i) = P(i) \cdot f$, and

(iii) for every morphism f_1 from X to B such that for every element i of I holds $F(i) = P(i) \cdot f_1$ holds $f = f_1$.

Let C be a category, let A be an objects family of $\emptyset$ and C, and let B be an object of C. Note that every morphisms family of B and A is feasible.

One can prove the following propositions:

(2) Let C be a category, A be an objects family of $\emptyset$ and C, and B be an object of C. If B is terminal, then there exists a morphisms family of B and A which is empty and projection morphisms family.

(3) For every objects family A of I and Ens_1 and for every object o of Ens_1 holds $I \longmapsto \emptyset$ is a morphisms family of o and A.

(4) Let A be an objects family of I and Ens_1, o be an object of Ens_1, and P be a morphisms family of o and A. If $P = I \longmapsto \emptyset$, then P is feasible and projection morphisms family.

Let C be a category. We say that C has products if and only if the condition (Def. 8) is satisfied.

(Def. 8) Let I be a set and A be an objects family of I and C. Then there exists an object B of C such that there exists a morphisms family of B and A which is feasible and projection morphisms family.

Let us note that Ens_1 has products.

One can check that there exists a category which has products.

Let C be a category, let I be a set, let A be an objects family of I and C, and let B be an object of C. We say that B is A-cat product-like if and only if:

(Def. 9) There exists a morphisms family of B and A which is feasible and projection morphisms family.

Let C be a category with products, let I be a set, and let A be an objects family of I and C. One can check that there exists an object of C which is A-cat product-like.

Let C be a category and let A be an objects family of $\emptyset$ and C. Note that every object of C which is A-cat product-like is also terminal.

We now state two propositions:

(5) Let C be a category, A be an objects family of $\emptyset$ and C, and B be an object of C. If B is terminal, then B is A-cat product-like.

(6) Let C be a category, A be an objects family of I and C, and C_1, C_2 be objects of C. Suppose C_1 is A-cat product-like and C_2 is A-cat product-like. Then C_1, C_2 are iso.

In the sequel A is an objects family of I and Ens_E.

Let us consider I, E, A. Let us assume that $\prod A \in E$. The functor EnsCatProductObj A yielding an object of Ens_E is defined by:

(Def. 10) EnsCatProductObj $A = \prod A$.

Let us consider I, E, A. Let us assume that $\prod A \in E$. The functor EnsCatProduct A yields a morphisms family of EnsCatProductObj A and A and is defined by:

(Def. 11) For every set i such that $i \in I$ holds (EnsCatProduct A)$(i) = \mathrm{proj}(A, i)$.

We now state four propositions:

(7) If $\prod A \in E$ and $\prod A = \emptyset$, then EnsCatProduct $A = I \longmapsto \emptyset$.

(8) If $\prod A \in E$, then EnsCatProduct A is feasible and projection morphisms family.

(9) If $\prod A \in E$, then EnsCatProductObj A is A-cat product-like.

(10) If for all I, A holds $\prod A \in E$, then Ens_E has products.

References

[1] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 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. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[5] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[6] Beata Madras. Basic properties of objects and morphisms. *Formalized Mathematics*, 6(**3**):329–334, 1997.
[7] Zbigniew Semadeni and Antoni Wiweger. *Wstęp do teorii kategorii i funktorów*, volume 45 of *Biblioteka Matematyczna*. PWN, Warszawa, 1978.
[8] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[9] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[10] Andrzej Trybulec. Categories without uniqueness of **cod** and **dom**. *Formalized Mathematics*, 5(**2**):259–267, 1996.
[11] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[12] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received August 19, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 4, Pages 309–341, 2012
DOI: 10.2478/v10037-012-0037-6

VERSITA
versita.com/fm/

Program Algebra over an Algebra[1]

Grzegorz Bancerek
Faculty of Computer Science
Białystok Technical University
Wiejska 45A, 15-351 Białystok, Poland

Summary. We introduce an algebra with free variables, an algebra with undefined values, a program algebra over a term algebra, an algebra with integers, and an algebra with arrays. Program algebra is defined as universal algebra with assignments. Programs depend on the set of generators with supporting variables and supporting terms which determine the value of free variables in the next state. The execution of a program is changing state according to successor function using supporting terms.

MML identifier: AOFA_A00, version: 8.0.01 5.3.1165

The terminology and notation used in this paper have been introduced in the following papers: [40], [9], [24], [16], [25], [1], [3], [7], [28], [13], [32], [10], [12], [17], [38], [23], [31], [18], [19], [20], [5], [14], [8], [37], [41], [36], [30], [35], [11], [34], [26], [4], [21], [33], [29], [42], [39], [2], [6], [27], [15], and [22].

1. Preliminaries

For simplicity, we adopt the following convention: i denotes a natural number, x, y, z denote sets, Σ denotes a non empty non void many sorted signature, and X denotes a non-empty many sorted set indexed by the carrier of Σ.

We now state three propositions:

(1) For all sets A, B and for every A-valued binary relation R holds $R^{\circ}B \subseteq A$.

[1]This work has been supported by the Polish Ministry of Science and Higher Education project "Managing a Large Repository of Computer-verified Mathematical Knowledge" (N N519 385136).

ISSN 1426–2630(p), 1898-9934(e)

(2) For all sets I, J such that $I \subseteq J$ holds $I^i \subseteq J^i$.

(3) Let I, J be non empty sets and f be a homogeneous partial function from I^* to J. Then f is quasi total and non empty if and only if $\mathrm{dom}\, f = I^{\mathrm{arity}\, f}$.

Let I be a set, let f be a many sorted set indexed by I, let i be a set, and let us consider x. Then $f +\cdot (i, x)$ is a many sorted set indexed by I.

Let A, B be sets, let f be a function from A into B, let x be a set, and let y be an element of B. Then $f +\cdot (x, y)$ is a function from A into B.

Let I be a set, let A, B be many sorted sets indexed by I, let F be a many sorted function from A into B, and let us consider x. Then $F(x)$ is a function from $A(x)$ into $B(x)$.

Let I be a set, let f be a non-empty many sorted set indexed by I, let i be a set, and let x be a non empty set. Note that $f +\cdot (i, x)$ is non-empty.

The following propositions are true:

(4) For every set I and for all many sorted sets f, g indexed by I such that $f \subseteq g$ holds $f^{\#} \subseteq g^{\#}$.

(5) Let I be a non empty set, J be a set, and A, B be many sorted sets indexed by I. If $A \subseteq B$, then for every function f from J into I holds $A \cdot f \subseteq B \cdot f$.

(6) For every set I and for all many sorted sets A, B indexed by I such that $A \subseteq B$ holds $\prod A \subseteq \prod B$.

Let f be a function yielding function. Note that $\mathrm{Frege}(f)$ is function yielding.

The following two propositions are true:

(7) For all function yielding functions f, g holds $\mathrm{dom}_\kappa (f \cdot g)(\kappa) = (\mathrm{dom}_\kappa\, f(\kappa)) \cdot g$.

(8) For all functions f, g such that $g = f(x)$ holds $g(y) = f(x)(y)$.

Let I be a set, let i be an element of I, and let us consider x. The functor i-singleton x yields a many sorted set indexed by I and is defined by:

(Def. 1) i-singleton $x = \mathbf{0}.I +\cdot (i, \{x\})$.

One can prove the following propositions:

(9) For every non empty set I and for all elements i, j of I and for every x holds $(i\text{-singleton}\, x)(i) = \{x\}$ and if $i \neq j$, then $(i\text{-singleton}\, x)(j) = \emptyset$.

(10) Let I be a non empty set, i be an element of I, A be a many sorted set indexed by I, and given x. If $x \in A(i)$, then i-singleton x is a many sorted subset of A.

Let I be a set, let A, B be many sorted sets indexed by I, let F be a many sorted function from A into B, and let i be a set. Let us assume that $i \in I$. Let j be a set. Let us assume that $j \in A(i)$. Let v be a set. Let us assume that $v \in B(i)$. The functor $F +\cdot (i, j, v)$ yields a many sorted function from A into B and is defined as follows:

(Def. 2) $(F +\cdot (i, j, v))(i) = F(i) +\cdot (j, v)$ and for every set s such that $s \in I$ and $s \neq i$ holds $(F +\cdot (i, j, v))(s) = F(s)$.

Let a, b, c, d, x, y, z, v be sets. The functor $(a, b, c, d) \mapsto (x, y, z, v)$ yielding a set is defined as follows:

(Def. 3) $(a, b, c, d) \mapsto (x, y, z, v) = (a, b, c) \mapsto (x, y, z) +\cdot (d \dot{\longmapsto} v)$.

Let a, b, c, d, x, y, z, v be sets. Observe that $(a, b, c, d) \mapsto (x, y, z, v)$ is relation-like and function-like.

Next we state a number of propositions:

(11) Let a_1, a_2, a_3, b_1, b_2, b_3 be sets. Then $((a_1, a_2, a_3) \mapsto (b_1, b_2, b_3))(a_3) = b_3$ and if $a_2 \neq a_3$, then $((a_1, a_2, a_3) \mapsto (b_1, b_2, b_3))(a_2) = b_2$ and if $a_1 \neq a_2$ and $a_1 \neq a_3$, then $((a_1, a_2, a_3) \mapsto (b_1, b_2, b_3))(a_1) = b_1$.

(12) For all sets a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 holds $\mathrm{dom}((a_1, a_2, a_3, a_4) \mapsto (b_1, b_2, b_3, b_4)) = \{a_1, a_2, a_3, a_4\}$.

(13) Let a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 be sets. Then

(i) $((a_1, a_2, a_3, a_4) \mapsto (b_1, b_2, b_3, b_4))(a_4) = b_4$,

(ii) if $a_3 \neq a_4$, then $((a_1, a_2, a_3, a_4) \mapsto (b_1, b_2, b_3, b_4))(a_3) = b_3$,

(iii) if $a_2 \neq a_3$ and $a_2 \neq a_4$, then $((a_1, a_2, a_3, a_4) \mapsto (b_1, b_2, b_3, b_4))(a_2) = b_2$, and

(iv) if $a_1 \neq a_2$ and $a_1 \neq a_3$ and $a_1 \neq a_4$, then $((a_1, a_2, a_3, a_4) \mapsto (b_1, b_2, b_3, b_4))(a_1) = b_1$.

(14) For all sets a_1, a_2, a_3, b_1, b_2, b_3 such that $a_2 \neq a_3$ and $a_1 \neq a_2$ and $a_1 \neq a_3$ holds $\mathrm{rng}((a_1, a_2, a_3) \mapsto (b_1, b_2, b_3)) = \{b_1, b_2, b_3\}$.

(15) For all sets a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 such that $a_2 \neq a_3$ and $a_1 \neq a_2$ and $a_1 \neq a_3$ and $a_4 \neq a_1$ and $a_4 \neq a_2$ and $a_4 \neq a_3$ holds $\mathrm{rng}((a_1, a_2, a_3, a_4) \mapsto (b_1, b_2, b_3, b_4)) = \{b_1, b_2, b_3, b_4\}$.

(16) For every set X and for all sets a_1, a_2, a_3 such that a_1, a_2, $a_3 \in X$ holds $\{a_1, a_2, a_3\} \subseteq X$.

(17) For every set X and for all sets a_1, a_2, a_3, a_4 such that a_1, a_2, a_3, $a_4 \in X$ holds $\{a_1, a_2, a_3, a_4\} \subseteq X$.

(18) Let X be a set and a_1, a_2, a_3, a_4, a_5, a_6 be sets. If a_1, a_2, a_3, a_4, a_5, $a_6 \in X$, then $\{a_1, a_2, a_3, a_4, a_5, a_6\} \subseteq X$.

(19) Let X be a set and a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 be sets. Suppose a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, $a_9 \in X$. Then $\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subseteq X$.

(20) Let X be a set and a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10} be sets. Suppose a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, $a_{10} \in X$. Then $\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\} \subseteq X$.

(21) For all sets a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 holds $\{a_1\} \cup \{a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\}$.

(22) For all sets a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10} holds $\{a_1\} \cup \{a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\} = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\}$.

(23) For all sets a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 holds $\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\} \cup \{a_9\} = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\}$.

(24) For all sets a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10} holds $\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \cup \{a_{10}\} = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\}$.

(25) For all sets a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 holds $\{a_1, a_2, a_3\} \cup \{a_4, a_5, a_6, a_7, a_8, a_9\} = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\}$.

(26) For all sets a_1, a_2, a_3, a_4 such that $a_1 \neq a_2$ and $a_1 \neq a_3$ and $a_1 \neq a_4$ and $a_2 \neq a_3$ and $a_2 \neq a_4$ and $a_3 \neq a_4$ holds $\langle a_1, a_2, a_3, a_4 \rangle$ is one-to-one.

Let a_1, a_2, a_3, a_4, a_5, a_6 be sets. The functor $\langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle$ yielding a finite sequence is defined as follows:

(Def. 4) $\langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle = \langle a_1, a_2, a_3, a_4, a_5 \rangle \frown \langle a_6 \rangle$.

Let X be a non empty set and let a_1, a_2, a_3, a_4, a_5, a_6 be elements of X. Then $\langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle$ is a finite sequence of elements of X.

Let a_1, a_2, a_3, a_4, a_5, a_6 be sets. One can check that $\langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle$ is 6-element.

We now state two propositions:

(27) Let a_1, a_2, a_3, a_4, a_5, a_6 be sets and f be a finite sequence. Then $f = \langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle$ if and only if the following conditions are satisfied: $\operatorname{len} f = 6$ and $f(1) = a_1$ and $f(2) = a_2$ and $f(3) = a_3$ and $f(4) = a_4$ and $f(5) = a_5$ and $f(6) = a_6$.

(28) For all sets a_1, a_2, a_3, a_4, a_5, a_6 holds $\operatorname{rng} \langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle = \{a_1, a_2, a_3, a_4, a_5, a_6\}$.

Let a_1, a_2, a_3, a_4, a_5, a_6, a_7 be sets. The functor $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7 \rangle$ yields a finite sequence and is defined by:

(Def. 5) $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7 \rangle = \langle a_1, a_2, a_3, a_4, a_5 \rangle \frown \langle a_6, a_7 \rangle$.

Let X be a non empty set and let a_1, a_2, a_3, a_4, a_5, a_6, a_7 be elements of X. Then $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7 \rangle$ is a finite sequence of elements of X.

Let a_1, a_2, a_3, a_4, a_5, a_6, a_7 be sets. Observe that $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7 \rangle$ is 7-element.

We now state two propositions:

(29) Let a_1, a_2, a_3, a_4, a_5, a_6, a_7 be sets and f be a finite sequence. Then $f = \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7 \rangle$ if and only if the following conditions are satisfied: $\operatorname{len} f = 7$ and $f(1) = a_1$ and $f(2) = a_2$ and $f(3) = a_3$ and $f(4) = a_4$ and $f(5) = a_5$ and $f(6) = a_6$ and $f(7) = a_7$.

(30) For all sets a_1, a_2, a_3, a_4, a_5, a_6, a_7 holds $\operatorname{rng} \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7 \rangle = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$.

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

(Def. 6) $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\rangle = \langle a_1, a_2, a_3, a_4, a_5\rangle \frown \langle a_6, a_7, a_8\rangle$.

Let X be a non empty set and let a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 be elements of X. Then $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\rangle$ is a finite sequence of elements of X.

Let a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 be sets.

Observe that $\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\rangle$ is 8-element.

The following propositions are true:

(31) Let a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 be sets and f be a finite sequence. Then $f = \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\rangle$ if and only if the following conditions are satisfied:
$\operatorname{len} f = 8$ and $f(1) = a_1$ and $f(2) = a_2$ and $f(3) = a_3$ and $f(4) = a_4$ and $f(5) = a_5$ and $f(6) = a_6$ and $f(7) = a_7$ and $f(8) = a_8$.

(32) For all sets a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 holds $\operatorname{rng} \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\rangle = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$.

(33) For all sets a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 holds $\operatorname{rng}(\langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\rangle \frown \langle a_9\rangle) = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\}$.

(34) $\operatorname{Seg} 9 = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

(35) $\operatorname{Seg} 10 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

We now state the proposition

(36) Let a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 be sets. Then $\operatorname{dom} w_9 = \operatorname{Seg} 9$ and $w_9(1) = a_1$ and $w_9(2) = a_2$ and $w_9(3) = a_3$ and $w_9(4) = a_4$ and $w_9(5) = a_5$ and $w_9(6) = a_6$ and $w_9(7) = a_7$ and $w_9(8) = a_8$ and $w_9(9) = a_9$, where $w_9 = \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\rangle \frown \langle a_9\rangle$.

The following proposition is true

(37) Let a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10} be sets. Then $\operatorname{dom} w_{10} = \operatorname{Seg} 10$ and $w_{10}(1) = a_1$ and $w_{10}(2) = a_2$ and $w_{10}(3) = a_3$ and $w_{10}(4) = a_4$ and $w_{10}(5) = a_5$ and $w_{10}(6) = a_6$ and $w_{10}(7) = a_7$ and $w_{10}(8) = a_8$ and $w_{10}(9) = a_9$ and $w_{10}(10) = a_{10}$, where $w_{10} = \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\rangle \frown \langle a_9, a_{10}\rangle$.

Let I, J be sets and let Σ be a many sorted set indexed by I. A many sorted function indexed by I is said to be a double many sorted set of Σ and J if:

(Def. 7) For all sets i, j such that $i \in I$ holds $\operatorname{dom} \operatorname{it}(i) = \Sigma(i)$ and if $j \in \Sigma(i)$, then $\operatorname{it}(i)(j)$ is a many sorted set indexed by J.

Let I, J be sets, let Σ_1 be a many sorted set indexed by I, and let Σ_2 be a many sorted set indexed by J. A double many sorted set of Σ_1 and J is said to be a double many sorted set of Σ_1 and Σ_2 if:

(Def. 8) For all sets i, a such that $i \in I$ and $a \in \Sigma_1(i)$ holds $\operatorname{it}(i)(a)$ is a many sorted subset of Σ_2.

Let I be a set, let X, Y be many sorted sets indexed by I, let f be a double many sorted set of X and Y, and let x, y be sets. Note that $f(x)(y)$ is function-like and relation-like.

Let Σ be a many sorted signature, let o, a be sets, and let r be an element of Σ. We say that o is of type $a \to r$ if and only if:

(Def. 9) (The arity of Σ)$(o) = a$ and (the result sort of Σ)$(o) = r$.

One can prove the following propositions:

(38) Let Σ be a non void non empty many sorted signature, o be an operation symbol of Σ, and r be a sort symbol of Σ. Suppose o is of type $\emptyset \to r$. Let $\mathfrak{A}$ be an algebra over Σ. Suppose (the sorts of $\mathfrak{A}$)$(r) \neq \emptyset$. Then (Den(o($\in$ the carrier' of Σ), $\mathfrak{A}$))$(\emptyset)$ is an element of (the sorts of $\mathfrak{A}$)(r).

(39) Let Σ be a non void non empty many sorted signature, o, a be sets, and r be a sort symbol of Σ. Suppose o is of type $\langle a \rangle \to r$. Let $\mathfrak{A}$ be an algebra over Σ. Suppose (the sorts of $\mathfrak{A}$)$(a) \neq \emptyset$ and (the sorts of $\mathfrak{A}$)$(r) \neq \emptyset$. Let x be an element of (the sorts of $\mathfrak{A}$)(a). Then (Den(o($\in$ the carrier' of Σ), $\mathfrak{A}$))$(\langle x \rangle)$ is an element of (the sorts of $\mathfrak{A}$)(r).

(40) Let Σ be a non void non empty many sorted signature, o, a, b be sets, and r be a sort symbol of Σ. Suppose o is of type $\langle a, b \rangle \to r$. Let $\mathfrak{A}$ be an algebra over Σ. Suppose (the sorts of $\mathfrak{A}$)$(a) \neq \emptyset$ and (the sorts of $\mathfrak{A}$)$(b) \neq \emptyset$ and (the sorts of $\mathfrak{A}$)$(r) \neq \emptyset$. Let x be an element of (the sorts of $\mathfrak{A}$)(a) and y be an element of (the sorts of $\mathfrak{A}$)(b). Then (Den(o($\in$ the carrier' of Σ), $\mathfrak{A}$))$(\langle x, y \rangle)$ is an element of (the sorts of $\mathfrak{A}$)(r).

(41) Let Σ be a non void non empty many sorted signature, o, a, b, c be sets, and r be a sort symbol of Σ. Suppose o is of type $\langle a, b, c \rangle \to r$. Let $\mathfrak{A}$ be an algebra over Σ. Suppose (the sorts of $\mathfrak{A}$)$(a) \neq \emptyset$ and (the sorts of $\mathfrak{A}$)$(b) \neq \emptyset$ and (the sorts of $\mathfrak{A}$)$(c) \neq \emptyset$ and (the sorts of $\mathfrak{A}$)$(r) \neq \emptyset$. Let x be an element of (the sorts of $\mathfrak{A}$)(a), y be an element of (the sorts of $\mathfrak{A}$)(b), and z be an element of (the sorts of $\mathfrak{A}$)(c). Then (Den(o($\in$ the carrier' of Σ), $\mathfrak{A}$))$(\langle x, y, z \rangle)$ is an element of (the sorts of $\mathfrak{A}$)(r).

(42) Let Σ_1, Σ_2 be many sorted signatures. Suppose the many sorted signature of Σ_1 = the many sorted signature of Σ_2. Let o, a be sets, r_1 be an element of Σ_1, and r_2 be an element of Σ_2. If $r_1 = r_2$, then if o is of type $a \to r_1$, then o is of type $a \to r_2$.

(43) Let o be an operation symbol of Σ, r be a sort symbol of Σ, and $\mathfrak{A}$ be an algebra over Σ. If o is of type $\emptyset \to r$, then $\emptyset \in \mathrm{Args}(o, \mathfrak{A})$.

(44) Let o be an operation symbol of Σ, s, r be sort symbols of Σ, and $\mathfrak{A}$ be an algebra over Σ. If o is of type $\langle s \rangle \to r$ and $x \in$ (the sorts of $\mathfrak{A}$)(s), then $\langle x \rangle \in \mathrm{Args}(o, \mathfrak{A})$.

(45) Let o be an operation symbol of Σ, s_1, s_2, r be sort symbols of Σ, and $\mathfrak{A}$ be an algebra over Σ. Suppose o is of type $\langle s_1, s_2 \rangle \to r$ and $x \in$ (the sorts of $\mathfrak{A}$)(s_1) and $y \in$ (the sorts of $\mathfrak{A}$)(s_2). Then $\langle x, y \rangle \in \mathrm{Args}(o, \mathfrak{A})$.

(46) Let o be an operation symbol of Σ, s_1, s_2, s_3, r be sort symbols of Σ, and $\mathfrak{A}$ be an algebra over Σ. Suppose o is of type $\langle s_1, s_2, s_3 \rangle \to r$ and $x \in$ (the

sorts of $\mathfrak{A})(s_1)$ and $y \in$ (the sorts of $\mathfrak{A})(s_2)$ and $z \in$ (the sorts of $\mathfrak{A})(s_3)$. Then $\langle x, y, z \rangle \in \mathrm{Args}(o, \mathfrak{A})$.

2. Free Variables

Let Σ be a non empty non void many sorted signature. We consider free variable algebras over Σ as extensions of algebra over Σ as systems

⟨ sorts, a characteristics, free variables ⟩,

where the sorts constitute a many sorted set indexed by the carrier of Σ, the characteristics is a many sorted function from the sorts$^{\#}$ $\cdot$ the arity of Σ into the sorts $\cdot$the result sort of Σ, and the free variables constitute a double many sorted set of the sorts and the sorts.

Let Σ be a non empty non void many sorted signature, let U be a non-empty many sorted set indexed by the carrier of Σ, let C be a many sorted function from $U^{\#} \cdot$ the arity of Σ into $U \cdot$ the result sort of Σ, and let v be a double many sorted set of U and U. Observe that $\langle U, C, v \rangle_V$ is non-empty.

Let Σ be a non empty non void many sorted signature and let X be a non-empty many sorted set indexed by the carrier of Σ. Observe that there exists a strict free variable algebra over Σ which is non-empty and including Σ-terms over X.

Let Σ be a non empty non void many sorted signature. One can check that there exists a free variable algebra over Σ which is non-empty and disjoint valued. Let X be a non-empty many sorted set indexed by the carrier of Σ. One can check that every including Σ-terms over X free variable algebra over Σ which has all variables is also non-empty.

Let Σ be a non empty non void many sorted signature, let $\mathfrak{A}$ be a non-empty free variable algebra over Σ, let a be a sort symbol of Σ, and let t be an element of $\mathfrak{A}$ from a. The functor $\mathrm{vf}\, t$ yields a many sorted subset of the sorts of $\mathfrak{A}$ and is defined as follows:

(Def. 10) $\mathrm{vf}\, t =$ (the free variables of $\mathfrak{A})(a)(t)$.

Let Σ be a non empty non void many sorted signature and let $\mathfrak{A}$ be a non-empty free variable algebra over Σ. We say that $\mathfrak{A}$ is vf-correct if and only if the condition (Def. 11) is satisfied.

(Def. 11) Let o be an operation symbol of Σ and p be a finite sequence. Suppose $p \in \mathrm{Args}(o, \mathfrak{A})$. Let b be an element of $\mathfrak{A}$ from the result sort of o. Suppose $b = (\mathrm{Den}(o, \mathfrak{A}))(p)$. Let s be a sort symbol of Σ. Then $(\mathrm{vf}\, b)(s) \subseteq \bigcup\{(\mathrm{vf}\, a)(s); s_0$ ranges over sort symbols of Σ, a ranges over elements of $\mathfrak{A}$ from s_0: $\bigvee_{i\,:\,\text{natural number}} (i \in \mathrm{dom}\, \mathrm{Arity}(o) \ \wedge \ s_0 = \mathrm{Arity}(o)(i) \ \wedge \ a = p(i))\}$.

Next we state three propositions:

(47) Let Σ be a non empty non void many sorted signature and $\mathfrak{A}$, $\mathfrak{B}$ be algebras over Σ. Suppose the algebra of $\mathfrak{A}$ = the algebra of $\mathfrak{B}$. Let G be a subset of $\mathfrak{A}$ and H be a subset of $\mathfrak{B}$. If $G = H$, then $\mathrm{Gen}(G) = \mathrm{Gen}(H)$.

(48) Let Σ be a non empty non void many sorted signature and $\mathfrak{A}$, $\mathfrak{B}$ be algebras over Σ. Suppose the algebra of $\mathfrak{A}$ = the algebra of $\mathfrak{B}$. Then every generator set of $\mathfrak{A}$ is a generator set of $\mathfrak{B}$.

(49) Let Σ be a non empty non void many sorted signature and $\mathfrak{A}$, $\mathfrak{B}$ be non-empty algebras over Σ. Suppose the algebra of $\mathfrak{A}$ = the algebra of $\mathfrak{B}$. Let G be a generator set of $\mathfrak{A}$ and H be a generator set of $\mathfrak{B}$. If $G = H$, then if G is free, then H is free.

Let Σ be a non empty non void many sorted signature and let X be a non-empty many sorted set indexed by the carrier of Σ. Observe that there exists a non-empty including Σ-terms over X strict free variable algebra over Σ which is free in itself, has all variables, and inherits operations.

Let Σ be a non empty non void many sorted signature, let X be a non-empty many sorted set indexed by the carrier of Σ, and let $\mathfrak{A}$ be a non-empty including Σ-terms over X free variable algebra over Σ. We say that $\mathfrak{A}$ is vf-free if and only if the condition (Def. 12) is satisfied.

(Def. 12) Let s, r be sort symbols of Σ and t be an element of $\mathfrak{A}$ from s. Then $(\mathrm{vf}\,t)(r) = \{t{\restriction}p; p$ ranges over elements of $\mathrm{dom}\,t : (t{\restriction}p)(\emptyset)_{\mathbf{2}} = r\}$.

The scheme *Scheme* deals with a non empty set $\mathcal{A}$, non-empty many sorted sets $\mathcal{B}$, $\mathcal{C}$ indexed by $\mathcal{A}$, and a ternary functor $\mathcal{F}$ yielding a set, and states that:

There exists a double many sorted set f of $\mathcal{B}$ and $\mathcal{C}$ such that for all elements s, r of $\mathcal{A}$ and for every element t of $\mathcal{B}(s)$ holds $f(s)(t)(r) = \mathcal{F}(s, r, t)$

provided the parameters satisfy the following condition:

- For all elements s, r of $\mathcal{A}$ and for every element t of $\mathcal{B}(s)$ holds $\mathcal{F}(s, r, t)$ is a subset of $\mathcal{C}(r)$.

Next we state the proposition

(50) Let Σ be a non empty non void many sorted signature, X be a non-empty many sorted set indexed by the carrier of Σ, and $\mathfrak{A}$ be a free in itself including Σ-terms over X algebra over Σ with all variables and inheriting operations. Then there exists a double many sorted set V_1 of the sorts of $\mathfrak{A}$ and the sorts of $\mathfrak{A}$ and there exists a free in itself including Σ-terms over X free variable algebra $\mathfrak{B}$ over Σ with all variables and inheriting operations such that $\mathfrak{B} = \langle$the sorts of $\mathfrak{A}$, the characteristics of $\mathfrak{A}$, $V_1\rangle_V$ and $\mathfrak{B}$ is vf-free.

Let Σ be a non empty non void many sorted signature and let X be a non-empty many sorted set indexed by the carrier of Σ. One can verify that there exists a free in itself including Σ-terms over X free variable algebra over Σ with all variables and inheriting operations which is strict and vf-free.

We now state two propositions:

(51) Let Σ be a non empty non void many sorted signature, X be a non-empty many sorted set indexed by the carrier of Σ, $\mathfrak{A}$ be a vf-free including Σ-terms over X free variable algebra over Σ with all variables and inheriting operations, s be a sort symbol of Σ, and t be an element of $\mathfrak{A}$ from s. Then vf t is a many sorted subset of FreeGenerator(X).

(52) Let Σ be a non empty non void many sorted signature, X be a non-empty many sorted set indexed by the carrier of Σ, $\mathfrak{A}$ be a vf-free non-empty including Σ-terms over X free variable algebra over Σ, s be a sort symbol of Σ, and x be an element of $\mathfrak{A}$ from s. If $x \in (\text{FreeGenerator}(X))(s)$, then vf $x = s$-singleton x.

3. Algebra with Undefined Values

Let I be a set and let Σ be a many sorted set indexed by I. A many sorted element of Σ is an element of Σ.

Let I be a non empty set, let A be a non-empty many sorted set indexed by I, let e be a many sorted element of A, and let i be an element of I. Then $e(i)$ is an element of $A(i)$.

Let Σ be a non empty non void many sorted signature. We introduce algebras over Σ with undefined values which are extensions of algebra over Σ and are systems

⟨ sorts, a characteristics, an undefined map ⟩,

where the sorts constitute a many sorted set indexed by the carrier of Σ, the characteristics is a many sorted function from the sorts$^{\#}$ · the arity of Σ into the sorts ·the result sort of Σ, and the undefined map is a many sorted element of the sorts.

Let Σ be a non empty non void many sorted signature. Note that there exists an algebra over Σ with undefined values which is non-empty.

Let Σ be a non empty non void many sorted signature, let $\mathfrak{A}$ be an algebra over Σ with undefined values, let s be a sort symbol of Σ, and let a be an element of $\mathfrak{A}$ from s. We say that a is undefined if and only if:

(Def. 13) $a = (\text{the undefined map of } \mathfrak{A})(s)$.

Let Σ be a non empty non void many sorted signature, let $\mathfrak{A}$ be an algebra over Σ, let s be a sort symbol of Σ, and let a be an element of $\mathfrak{A}$ from s. We say that a is defined if and only if:

(Def. 14) For every algebra $\mathfrak{B}$ over Σ with undefined values such that $\mathfrak{B} = \mathfrak{A}$ holds $a \neq (\text{the undefined map of } \mathfrak{B})(s)$.

Let Σ be a non empty non void many sorted signature and let $\mathfrak{A}$ be an algebra over Σ. The defined sorts of $\mathfrak{A}$ constitute a many sorted subset of the sorts of $\mathfrak{A}$ defined by:

(Def. 15)(i) For every algebra $\mathfrak{B}$ over Σ with undefined values such that $\mathfrak{A} = \mathfrak{B}$ and for every many sorted set U indexed by the carrier of Σ such that for every sort symbol s of Σ holds $U(s) = \{(\text{the undefined map of } \mathfrak{B})(s)\}$ holds the defined sorts of $\mathfrak{A}$ = (the sorts of $\mathfrak{A}$) $\setminus U$ if $\mathfrak{A}$ is an algebra over Σ with undefined values,

(ii) the defined sorts of $\mathfrak{A}$ = the sorts of $\mathfrak{A}$, otherwise.

We now state the proposition

(53) Let Σ_1, Σ_2 be non empty non void many sorted signatures, $\mathfrak{A}_1$ be an algebra over Σ_1 with undefined values, and $\mathfrak{A}_2$ be an algebra over Σ_2 with undefined values. Suppose the sorts of $\mathfrak{A}_1$ = the sorts of $\mathfrak{A}_2$ and the undefined map of $\mathfrak{A}_1$ = the undefined map of $\mathfrak{A}_2$. Then the defined sorts of $\mathfrak{A}_1$ = the defined sorts of $\mathfrak{A}_2$.

Let Σ be a non empty non void many sorted signature and let $\mathfrak{A}$ be an algebra over Σ. We say that $\mathfrak{A}$ has defined elements if and only if:

(Def. 16) The defined sorts of $\mathfrak{A}$ are non-empty.

Let Σ be a non empty non void many sorted signature, let $\mathfrak{A}$ be a non-empty algebra over Σ with undefined values, let s be a sort symbol of Σ, and let a be an element of $\mathfrak{A}$ from s. Let us observe that a is defined if and only if:

(Def. 17) $a \in$ (the defined sorts of $\mathfrak{A}$)(s).

Let Σ be a non empty non void many sorted signature and let $\mathfrak{A}$ be an algebra over Σ with undefined values. We say that $\mathfrak{A}$ is undefined consequently if and only if the condition (Def. 18) is satisfied.

(Def. 18) Let o be an operation symbol of Σ and p be a finite sequence. Suppose that

(i) $p \in \mathrm{Args}(o, \mathfrak{A})$, and

(ii) there exists a natural number i and there exists a sort symbol s of Σ and there exists an element a of $\mathfrak{A}$ from s such that $i \in \mathrm{dom}\,\mathrm{Arity}(o)$ and $s = \mathrm{Arity}(o)(i)$ and $a = p(i)$ and a is undefined.

Let b be an element of $\mathfrak{A}$ from the result sort of o. If $b = (\mathrm{Den}(o, \mathfrak{A}))(p)$, then b is undefined.

Let I be a set and let A be a many sorted set indexed by I. The functor $\mathrm{succ}\,A$ yielding a many sorted set indexed by I is defined as follows:

(Def. 19) For every set i such that $i \in I$ holds $(\mathrm{succ}\,A)(i) = \mathrm{succ}\,A(i)$.

Let I be a set and let A be a many sorted set indexed by I. Note that $\mathrm{succ}\,A$ is non-empty.

Let Σ be a non empty non void many sorted signature, let $\mathfrak{A}$ be an algebra over Σ, and let $\mathfrak{B}$ be an algebra over Σ with undefined values. We say that $\mathfrak{B}$ is $\mathfrak{A}$ with undefined values if and only if the conditions (Def. 20) are satisfied.

(Def. 20)(i) $\mathfrak{B}$ is undefined consequently,

(ii) the undefined map of $\mathfrak{B}$ = the sorts of $\mathfrak{A}$,

(iii) the sorts of $\mathfrak{B}$ = succ (the sorts of $\mathfrak{A}$), and

(iv) for every operation symbol o of Σ and for every element a of Args($o, \mathfrak{A}$) such that Args($o, \mathfrak{A}$) $\neq \emptyset$ holds if (Den($o, \mathfrak{B}$))(a) $\neq$ (Den($o, \mathfrak{A}$))(a), then (Den($o, \mathfrak{B}$))(a) = (the undefined map of $\mathfrak{B}$)(the result sort of o).

We now state the proposition

(54) Let Σ be a non empty non void many sorted signature, $\mathfrak{A}$ be an algebra over Σ, and $\mathfrak{B}$ be an algebra over Σ with undefined values. Suppose $\mathfrak{B}$ is $\mathfrak{A}$ with undefined values. Then the defined sorts of $\mathfrak{B}$ = the sorts of $\mathfrak{A}$.

Let Σ be a non empty many sorted signature and let $\mathfrak{A}$ be an algebra over Σ. Observe that the characteristics of $\mathfrak{A}$ is function yielding.

Let Σ be a non empty non void many sorted signature. Note that every algebra over Σ which has defined elements is also non-empty.

The scheme *UndefAlgebra* deals with a non empty non void many sorted signature $\mathcal{A}$, a non-empty algebra $\mathcal{B}$ over $\mathcal{A}$, and a binary predicate $\mathcal{P}$, and states that:

There exists a strict algebra $\mathfrak{B}$ over $\mathcal{A}$ with undefined values such that

(i) $\mathfrak{B}$ is $\mathcal{B}$ with undefined values and has defined elements,

(ii) the undefined map of $\mathfrak{B}$ = the sorts of $\mathcal{B}$,

(iii) the sorts of $\mathfrak{B}$ = succ (the sorts of $\mathcal{B}$), and

(iv) for every operation symbol o of $\mathcal{A}$ and for every element a of Args($o, \mathcal{B}$) holds if not $\mathcal{P}[o, a]$, then (Den($o, \mathfrak{B}$))(a) = (Den(o, $\mathcal{B}$))(a) and if $\mathcal{P}[o, a]$, then (Den($o, \mathfrak{B}$))(a) = (the undefined map of $\mathfrak{B}$)(the result sort of o)

for all values of the parameters.

One can prove the following proposition

(55) Let $\mathfrak{A}$ be a non-empty algebra over Σ. Then there exists a strict algebra $\mathfrak{B}$ over Σ with undefined values such that

(i) $\mathfrak{B}$ is $\mathfrak{A}$ with undefined values and has defined elements,

(ii) the undefined map of $\mathfrak{B}$ = the sorts of $\mathfrak{A}$,

(iii) the sorts of $\mathfrak{B}$ = succ (the sorts of $\mathfrak{A}$), and

(iv) for every operation symbol o of Σ and for every element a of Args($o, \mathfrak{A}$) holds (Den($o, \mathfrak{B}$))(a) = (Den($o, \mathfrak{A}$))(a).

Let Σ be a non empty non void many sorted signature and let $\mathfrak{A}$ be a non-empty algebra over Σ. Note that every algebra over Σ with undefined values which is $\mathfrak{A}$ with undefined values is also undefined consequently and there exists a strict algebra over Σ with undefined values which is $\mathfrak{A}$ with undefined values and has defined elements.

Let Σ be a non empty non void many sorted signature. One can verify that there exists an algebra over Σ which has defined elements.

Let Σ be a non empty non void many sorted signature and let $\mathfrak{A}$ be an algebra over Σ with defined elements. One can verify that the defined sorts of $\mathfrak{A}$ is non-empty. Let s be a sort symbol of Σ. Note that there exists an element of $\mathfrak{A}$ from s which is defined.

Let us consider Σ, let $\mathfrak{A}$ be an algebra over Σ with undefined values with defined elements, and let s be a sort symbol of Σ. Note that there exists an element of $\mathfrak{A}$ from s which is defined.

4. Program Algebra

Let J be a non empty non void many sorted signature, let $\mathfrak{T}$ be an algebra over J, and let X be a generator set of $\mathfrak{T}$. We introduce program algebra structures of J, $\mathfrak{T}$, and X which are extensions of universal algebra structures and are systems

$\langle$ a carrier, a characteristic, assignments $\rangle$,

where the carrier is a set, the characteristic is a finite sequence of operational functions of the carrier, and the assignments constitute a function from $\bigcup [\![X$, the sorts of $\mathfrak{T}]\!]$ into the carrier.

Let J be a non empty non void many sorted signature, let $\mathfrak{T}$ be an algebra over J, let X be a generator set of $\mathfrak{T}$, and let A be a program algebra structure of J, $\mathfrak{T}$, and X. We say that A is disjoint valued if and only if:

(Def. 21) The sorts of $\mathfrak{T}$ are disjoint valued and the assignments of A are one-to-one.

Let J be a non empty non void many sorted signature, let $\mathfrak{T}$ be an algebra over J, and let X be a generator set of $\mathfrak{T}$. Note that there exists a strict program algebra structure of J, $\mathfrak{T}$, and X which is partial, quasi total, and non-empty.

Let J be a non empty non void many sorted signature, let $\mathfrak{T}$ be an algebra over J, and let X be a generator set of $\mathfrak{T}$. Note that there exists a partial quasi total non-empty non empty strict program algebra structure of J, $\mathfrak{T}$, and X which has empty-instruction, catenation, if-instruction, and while-instruction.

We now state several propositions:

(56) Let U_1, U_2 be pre-if-while algebras. Suppose the universal algebra structure of U_1 = the universal algebra structure of U_2. Then

(i) $\mathrm{EmptyIns}_{(U_1)} = \mathrm{EmptyIns}_{(U_2)}$, and

(ii) for all elements I_1, J_1 of U_1 and for all elements I_2, J_2 of U_2 such that $I_1 = I_2$ and $J_1 = J_2$ holds $I_1; J_1 = I_2; J_2$ and while I_1 do J_1 = while I_2 do J_2 and for every element C_1 of U_1 and for every element C_2 of U_2 such that $C_1 = C_2$ holds if C_1 then I_1 else J_1 = if C_2 then I_2 else J_2.

(57) Let U_1, U_2 be pre-if-while algebras. Suppose the universal algebra structure of U_1 = the universal algebra structure of U_2. Then $\mathrm{ElementaryInstructions}_{(U_1)} = \mathrm{ElementaryInstructions}_{(U_2)}$.

(58) Let U_1, U_2 be universal algebras, Σ_1 be a subset of U_1, and Σ_2 be a subset of U_2. Suppose $\Sigma_1 = \Sigma_2$. Let o_1 be an operation of U_1 and o_2 be an operation of U_2. If $o_1 = o_2$, then if Σ_1 is closed on o_1, then Σ_2 is closed on o_2.

(59) Let U_1, U_2 be universal algebras. Suppose the universal algebra structure of U_1 = the universal algebra structure of U_2. Let Σ_1 be a subset of U_1 and Σ_2 be a subset of U_2. If $\Sigma_1 = \Sigma_2$, then if Σ_1 is operations closed, then Σ_2 is operations closed.

(60) Let U_1, U_2 be universal algebras. Suppose the universal algebra structure of U_1 = the universal algebra structure of U_2. Then every generator set of U_1 is a generator set of U_2.

(61) Let U_1, U_2 be universal algebras. Suppose the universal algebra structure of U_1 = the universal algebra structure of U_2. Then signature U_1 = signature U_2.

Let J be a non empty non void many sorted signature, let $\mathfrak{T}$ be an algebra over J, and let X be a generator set of $\mathfrak{T}$. Note that there exists a partial quasi total non-empty non empty strict program algebra structure of J, $\mathfrak{T}$, and X with empty-instruction, catenation, if-instruction, and while-instruction which is non degenerated, well founded, E.C.I.W.-strict, and infinite.

Let J be a non empty non void many sorted signature, let $\mathfrak{T}$ be an algebra over J, and let X be a generator set of $\mathfrak{T}$. A pre-if-while algebra over X is a partial quasi total non-empty non empty program algebra structure of J, $\mathfrak{T}$, and X with empty-instruction, catenation, if-instruction, and while-instruction.

Let J be a non empty non void many sorted signature, let $\mathfrak{T}$ be an algebra over J, and let X be a generator set of $\mathfrak{T}$. A if-while algebra over X is a non degenerated well founded E.C.I.W.-strict pre-if-while algebra over X.

Let J be a non empty non void many sorted signature, let $\mathfrak{T}$ be a non-empty algebra over J, let X be a non-empty generator set of $\mathfrak{T}$, let A be a non empty program algebra structure of J, $\mathfrak{T}$, and X, let a be a sort symbol of J, let x be an element of $X(a)$, and let t be an element of $\mathfrak{T}$ from a. The functor $x :=_A t$ yielding an algorithm of A is defined as follows:

(Def. 22) $x :=_A t =$ (the assignments of A)($\langle x, t \rangle$).

Let Σ be a set and let $\mathfrak{T}$ be a disjoint valued non-empty many sorted set indexed by Σ. Note that there exists a many sorted subset of $\mathfrak{T}$ which is non-empty.

Let J be a non void non empty many sorted signature, let $\mathfrak{T}$, $\mathfrak{C}$ be non-empty algebras over J, and let X be a non-empty generator set of $\mathfrak{T}$. The functor $\mathfrak{C}$-States(X) yields a subset of MSFuncs(X, the sorts of $\mathfrak{C}$) and is defined by the condition (Def. 23).

(Def. 23) Let s be a many sorted function from X into the sorts of $\mathfrak{C}$. Then $s \in \mathfrak{C}$-States(X) if and only if there exists a many sorted function f from $\mathfrak{T}$

into $\mathfrak{C}$ such that f is a homomorphism of $\mathfrak{T}$ into $\mathfrak{C}$ and $s = f \restriction X$.

Let J be a non void non empty many sorted signature, let $\mathfrak{T}$ be a non-empty algebra over J, let $\mathfrak{C}$ be a non-empty image of $\mathfrak{T}$, and let X be a non-empty generator set of $\mathfrak{T}$. One can verify that $\mathfrak{C}$-States(X) is non empty.

The following proposition is true

(62) Let B be a non void non empty many sorted signature, $\mathfrak{T}$, $\mathfrak{C}$ be non-empty algebras over B, X be a non-empty generator set of $\mathfrak{T}$, and g be a set. Suppose $g \in \mathfrak{C}$-States(X). Then g is a many sorted function from X into the sorts of $\mathfrak{C}$.

Let B be a non void non empty many sorted signature, let $\mathfrak{T}$, $\mathfrak{C}$ be non-empty algebras over B, and let X be a non-empty generator set of $\mathfrak{T}$. Note that every element of $\mathfrak{C}$-States(X) is relation-like and function-like.

Let B be a non void non empty many sorted signature, let $\mathfrak{T}$, $\mathfrak{C}$ be non-empty algebras over B, and let X be a non-empty generator set of $\mathfrak{T}$. One can check that every element of $\mathfrak{C}$-States(X) is function yielding and the carrier of B-defined.

Let B be a non void non empty many sorted signature, let $\mathfrak{T}$ be a non-empty algebra over B, let $\mathfrak{C}$ be a non-empty image of $\mathfrak{T}$, and let X be a non-empty generator set of $\mathfrak{T}$. Observe that every element of $\mathfrak{C}$-States(X) is total.

Let B be a non void non empty many sorted signature, let $\mathfrak{T}$ be a non-empty algebra over B, let $\mathfrak{C}$ be a non-empty algebra over B, let X be a non-empty generator set of $\mathfrak{T}$, let a be a sort symbol of B, let x be an element of $X(a)$, and let f be an element of $\mathfrak{C}$ from a. The functor $\mathrm{States}_{x \not\to f}(X)$ yields a subset of $\mathfrak{C}$-States(X) and is defined by the condition (Def. 24).

(Def. 24) Let s be a many sorted function from X into the sorts of $\mathfrak{C}$. Then $s \in \mathrm{States}_{x \not\to f}(X)$ if and only if $s \in \mathfrak{C}$-States(X) and $s(a)(x) \neq f$.

Let Σ be a non empty non void many sorted signature, let $\mathfrak{A}$ be a non-empty algebra over Σ, and let o be an operation symbol of Σ. Observe that every element of $\mathrm{Args}(o, \mathfrak{A})$ is function-like and relation-like.

Let B be a non void non empty many sorted signature, let X be a non-empty many sorted set indexed by the carrier of B, let $\mathfrak{T}$ be an including B-terms over X non-empty algebra over B, let $\mathfrak{C}$ be a non-empty image of $\mathfrak{T}$, let a be a sort symbol of B, let t be an element of $\mathfrak{T}$ from a, and let s be a function yielding function. Let us assume that there exist a many sorted function h from $\mathfrak{T}$ into $\mathfrak{C}$ and a generator set Q of $\mathfrak{T}$ such that h is a homomorphism of $\mathfrak{T}$ into $\mathfrak{C}$ and $Q = \mathrm{dom}_\kappa\, s(\kappa)$ and $s = h \restriction Q$. The functor $t\,\mathrm{value\ at}(\mathfrak{C}, s)$ yielding an element of $\mathfrak{C}$ from a is defined by the condition (Def. 25).

(Def. 25) There exists a many sorted function f from $\mathfrak{T}$ into $\mathfrak{C}$ and there exists a generator set Q of $\mathfrak{T}$ such that f is a homomorphism of $\mathfrak{T}$ into $\mathfrak{C}$ and $Q = \mathrm{dom}_\kappa\, s(\kappa)$ and $s = f \restriction Q$ and $t\,\mathrm{value\ at}(\mathfrak{C}, s) = f(a)(t)$.

5. GENERATOR SYSTEM

Let us consider Σ, X and let $\mathfrak{T}$ be a non-empty including Σ-terms over X algebra over Σ. We introduce generator systems over Σ, X, and $\mathfrak{T}$ which are systems

⟨ generators, a supported variable, a supported term ⟩,

where the generators constitute a non-empty generator set of $\mathfrak{T}$, the supported variable is a many sorted function from the generators into FreeGenerator(X), and the supported term is a double many sorted set of the generators and the carrier of Σ.

Let us consider Σ, X, let $\mathfrak{T}$ be a non-empty including Σ-terms over X algebra over Σ, let G be a generator system over Σ, X, and $\mathfrak{T}$, and let s be a sort symbol of Σ. An element of $\mathfrak{T}$ from s is said to be an element of G from s if:

(Def. 26) It $\in$ (the generators of G)(s).

Let us consider Σ, X, let $\mathfrak{T}$ be a non-empty including Σ-terms over X algebra over Σ, let G be a generator system over Σ, X, and $\mathfrak{T}$, and let s be a sort symbol of Σ. The functor $G(s)$ yields a component of the generators of G and is defined by:

(Def. 27) $G(s) =$ (the generators of G)(s).

Let g be an element of G from s. The functor supp-var g yielding an element of (FreeGenerator(X))(s) is defined as follows:

(Def. 28) supp-var $g =$ (the supported variable of G)(s)(g).

Let us consider Σ, X, let $\mathfrak{T}$ be a non-empty including Σ-terms over X free variable algebra over Σ, let G be a generator system over Σ, X, and $\mathfrak{T}$, let s be a sort symbol of Σ, and let g be an element of G from s. Let us assume that (the supported term of G)(s)(g) is a many sorted function from vf g into the sorts of $\mathfrak{T}$. The functor supp-term g yielding a many sorted function from vf g into the sorts of $\mathfrak{T}$ is defined as follows:

(Def. 29) supp-term $g =$ (the supported term of G)(s)(g).

Let Σ be a non void non empty many sorted signature, let X be a non-empty many sorted set indexed by the carrier of Σ, let $\mathfrak{T}$ be a non-empty including Σ-terms over X free variable algebra over Σ, let $\mathfrak{C}$ be a non-empty image of $\mathfrak{T}$, and let G be a generator system over Σ, X, and $\mathfrak{T}$. We say that G is $\mathfrak{C}$-supported if and only if the conditions (Def. 30) are satisfied.

(Def. 30)(i) FreeGenerator(X) is a many sorted subset of the generators of G, and

(ii) for every sort symbol s of Σ holds dom (the supported term of G)(s) $= G(s)$ and for every element t of G from s holds (the supported term of G)(s)(t) is a many sorted function from vf t into the sorts of $\mathfrak{T}$ and if $t \in$ (FreeGenerator(X))(s), then supp-term $t = \mathrm{id}_{s\text{-singleton}\,t}$ and supp-var $t = t$ and for every element v of $\mathfrak{C}$-States(the generators of G) such that $v(s)(\text{supp-var}\,t) = v(s)(t)$ and for every sort symbol r of Σ and for every element x of $(\text{FreeGenerator}(X))(r)$ and for every element q of (the sorts of $\mathfrak{T})(r)$ such that $x \in (\text{vf}\, t)(r)$ and $q = (\text{supp-term}\, t)(r)(x)$ and $q\,\text{value at}(\mathfrak{C}, v)$ is defined holds $v(r)(x) = q\,\text{value at}(\mathfrak{C}, v)$ and if $t \notin (\text{FreeGenerator}(X))(s)$, then for every many sorted subset H of the generators of G such that $H = \text{FreeGenerator}(X)$ and for every element v of $\mathfrak{C}$ from s and for every many sorted function f from the generators of G into the sorts of $\mathfrak{C}$ such that $f \in \mathfrak{C}$-States(the generators of G) and for every many sorted function u from FreeGenerator(X) into the sorts of $\mathfrak{C}$ such that for every sort symbol a of Σ and for every element z of $(\text{FreeGenerator}(X))(a)$ such that $z \in (\text{vf}\, t)(a)$ and for every element q of $\mathfrak{T}$ from a such that $q = (\text{supp-term}\, t)(a)(z)$ holds $u(a)(z) = q\,\text{value at}(\mathfrak{C}, (f \restriction H) +\cdot (s, \text{supp-var}\, t, v))$ and for every many sorted subset H of the sorts of $\mathfrak{T}$ such that $H = \text{FreeGenerator}(X)$ and for every many sorted function h from $\mathfrak{T}$ into $\mathfrak{C}$ such that h is a homomorphism of $\mathfrak{T}$ into $\mathfrak{C}$ and $h \restriction H = u$ holds $v = h(s)(t)$.

Let us consider Σ, let us consider X, let $\mathfrak{A}$ be a vf-free free in itself including Σ-terms over X free variable algebra over Σ with all variables and inheriting operations, let $\mathfrak{C}$ be a non-empty image of $\mathfrak{A}$, and let G be a generator system over Σ, X, and $\mathfrak{A}$. Let us assume that G is $\mathfrak{C}$-supported. Let s be an element of $\mathfrak{C}$-States(the generators of G), let r be a sort symbol of Σ, let v be an element of $\mathfrak{C}$ from r, and let t be an element of G from r. The functor $\text{succ}_{t:=v}(s)$ yields an element of $\mathfrak{C}$-States(the generators of G) and is defined by the conditions (Def. 31).

(Def. 31)(i) $(\text{succ}_{t:=v}(s))(r)(t) = v$, and

(ii) for every sort symbol p of Σ and for every element x of $(\text{FreeGenerator}(X))(p)$ such that if $p = r$, then $x \neq t$ holds if $x \notin (\text{vf}\, t)(p)$, then $(\text{succ}_{t:=v}(s))(p)(x) = s(p)(x)$ and for every many sorted function u from FreeGenerator(X) into the sorts of $\mathfrak{C}$ and for every many sorted subset H of the generators of G such that $H = \text{FreeGenerator}(X)$ and for every many sorted function f from the generators of G into the sorts of $\mathfrak{C}$ such that $f = s$ and $u = (f \restriction H) +\cdot (r, \text{supp-var}\, t, v)$ holds if $x \in (\text{vf}\, t)(p)$, then for every element q of $\mathfrak{A}$ from p such that $q = (\text{supp-term}\, t)(p)(x)$ holds $(\text{succ}_{t:=v}(s))(p)(x) = q\,\text{value at}(\mathfrak{C}, u)$.

Let B be a non void non empty many sorted signature, let Y be a non-empty many sorted set indexed by the carrier of B, let $\mathfrak{T}$ be a vf-free free in itself including B-terms over Y free variable algebra over B with all variables and inheriting operations, let $\mathfrak{C}$ be a non-empty image of $\mathfrak{T}$, let X be a generator system over B, Y, and $\mathfrak{T}$, let A be a pre-if-while algebra over the generators of X, let a be a sort symbol of B, let x be an element of (the generators of $X)(a)$, and let z be an element of $\mathfrak{C}$ from a. The functor $\mathfrak{C}\text{-Execution}_{x \not\to z}(A)$ yields a subset of $(\mathfrak{C}\text{-States(the generators of } X))^{(\mathfrak{C}\text{-States(the generators of } X)) \times \text{the carrier of } A}$ and is defined by the condition (Def. 32).

(Def. 32) Let f be a function from ($\mathfrak{C}$-States(the generators of X)) $\times$ the carrier of A into $\mathfrak{C}$-States(the generators of X). Then $f \in \mathfrak{C}$-Execution$_{x \not\to z}(A)$ if and only if f is an execution function of A over $\mathfrak{C}$-States(the generators of X) and States$_{x \not\to z}$(the generators of X).

6. Boolean Signature

We consider connectives signatures as extensions of many sorted signature as systems

⟨ a carrier, a carrier', an arity, a result sort, connectives ⟩,

where the carrier and the carrier' are sets, the arity is a function from the carrier' into the carrier*, the result sort is a function from the carrier' into the carrier, and the connectives constitute a finite sequence of elements of the carrier'.

Let Σ be a connectives signature. We say that Σ is 1-1-connectives if and only if:

(Def. 33) The connectives of Σ are one-to-one.

Let n be a natural number and let Σ be a connectives signature. We say that Σ is n-connectives if and only if:

(Def. 34) len (the connectives of Σ) $= n$.

Let n be a natural number. Note that there exists a strict connectives signature which is n-connectives, non empty, and non void.

We consider boolean signatures as extensions of connectives signature as systems

⟨ a carrier, a carrier', an arity, a result sort, a boolean sort, connectives ⟩,

where the carrier and the carrier' are sets, the arity is a function from the carrier' into the carrier*, the result sort is a function from the carrier' into the carrier, the boolean sort is an element of the carrier, and the connectives constitute a finite sequence of elements of the carrier'.

Let n be a natural number. Note that there exists a strict boolean signature which is n-connectives, non empty, and non void.

Let B be a boolean signature. We say that B is boolean correct if and only if the conditions (Def. 35) are satisfied.

(Def. 35)(i) len (the connectives of B) ≥ 3,

(ii) (the connectives of B)(1) is of type $\emptyset \to$ the boolean sort of B,

(iii) (the connectives of B)(2) is of type ⟨the boolean sort of B⟩ $\to$ the boolean sort of B, and

(iv) (the connectives of B)(3) is of type ⟨the boolean sort of B, the boolean sort of B⟩ $\to$ the boolean sort of B.

One can verify that there exists a strict boolean signature which is 3-connectives, 1-1-connectives, boolean correct, non empty, and non void.

Let us note that there exists a connectives signature which is 1-1-connectives, non empty, and non void.

Let Σ be a 1-1-connectives non empty non void connectives signature. Note that the connectives of Σ is one-to-one.

Let Σ be a non empty non void boolean signature and let $\mathfrak{B}$ be an algebra over Σ. We say that $\mathfrak{B}$ is boolean correct if and only if the conditions (Def. 36) are satisfied.

(Def. 36)(i) (The defined sorts of $\mathfrak{B}$)(the boolean sort of Σ) = *Boolean*,

(ii) (Den((the connectives of Σ)(1)($\in$ the carrier' of Σ), $\mathfrak{B}$))($\emptyset$) = *true*, and

(iii) for all boolean sets x, y holds (Den((the connectives of Σ)(2)($\in$ the carrier' of Σ), $\mathfrak{B}$))($\langle x \rangle$) $= \neg x$ and (Den((the connectives of Σ)(3)($\in$ the carrier' of Σ), $\mathfrak{B}$))($\langle x, y \rangle$) $= x \wedge y$.

One can prove the following proposition

(63) Let A, B be non empty sets, n be a natural number, and f be a function from A^n into B. Then

(i) f is a homogeneous quasi total non empty partial function from A^* to B, and

(ii) for every homogeneous function g such that $f = g$ holds g is n-ary.

Let A, B be non empty sets and let n be a natural number. Note that there exists a homogeneous quasi total non empty partial function from A^* to B which is n-ary.

Now we present two schemes. The scheme *Sch1* deals with non empty sets $\mathcal{A}$, $\mathcal{B}$ and a unary functor $\mathcal{F}$ yielding an element of $\mathcal{B}$, and states that:

> There exists a 1-ary homogeneous quasi total non empty partial function f from $\mathcal{A}^*$ to $\mathcal{B}$ such that for every element a of $\mathcal{A}$ holds $f(\langle a \rangle) = \mathcal{F}(a)$

for all values of the parameters.

The scheme *Sch2* deals with non empty sets $\mathcal{A}$, $\mathcal{B}$ and a binary functor $\mathcal{F}$ yielding an element of $\mathcal{B}$, and states that:

> There exists a 2-ary homogeneous quasi total non empty partial function f from $\mathcal{A}^*$ to $\mathcal{B}$ such that for all elements a, b of $\mathcal{A}$ holds $f(\langle a, b \rangle) = \mathcal{F}(a, b)$

for all values of the parameters.

One can prove the following propositions:

(64) Let Σ be a non empty non void many sorted signature, A be a non-empty many sorted set indexed by the carrier of Σ, f be a many sorted function from $A^\#$ $\cdot$ the arity of Σ into A $\cdot$ the result sort of Σ, o be an operation symbol of Σ, and d be a function from $(A^\# \cdot \text{the arity of } \Sigma)(o)$ into $(A \cdot \text{the}$

result sort of $\Sigma)(o)$. Then $f +\cdot (o, d)$ is a many sorted function from $A^{\#} \cdot$ the arity of Σ into $A \cdot$ the result sort of Σ.

(65) Let Σ be a boolean correct non empty non void boolean signature and A be a non-empty many sorted set indexed by the carrier of Σ. Then there exists a strict algebra $\mathfrak{B}$ over Σ with undefined values with defined elements such that

(i) the defined sorts of $\mathfrak{B} = A +\cdot$ (the boolean sort of Σ, *Boolean*),

(ii) the undefined map of $\mathfrak{B}$ = the defined sorts of $\mathfrak{B}$,

(iii) the sorts of $\mathfrak{B}$ = succ (the defined sorts of $\mathfrak{B}$), and

(iv) $\mathfrak{B}$ is boolean correct and undefined consequently.

Let Σ be a boolean correct non empty non void boolean signature. One can verify that there exists a strict algebra over Σ with undefined values which is boolean correct and undefined consequently and has defined elements and there exists an algebra over Σ which is boolean correct and has defined elements.

Let Σ be a boolean correct non empty non void boolean signature and let $\mathfrak{B}$ be a non-empty algebra over Σ. The functor $\mathrm{true}_{\mathfrak{B}}$ yielding an element of $\mathfrak{B}$ from the boolean sort of Σ is defined as follows:

(Def. 37) $\mathrm{true}_{\mathfrak{B}} = (\mathrm{Den}((\text{the connectives of } \Sigma)(1)(\in \text{the carrier' of } \Sigma), \mathfrak{B}))(\emptyset)$.

Let p be an element of $\mathfrak{B}$ from the boolean sort of Σ. The functor $\neg p$ yields an element of $\mathfrak{B}$ from the boolean sort of Σ and is defined as follows:

(Def. 38) $\neg p = (\mathrm{Den}((\text{the connectives of } \Sigma)(2)(\in \text{the carrier' of } \Sigma), \mathfrak{B}))(\langle p \rangle)$.

Let q be an element of $\mathfrak{B}$ from the boolean sort of Σ. The functor $p \wedge q$ yielding an element of $\mathfrak{B}$ from the boolean sort of Σ is defined as follows:

(Def. 39) $p \wedge q = (\mathrm{Den}((\text{the connectives of } \Sigma)(3)(\in \text{the carrier' of } \Sigma), \mathfrak{B}))(\langle p, q \rangle)$.

Let Σ be a boolean correct non empty non void boolean signature and let $\mathfrak{B}$ be a non-empty algebra over Σ. The functor $\mathrm{false}_{\mathfrak{B}}$ yielding an element of $\mathfrak{B}$ from the boolean sort of Σ is defined as follows:

(Def. 40) $\mathrm{false}_{\mathfrak{B}} = \neg\, \mathrm{true}_{\mathfrak{B}}$.

Let p be an element of $\mathfrak{B}$ from the boolean sort of Σ and let q be an element of $\mathfrak{B}$ from the boolean sort of Σ. The functor $p \vee q$ yields an element of $\mathfrak{B}$ from the boolean sort of Σ and is defined by:

(Def. 41) $p \vee q = \neg(\neg p \wedge \neg q)$.

The functor $p \Rightarrow q$ yielding an element of $\mathfrak{B}$ from the boolean sort of Σ is defined by:

(Def. 42) $p \Rightarrow q = \neg(p \wedge \neg q)$.

Let Σ be a boolean correct non empty non void boolean signature, let $\mathfrak{B}$ be a non-empty algebra over Σ, let p be an element of $\mathfrak{B}$ from the boolean sort of Σ, and let q be an element of $\mathfrak{B}$ from the boolean sort of Σ. The functor $p \Leftrightarrow q$ yielding an element of $\mathfrak{B}$ from the boolean sort of Σ is defined by:

(Def. 43) $p \Leftrightarrow q = (p \wedge q) \vee (\neg p \wedge \neg q)$.

The following proposition is true

(66) Let Σ be a boolean correct non empty non void boolean signature and $\mathfrak{B}$ be a boolean correct algebra over Σ with undefined values with defined elements. Then

(i) $\mathrm{true}_{\mathfrak{B}} = \mathit{true}$,

(ii) $\mathrm{false}_{\mathfrak{B}} = \mathit{false}$, and

(iii) for all defined elements x, y of $\mathfrak{B}$ from the boolean sort of Σ and for all boolean numbers a, b such that $a = x$ and $b = y$ holds $\neg x = \neg a$ and $x \wedge y = a \wedge b$ and $x \vee y = a \vee b$ and $x \Rightarrow y = a \Rightarrow b$ and $x \Leftrightarrow y = a \Leftrightarrow b$.

7. Algebra with Integers

Let i be a natural number, let s be a set, and let Σ be a boolean signature. We say that Σ has integers with connectives from i and the sort at s if and only if the conditions (Def. 44) are satisfied.

(Def. 44)(i) len (the connectives of Σ) $\geq i + 6$, and

(ii) there exists an element I of Σ such that $I = s$ and $I \neq$ the boolean sort of Σ and (the connectives of Σ)(i) is of type $\emptyset \to I$ and (the connectives of Σ)$(i+1)$ is of type $\emptyset \to I$ and (the connectives of Σ)$(i) \neq$ (the connectives of Σ)$(i + 1)$ and (the connectives of Σ)$(i + 2)$ is of type $\langle I \rangle \to I$ and (the connectives of Σ)$(i + 3)$ is of type $\langle I, I \rangle \to I$ and (the connectives of Σ)$(i + 4)$ is of type $\langle I, I \rangle \to I$ and (the connectives of Σ)$(i + 5)$ is of type $\langle I, I \rangle \to I$ and (the connectives of Σ)$(i + 3) \neq$ (the connectives of Σ)$(i+4)$ and (the connectives of Σ)$(i+3) \neq$ (the connectives of Σ)$(i+5)$ and (the connectives of Σ)$(i+4) \neq$ (the connectives of Σ)$(i+5)$ and (the connectives of Σ)$(i+6)$ is of type $\langle I, I \rangle \to$ the boolean sort of Σ.

The following proposition is true

(67) There exists an 10-connectives non empty non void strict boolean signature Σ such that

(i) Σ is 1-1-connectives and boolean correct and has integers with connectives from 4 and the sort at 1,

(ii) the carrier of $\Sigma = \{0, 1\}$, and

(iii) there exists a sort symbol I of Σ such that $I = 1$ and (the connectives of Σ)(4) is of type $\emptyset \to I$.

Let us mention that there exists a strict boolean signature which is 10-connectives, 1-1-connectives, boolean correct, non empty, and non void and has integers with connectives from 4 and the sort at 1.

Let Σ be a non empty non void boolean signature, let N be a set, and let I be a sort symbol of Σ. We say that I is integer sort of N if and only if:

(Def. 45) $I = N$.

Let Σ be a non empty non void boolean signature and let I be a sort symbol of Σ. We say that I is integer if and only if:

(Def. 46) I is integer sort of 1.

Let Σ be a non empty non void boolean signature. Observe that every sort symbol of Σ which is integer is also integer sort of 1 and every sort symbol of Σ which is integer sort of 1 is also integer.

Let Σ be a non empty non void boolean signature with integers with connectives from 4 and the sort at 1. One can verify that there exists a sort symbol of Σ which is integer.

We now state the proposition

(68) Let Σ be a non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and I be an integer sort symbol of Σ. Then $I \neq$ the boolean sort of Σ and (the connectives of Σ)(4) is of type $\emptyset \to I$ and (the connectives of Σ)$(4+1)$ is of type $\emptyset \to I$ and (the connectives of Σ)(4) $\neq$ (the connectives of Σ)$(4+1)$ and (the connectives of Σ)$(4+2)$ is of type $\langle I \rangle \to I$ and (the connectives of Σ)$(4+3)$ is of type $\langle I, I \rangle \to I$ and (the connectives of Σ)$(4+4)$ is of type $\langle I, I \rangle \to I$ and (the connectives of Σ)$(4+5)$ is of type $\langle I, I \rangle \to I$ and (the connectives of Σ)(4+3) $\neq$ (the connectives of Σ)(4+4) and (the connectives of Σ)(4+3) $\neq$ (the connectives of Σ)$(4+5)$ and (the connectives of Σ)$(4+4)$ $\neq$ (the connectives of Σ)$(4+5)$ and (the connectives of Σ)$(4+6)$ is of type $\langle I, I \rangle$ $\to$ the boolean sort of Σ.

Let Σ be a non empty non void boolean signature with integers with connectives from 4 and the sort at 1, let $\mathfrak{A}$ be a non-empty algebra over Σ, and let I be an integer sort symbol of Σ. The functor $0^I_{\mathfrak{A}}$ yields an element of (the sorts of $\mathfrak{A}$)(I) and is defined by:

(Def. 47) $0^I_{\mathfrak{A}} =$ (Den((the connectives of Σ)(4)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\emptyset$).

The functor $1^I_{\mathfrak{A}}$ yields an element of (the sorts of $\mathfrak{A}$)(I) and is defined as follows:

(Def. 48) $1^I_{\mathfrak{A}} =$ (Den((the connectives of Σ)(5)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\emptyset$).

Let a be an element of (the sorts of $\mathfrak{A}$)(I). The functor $-a$ yielding an element of (the sorts of $\mathfrak{A}$)(I) is defined as follows:

(Def. 49) $-a =$ (Den((the connectives of Σ)(6)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a \rangle$).

Let b be an element of (the sorts of $\mathfrak{A}$)(I). The functor $a+b$ yielding an element of (the sorts of $\mathfrak{A}$)(I) is defined as follows:

(Def. 50) $a + b =$ (Den((the connectives of Σ)(7)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a, b \rangle$).

The functor $a \cdot b$ yielding an element of (the sorts of $\mathfrak{A}$)(I) is defined as follows:

(Def. 51) $a \cdot b =$ (Den((the connectives of Σ)(8)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a, b \rangle$).

The functor $a \operatorname{div} b$ yielding an element of (the sorts of $\mathfrak{A}$)(I) is defined by:

(Def. 52) $a \operatorname{div} b =$ (Den((the connectives of Σ)(9)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a, b \rangle$).

The functor leq(a, b) yielding an element of (the sorts of $\mathfrak{A}$)(the boolean sort of Σ) is defined by:

(Def. 53) leq$(a, b) = $ (Den((the connectives of Σ)(10)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a, b\rangle$).

Let Σ be a non empty non void boolean signature with integers with connectives from 4 and the sort at 1, let $\mathfrak{A}$ be a non-empty algebra over Σ, let I be an integer sort symbol of Σ, and let a, b be elements of $\mathfrak{A}$ from I. The functor $a - b$ yields an element of $\mathfrak{A}$ from I and is defined by:

(Def. 54) $a - b = a + -b$.

The functor a mod b yields an element of $\mathfrak{A}$ from I and is defined by:

(Def. 55) $a \bmod b = a + -(a \operatorname{div} b) \cdot b$.

Let Σ be a non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and let X be a non-empty many sorted set indexed by the carrier of Σ. One can verify that $X(1)$ is non empty.

Let n be a natural number, let s be a set, let Σ be a boolean correct non empty non void boolean signature, and let $\mathfrak{A}$ be a boolean correct algebra over Σ. We say that $\mathfrak{A}$ has integers with connectives from n and the sort at s if and only if the condition (Def. 56) is satisfied.

(Def. 56) There exists a sort symbol I of Σ such that

(i) $I = s$,

(ii) (the connectives of Σ)(n) is of type $\emptyset \to I$,

(iii) (the defined sorts of $\mathfrak{A}$)(I) $= \mathbb{Z}$,

(iv) (Den((the connectives of Σ)(n)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\emptyset$) $= 0$,

(v) (Den((the connectives of Σ)($n+1$)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\emptyset$) $= 1$, and

(vi) for all integers i, j holds (Den((the connectives of Σ)($n+2$)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle i\rangle$) $= -i$ and (Den((the connectives of Σ)($n+3$)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle i, j\rangle$) $= i + j$ and (Den((the connectives of Σ)($n+4$)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle i, j\rangle$) $= i \cdot j$ and if $j \neq 0$, then (Den((the connectives of Σ)($n+5$)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle i, j\rangle$) $= i \operatorname{div} j$ and (Den((the connectives of Σ)($n+6$)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle i, j\rangle$) $= (i > j \to$ *false*, *true*).

Let Σ be a non empty non void boolean signature, let I be a set, let n be a natural number, and let $\mathfrak{A}$ be an algebra over Σ with undefined values with defined elements. We say that $\mathfrak{A}$ has division by 0 undefined with n and I if and only if the condition (Def. 57) is satisfied.

(Def. 57) Let J be a sort symbol of Σ. Suppose $I = J$. Let a be a defined element of (the sorts of $\mathfrak{A}$)(J). Then (Den((the connectives of Σ)($n+5$)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a$, (Den((the connectives of Σ)(n)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\emptyset$)$\rangle$) $=$ (the undefined map of $\mathfrak{A}$)(J).

Let Σ be a non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and let $\mathfrak{A}$ be an algebra over Σ with undefined values with defined elements. We say that $\mathfrak{A}$ has division by 0 undefined if and only if:

(Def. 58) $\mathfrak{A}$ has division by 0 undefined with 4 and 1.

Let Σ be a non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and let $\mathfrak{A}$ be an algebra over Σ with undefined values with defined elements. Let us observe that $\mathfrak{A}$ has division by 0 undefined if and only if the condition (Def. 59) is satisfied.

(Def. 59) Let I be an integer sort symbol of Σ and a be a defined element of (the sorts of $\mathfrak{A}$)(I). Then $a \operatorname{div} 0^{I}_{\mathfrak{A}}$ is undefined.

The following proposition is true

(69) Let n be a natural number and I be a set. Suppose $n \geq 1$. Let Σ be a boolean correct non empty non void boolean signature. Suppose Σ has integers with connectives from n and the sort at I. Then there exists a boolean correct strict algebra $\mathfrak{A}$ over Σ with undefined values with defined elements such that

(i) the undefined map of $\mathfrak{A} =$ the defined sorts of $\mathfrak{A}$,

(ii) the sorts of $\mathfrak{A} = \operatorname{succ}$ (the defined sorts of $\mathfrak{A}$), and

(iii) $\mathfrak{A}$ is undefined consequently and has integers with connectives from n and the sort at I and division by 0 undefined with n and I.

Let Σ be a boolean correct non empty non void boolean signature with integers with connectives from 4 and the sort at 1. Note that there exists a boolean correct strict algebra over Σ with undefined values with defined elements which is undefined consequently and has integers with connectives from 4 and the sort at 1 and division by 0 undefined.

One can prove the following proposition

(70) Let Σ be a boolean correct non empty non void boolean signature with integers with connectives from 4 and the sort at 1, $\mathfrak{A}$ be a boolean correct algebra over Σ with undefined values with integers with connectives from 4 and the sort at 1 and defined elements, and I be an integer sort symbol of Σ. Then

(i) (the defined sorts of $\mathfrak{A}$)(I) $= \mathbb{Z}$,

(ii) $0^{I}_{\mathfrak{A}} = 0$,

(iii) $1^{I}_{\mathfrak{A}} = 1$, and

(iv) for all integers i, j and for all elements a, b of (the sorts of $\mathfrak{A}$)(I) such that $a = i$ and $b = j$ holds $-a = -i$ and $a + b = i + j$ and $a - b = i - j$ and $a \cdot b = i \cdot j$ and if $j \neq 0$, then $a \operatorname{div} b = i \operatorname{div} j$ and $a \bmod b = i \bmod j$ and $\operatorname{leq}(a, b) = (i > j \to \mathit{false}, \mathit{true})$ and $\operatorname{leq}(a, b) = \mathit{true}$ iff $i \leq j$ and $\operatorname{leq}(a, b) = \mathit{false}$ iff $i > j$.

8. Algebras with Arrays

Let I, N be sets, let n be a natural number, and let Σ be a connectives signature. We say that Σ has arrays of type I with connectives from n and integers at N if and only if the conditions (Def. 60) are satisfied.

(Def. 60)(i) len (the connectives of Σ) $\geq n+3$, and

(ii) there exist elements J, K, L of Σ such that $L = I$ and $K = N$ and $J \neq L$ and $J \neq K$ and (the connectives of Σ)(n) is of type $\langle J, K \rangle \to L$ and (the connectives of Σ)($n+1$) is of type $\langle J, K, L \rangle \to J$ and (the connectives of Σ)($n+2$) is of type $\langle J \rangle \to K$ and (the connectives of Σ)($n+3$) is of type $\langle K, L \rangle \to J$.

Next we state the proposition

(71) Let Σ_1, Σ_2 be non empty non void connectives signatures. Suppose the connectives signature of Σ_1 = the connectives signature of Σ_2. Let I, N be sets and n be a natural number such that Σ_1 has arrays of type I with connectives from n and integers at N. Then Σ_2 has arrays of type I with connectives from n and integers at N.

Let Σ be a non empty non void connectives signature, let I, N be sets, let n be a natural number, and let $\mathfrak{A}$ be an algebra over Σ with defined elements. We say that $\mathfrak{A}$ has arrays of type I with connectives from n and integers at N if and only if the condition (Def. 61) is satisfied.

(Def. 61) There exist elements J, K of Σ such that

(i) $K = I$,

(ii) (the connectives of Σ)(n) is of type $\langle J, N \rangle \to K$,

(iii) (the defined sorts of $\mathfrak{A}$)(J) = (the defined sorts of $\mathfrak{A}$)$(K)^{\omega}$,

(iv) (the defined sorts of $\mathfrak{A}$)(N) = $\mathbb{Z}$,

(v) for every 0-based finite array a of (the defined sorts of $\mathfrak{A}$)(K) holds for every integer i such that $i \in \operatorname{dom} a$ holds (Den((the connectives of $\Sigma)_n, \mathfrak{A}))(\langle a, i \rangle) = a(i)$ and for every defined element x of $\mathfrak{A}$ from K holds (Den((the connectives of $\Sigma)_{n+1}, \mathfrak{A}))(\langle a, i, x \rangle) = a +\cdot (i, x)$ and (Den((the connectives of $\Sigma)_{n+2}, \mathfrak{A}))(\langle a \rangle) = \overline{\overline{a}}$, and

(vi) for every integer i and for every defined element x of $\mathfrak{A}$ from K such that $i \geq 0$ holds (Den((the connectives of $\Sigma)_{n+3}, \mathfrak{A}))(\langle i, x \rangle) = i \longmapsto x$.

Let B be a non empty boolean signature and let C be a non empty connectives signature. The functor $B {+}{\cdot} C$ yielding a strict boolean signature is defined by the conditions (Def. 62).

(Def. 62)(i) The many sorted signature of $B {+}{\cdot} C = B {+}{\cdot} C$,

(ii) the boolean sort of $B {+}{\cdot} C$ = the boolean sort of B, and

(iii) the connectives of $B {+}{\cdot} C$ = (the connectives of B) $\frown$ (the connectives of C).

Next we state the proposition

(72) Let B be a non empty boolean signature and C be a non empty connectives signature. Then

(i) the carrier of $B+\cdot C =$ (the carrier of B) $\cup$ (the carrier of C),

(ii) the carrier' of $B+\cdot C =$ (the carrier' of B) $\cup$ (the carrier' of C),

(iii) the arity of $B+\cdot C =$ (the arity of B)$+\cdot$(the arity of C), and

(iv) the result sort of $B+\cdot C =$ (the result sort of B)$+\cdot$(the result sort of C).

Let B be a non empty boolean signature and let C be a non empty connectives signature. Note that $B+\cdot C$ is non empty.

Let B be a non void non empty boolean signature and let C be a non empty connectives signature. One can verify that $B+\cdot C$ is non void.

Let n_1, n_2 be natural numbers, let B be an n_1-connectives non empty non void boolean signature, and let C be an n_2-connectives non empty non void connectives signature. One can check that $B+\cdot C$ is $n_1 + n_2$-connectives.

One can prove the following proposition

(73) Let M, O be sets and N, I be sets. Suppose $I, N \in M$. Then there exists an 4-connectives non empty non void strict connectives signature C such that

(i) C is 1-1-connectives and has arrays of type I with connectives from 1 and integers at N,

(ii) $M \subseteq$ the carrier of C,

(iii) O misses the carrier' of C, and

(iv) (the result sort of C)((the connectives of C)(2)) $\notin M$.

Let I, N be sets. Note that there exists a non empty non void strict connectives signature which is 4-connectives and has arrays of type I with connectives from 1 and integers at N.

The following propositions are true:

(74) Let n, m be natural numbers. Suppose $m > 0$. Let B be an n-connectives non empty non void boolean signature, I, N be sets, and C be a non empty non void connectives signature. Suppose C has arrays of type I with connectives from m and integers at N. Then $B+\cdot C$ has arrays of type I with connectives from $n + m$ and integers at N.

(75) Let m be a natural number. Suppose $m > 0$. Let s be a set, B be a non empty non void boolean signature, and C be a non empty non void connectives signature. Suppose that

(i) B has integers with connectives from m and the sort at s, and

(ii) the carrier' of B misses the carrier' of C.

Then $B+\cdot C$ has integers with connectives from m and the sort at s.

(76) Let B be a boolean correct non empty non void boolean signature and C be a non empty non void connectives signature. Suppose the carrier' of B misses the carrier' of C. Then $B+\cdot C$ is boolean correct.

Let n be a natural number and let B be a boolean signature. We say that B is n-array correct if and only if:

(Def. 63) (The result sort of B)((the connectives of B)$(n+1)$) $\neq$ the boolean sort of B.

Let us note that there exists a strict boolean signature which is 1-1-connectives, 14-connectives, 11-array correct, boolean correct, non empty, and non void and has arrays of type 1 with connectives from 11 and integers at 1 and integers with connectives from 4 and the sort at 1.

Let Σ be a non empty non void boolean signature with arrays of type 1 with connectives from 11 and integers at 1. Observe that there exists a sort symbol of Σ which is integer.

Let Σ be a non empty non void boolean signature with arrays of type 1 with connectives from 11 and integers at 1. The array sort of Σ yields a sort symbol of Σ and is defined as follows:

(Def. 64) The array sort of Σ = (the result sort of Σ)((the connectives of Σ)(12)).

Let Σ be a non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and arrays of type 1 with connectives from 11 and integers at 1, let $\mathfrak{A}$ be a non-empty algebra over Σ, let a be an element of (the sorts of $\mathfrak{A}$)(the array sort of Σ), and let I be an integer sort symbol of Σ. The functor $\mathrm{length}_I\, a$ yields an element of (the sorts of $\mathfrak{A}$)(I) and is defined as follows:

(Def. 65) $\mathrm{length}_I\, a$ = (Den((the connectives of Σ)(13)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a \rangle$).

Let i be an element of (the sorts of $\mathfrak{A}$)(I). The functor $a(i)$ yields an element of (the sorts of $\mathfrak{A}$)(I) and is defined by:

(Def. 66) $a(i)$ = (Den((the connectives of Σ)(11)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a, i \rangle$).

Let x be an element of (the sorts of $\mathfrak{A}$)(I). The functor $a_{i \leftarrow x}$ yielding an element of (the sorts of $\mathfrak{A}$)(the array sort of Σ) is defined as follows:

(Def. 67) $a_{i \leftarrow x}$ = (Den((the connectives of Σ)(12)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a, i, x \rangle$).

Let Σ be a boolean correct non empty non void boolean signature, let I, s be sets, let n, m be natural numbers, and let $\mathfrak{A}$ be a non-empty algebra over Σ with undefined values. We say that $\mathfrak{A}$ has index overflow undefined with n, m, I, and s if and only if the condition (Def. 68) is satisfied.

(Def. 68) Let J, K be sort symbols of Σ. Suppose $I = J$ and $s = K$. Let a be a defined element of (the sorts of $\mathfrak{A}$)(K) and i, x be defined elements of (the sorts of $\mathfrak{A}$)(J). Suppose that

(i) (Den((the connectives of Σ)$(n+6)$($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle$(Den((the connectives of Σ)(n)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\emptyset$), $i \rangle$) = $\mathrm{false}_{\mathfrak{A}}$, or

(ii) (Den((the connectives of Σ)$(n+6)$($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle$(Den((the connectives of Σ)$(m+2)$($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a \rangle$), $i\rangle$) = $\mathrm{true}_{\mathfrak{A}}$.
Then

(iii) (Den((the connectives of Σ)(m)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a, i\rangle$) = (the undefined map of $\mathfrak{A}$)(J), and

(iv) (Den((the connectives of Σ)$(m+1)$($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a, i, x\rangle$) = (the undefined map of $\mathfrak{A}$)(K).

Let Σ be a boolean correct non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and arrays of type 1 with connectives from 11 and integers at 1 and let $\mathfrak{A}$ be a non-empty algebra over Σ with undefined values. We say that $\mathfrak{A}$ has index overflow undefined if and only if:

(Def. 69) $\mathfrak{A}$ has index overflow undefined with 4, 11, 1, and the array sort of Σ.

Let Σ be a boolean correct non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and arrays of type 1 with connectives from 11 and integers at 1 and let $\mathfrak{A}$ be a non-empty algebra over Σ with undefined values. Let us observe that $\mathfrak{A}$ has index overflow undefined if and only if the condition (Def. 70) is satisfied.

(Def. 70) Let I be an integer sort symbol of Σ, a be a defined element of (the sorts of $\mathfrak{A}$)(the array sort of Σ), and i, x be defined elements of (the sorts of $\mathfrak{A}$)(I). If $\mathrm{leq}(0^I_{\mathfrak{A}}, i) = \mathrm{false}_{\mathfrak{A}}$ or $\mathrm{leq}(\mathrm{length}_I\, a, i) = \mathrm{true}_{\mathfrak{A}}$, then $a(i)$ is undefined and $a_{i \leftarrow x}$ is undefined.

Let Σ be a non empty non void boolean signature with integers with connectives from 4 and the sort at 1 and arrays of type 1 with connectives from 11 and integers at 1, let $\mathfrak{A}$ be a non-empty algebra over Σ, let I be an integer sort symbol of Σ, let i be an element of (the sorts of $\mathfrak{A}$)(I), and let x be an element of (the sorts of $\mathfrak{A}$)(I). The functor init.array(i, x) yielding an element of (the sorts of $\mathfrak{A}$)(the array sort of Σ) is defined as follows:

(Def. 71) init.array(i, x) = (Den((the connectives of Σ)(14)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle i, x\rangle$).

Let X be a non empty set. One can check that $\langle X\rangle$ is non-empty. Let Y, Z be non empty sets. One can verify that $\langle X, Y, Z\rangle$ is non-empty.

Let X be a functional non empty set, let Y, Z be non empty sets, and let f be an element of $\prod\langle X, Y, Z\rangle$. Observe that $f(1)$ is relation-like and function-like.

Let X be an integer-membered non empty set, let Y be a non empty set, and let f be an element of $\prod\langle X, Y\rangle$. Observe that $f(1)$ is integer.

The following proposition is true

(77) Let I, N be sets, Σ be a non empty non void connectives signature with arrays of type I with connectives from 1 and integers at N, Y be a non empty set, and X be a non-empty many sorted set indexed by Y. Suppose that

(i) (the result sort of Σ)((the connectives of Σ)(2)) $\notin Y$ or X((the result sort of Σ)((the connectives of Σ)(2))) $= X(I)^{\omega}$,

(ii) $X(N) = \mathbb{Z}$, and

(iii) $I \in Y$.

Then there exists a strict algebra $\mathfrak{A}$ over Σ with undefined values with defined elements such that

(iv) $\mathfrak{A}$ has arrays of type I with connectives from 1 and integers at N,

(v) the defined sorts of $\mathfrak{A} \approx X$, and

(vi) for every 0-based finite array a of (the defined sorts of $\mathfrak{A}$)(I) and for every integer i such that $i \notin \operatorname{dom} a$ holds (Den((the connectives of Σ)(1)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a, i\rangle$) = (the undefined map of $\mathfrak{A}$)(I) and for every element x of (the defined sorts of $\mathfrak{A}$)(I) holds (Den((the connectives of Σ)(2)($\in$ the carrier' of Σ), $\mathfrak{A}$))($\langle a, i, x\rangle$) = (the undefined map of $\mathfrak{A}$)(the result sort of (the connectives of Σ)(2)($\in$ the carrier' of Σ)).

Let I, N be sets and let Σ be a non empty non void connectives signature with arrays of type I with connectives from 1 and integers at N. One can verify that there exists a strict algebra over Σ with undefined values with defined elements which has arrays of type I with connectives from 1 and integers at N.

Let Σ_1 be a non empty non void boolean signature, let Σ_2 be a non empty non void connectives signature, let $\mathfrak{A}_1$ be an algebra over Σ_1 with undefined values with defined elements, and let $\mathfrak{A}_2$ be an algebra over Σ_2 with undefined values with defined elements. Let us assume that the sorts of $\mathfrak{A}_1 \approx$ the sorts of $\mathfrak{A}_2$ and the undefined map of $\mathfrak{A}_1 \approx$ the undefined map of $\mathfrak{A}_2$. The functor $\mathfrak{A}_{1\Sigma_1}{+\cdot}_{\Sigma_2}\mathfrak{A}_2$ yields a strict algebra over $\Sigma_1{+\cdot}\Sigma_2$ with undefined values with defined elements and is defined by the conditions (Def. 72).

(Def. 72)(i) The sorts of $\mathfrak{A}_{1\Sigma_1}{+\cdot}_{\Sigma_2}\mathfrak{A}_2$ = (the sorts of $\mathfrak{A}_1$)$+\cdot$(the sorts of $\mathfrak{A}_2$),

(ii) the characteristics of $\mathfrak{A}_{1\Sigma_1}{+\cdot}_{\Sigma_2}\mathfrak{A}_2$ = (the characteristics of $\mathfrak{A}_1$)$+\cdot$(the characteristics of $\mathfrak{A}_2$), and

(iii) the undefined map of $\mathfrak{A}_{1\Sigma_1}{+\cdot}_{\Sigma_2}\mathfrak{A}_2$ = (the undefined map of $\mathfrak{A}_1$)$+\cdot$(the undefined map of $\mathfrak{A}_2$).

The following propositions are true:

(78) Let B, C be non empty non void connectives signatures, $\mathfrak{A}_1$ be an algebra over B with undefined values with defined elements, and $\mathfrak{A}_2$ be an algebra over C with undefined values with defined elements. Suppose the sorts of $\mathfrak{A}_1 \approx$ the sorts of $\mathfrak{A}_2$ and the undefined map of $\mathfrak{A}_1 \approx$ the undefined map of $\mathfrak{A}_2$. Then the defined sorts of $\mathfrak{A}_1 \approx$ the defined sorts of $\mathfrak{A}_2$.

(79) Let B be a non empty non void boolean signature, $\mathfrak{A}_1$ be an algebra over B with undefined values with defined elements, C be a non empty non void connectives signature, and $\mathfrak{A}_2$ be an algebra over C with undefined values with defined elements. Suppose the sorts of $\mathfrak{A}_1 \approx$ the sorts of $\mathfrak{A}_2$ and the undefined map of $\mathfrak{A}_1 \approx$ the undefined map of $\mathfrak{A}_2$. Then the defined sorts

of $\mathfrak{A}_1{}_B{+}{\cdot}_C\mathfrak{A}_2$ = (the defined sorts of $\mathfrak{A}_1$)+·(the defined sorts of $\mathfrak{A}_2$).

(80) Let B be a boolean correct non empty non void boolean signature, $\mathfrak{A}_1$ be a boolean correct algebra over B with undefined values with defined elements, and C be a non empty non void connectives signature. Suppose the carrier' of B misses the carrier' of C. Let $\mathfrak{A}_2$ be an algebra over C with undefined values with defined elements. Suppose the sorts of $\mathfrak{A}_1 \approx$ the sorts of $\mathfrak{A}_2$ and the undefined map of $\mathfrak{A}_1 \approx$ the undefined map of $\mathfrak{A}_2$. Then $\mathfrak{A}_1{}_B{+}{\cdot}_C\mathfrak{A}_2$ is boolean correct.

(81) Let n be a natural number and I be a set. Suppose $n \geq 4$. Let B be a boolean correct non empty non void boolean signature. Suppose B has integers with connectives from n and the sort at I. Let $\mathfrak{A}_1$ be a boolean correct algebra over B with undefined values with defined elements. Suppose $\mathfrak{A}_1$ has integers with connectives from n and the sort at I. Let C be a non empty non void connectives signature. Suppose the carrier' of B misses the carrier' of C. Let $\mathfrak{A}_2$ be an algebra over C with undefined values with defined elements. Suppose the sorts of $\mathfrak{A}_1 \approx$ the sorts of $\mathfrak{A}_2$ and the undefined map of $\mathfrak{A}_1 \approx$ the undefined map of $\mathfrak{A}_2$. Let Σ be a boolean correct non empty non void boolean signature. Suppose the boolean signature of $\Sigma = B{+}{\cdot}C$. Let $\mathfrak{A}$ be a boolean correct algebra over Σ with undefined values with defined elements. Suppose the algebra of $\mathfrak{A}$ with undefined values $= \mathfrak{A}_1{}_B{+}{\cdot}_C\mathfrak{A}_2$. Then

(i) $\mathfrak{A}$ has integers with connectives from n and the sort at I, and

(ii) if $\mathfrak{A}_1$ has division by 0 undefined with n and I, then $\mathfrak{A}$ has division by 0 undefined with n and I.

(82) Let n, m be natural numbers and s, r be sets. Suppose $n \geq 1$ and $m \geq 1$. Let B be an m-connectives non empty non void boolean signature, $\mathfrak{A}_1$ be an algebra over B with undefined values with defined elements, and C be a non empty non void connectives signature. Suppose that

(i) the carrier' of B misses the carrier' of C, and

(ii) C has arrays of type s with connectives from n and integers at r.

Let $\mathfrak{A}_2$ be an algebra over C with undefined values with defined elements. Suppose that

(iii) the sorts of $\mathfrak{A}_1 \approx$ the sorts of $\mathfrak{A}_2$,

(iv) the undefined map of $\mathfrak{A}_1 \approx$ the undefined map of $\mathfrak{A}_2$, and

(v) $\mathfrak{A}_2$ has arrays of type s with connectives from n and integers at r.

Let Σ be a non empty non void boolean signature. Suppose the boolean signature of $\Sigma = B{+}{\cdot}C$. Let $\mathfrak{A}$ be an algebra over Σ with undefined values with defined elements. Suppose the algebra of $\mathfrak{A}$ with undefined values $= \mathfrak{A}_1{}_B{+}{\cdot}_C\mathfrak{A}_2$. Then

(vi) $\mathfrak{A}$ has arrays of type s with connectives from $m + n$ and integers at r, and

(vii) if the characteristics of $\mathfrak{A}_1 \approx$ the characteristics of $\mathfrak{A}_2$ and $B \approx C$ and $\mathfrak{A}_1$ is undefined consequently and $\mathfrak{A}_2$ is undefined consequently, then $\mathfrak{A}$ is undefined consequently.

(83) Let n, n_1, m be natural numbers and r be a set. Suppose $n \geq 1$ and $n_1 \geq 4$. Let B be a boolean correct non empty non void boolean signature. Suppose B is m-connectives. Let $\mathfrak{A}_1$ be a boolean correct algebra over B with undefined values with defined elements. Suppose that

(i) B has integers with connectives from n_1 and the sort at r, and

(ii) $\mathfrak{A}_1$ has integers with connectives from n_1 and the sort at r.

Let C be a non empty non void connectives signature. Suppose that

(iii) the carrier' of B misses the carrier' of C, and

(iv) C has arrays of type r with connectives from n and integers at r.

Let $\mathfrak{A}_2$ be an algebra over C with undefined values with defined elements. Suppose that

(v) the sorts of $\mathfrak{A}_1 \approx$ the sorts of $\mathfrak{A}_2$,

(vi) the undefined map of $\mathfrak{A}_1 \approx$ the undefined map of $\mathfrak{A}_2$, and

(vii) $\mathfrak{A}_2$ has arrays of type r with connectives from n and integers at r.

Let Σ be a boolean correct non empty non void boolean signature. Suppose the boolean signature of $\Sigma = B {+\cdot} C$. Let A be a boolean correct algebra over Σ with undefined values with defined elements such that the algebra of $\mathfrak{A}$ with undefined values $= \mathfrak{A}_1{}_B{+\cdot}_C\mathfrak{A}_2$ and for every 0-based finite array a of $\mathbb{Z}$ and for every integer i such that $i \notin \operatorname{dom} a$ holds (Den((the connectives of C)(n)($\in$ the carrier' of C), $\mathfrak{A}_2$))($\langle a, i\rangle$) = (the undefined map of $\mathfrak{A}_2$)(r) and for every integer x holds (Den((the connectives of C)($n+1$)($\in$ the carrier' of C), $\mathfrak{A}_2$))($\langle a, i, x\rangle$) = (the undefined map of $\mathfrak{A}_2$)(the result sort of (the connectives of C)($n{+}1$)($\in$ the carrier' of C)). Then $\mathfrak{A}$ has index overflow undefined with n_1, $n + m$, r, and the result sort of the connectives of $\Sigma(n + m + 1)$($\in$ the carrier' of Σ).

(84) Let n be a natural number, s be a set, and Σ_1, Σ_2 be boolean signatures. Suppose that

(i) the boolean sort of $\Sigma_1 =$ the boolean sort of Σ_2,

(ii) len (the connectives of Σ_2) ≥ 3, and

(iii) for every i such that $i \geq 1$ and $i \leq 3$ holds (the arity of Σ_1)((the connectives of Σ_1)(i)) = (the arity of Σ_2)((the connectives of Σ_2)(i)) and (the result sort of Σ_1)((the connectives of Σ_1)(i)) = (the result sort of Σ_2)((the connectives of Σ_2)(i)).

If Σ_1 is boolean correct, then Σ_2 is boolean correct.

(85) Let n be a natural number, s be a set, and Σ_1, Σ_2 be non empty boolean signatures. Suppose that $n \geq 1$ and the boolean sort of $\Sigma_1 =$ the boolean sort of Σ_2 and len (the connectives of Σ_2) $\geq n + 6$ and (the connectives of Σ_2)(n) $\neq$ (the connectives of Σ_2)($n + 1$) and (the connecti-

ves of Σ_2)$(n+3) \neq$ (the connectives of Σ_2)$(n+4)$ and (the connectives of Σ_2)$(n+3) \neq$ (the connectives of Σ_2)$(n+5)$ and (the connectives of Σ_2)$(n+4) \neq$ (the connectives of Σ_2)$(n+5)$ and for every i such that $i \geq n$ and $i \leq n+6$ holds (the arity of Σ_1)((the connectives of Σ_1)(i)) = (the arity of Σ_2)((the connectives of Σ_2)(i)) and (the result sort of Σ_1)((the connectives of Σ_1)(i)) = (the result sort of Σ_2)((the connectives of Σ_2)(i)). Suppose Σ_1 has integers with connectives from n and the sort at s. Then Σ_2 has integers with connectives from n and the sort at s.

(86) Let n, m be natural numbers, s, r be sets, and Σ_1, Σ_2 be non empty connectives signatures. Suppose that

(i) $1 \leq n$,

(ii) len (the connectives of Σ_1) $\geq n+3$, and

(iii) for every i such that $i \geq n$ and $i \leq n+3$ holds (the arity of Σ_1)((the connectives of Σ_1)(i)) = (the arity of Σ_2)((the connectives of Σ_2)$(i+m)$) and (the result sort of Σ_1)((the connectives of Σ_1)(i)) = (the result sort of Σ_2)((the connectives of Σ_2)$(i+m)$).

Suppose Σ_2 has arrays of type s with connectives from $n+m$ and integers at r. Then Σ_1 has arrays of type s with connectives from n and integers at r.

(87) Let j, k be sets and i, m, n be natural numbers. Suppose $m \geq 4$ and $m+6 \leq n$ and $i \geq 1$. Let Σ be a 1-1-connectives boolean correct non empty non void boolean signature. Suppose that

then there exists a boolean correct non empty non void boolean signature B and there exists a non empty non void connectives signature C such that

the boolean signature of $\Sigma = B {+\cdot} C$ and B is n-connectives and has integers with connectives from m and the sort at k and C has arrays of type j with connectives from i and integers at k and the carrier of B = the carrier of C and the carrier' of B = (the carrier' of Σ) $\setminus$ rng (the connectives of C) and the carrier' of C = rng (the connectives of C) and the connectives of B = (the connectives of Σ)$\restriction n$ and the connectives of C = (the connectives of Σ)$_{\lfloor n}$.

(88) Let s, I be sets and Σ be a boolean correct non empty non void boolean signature. Suppose Σ has integers with connectives from 4 and the sort at I. Let X be a non empty set. Suppose $s \in$ the carrier of Σ and $s \neq I$ and $s \neq$ the boolean sort of Σ. Then there exists a boolean correct strict algebra $\mathfrak{A}$ over Σ with undefined values with defined elements such that

(i) the undefined map of $\mathfrak{A}$ = the defined sorts of $\mathfrak{A}$,

(ii) the sorts of $\mathfrak{A}$ = succ (the defined sorts of $\mathfrak{A}$),

(iii) $\mathfrak{A}$ is undefined consequently and has integers with connectives from 4 and the sort at I,

(iv) (the defined sorts of $\mathfrak{A})(s) = X$, and

(v) $\mathfrak{A}$ has division by 0 undefined with 4 and I.

Let Σ be a 1-1-connectives 11-array correct boolean correct non empty non void boolean signature with arrays of type 1 with connectives from 11 and integers at 1 and integers with connectives from 4 and the sort at 1. One can check that there exists a boolean correct strict algebra over Σ with undefined values with defined elements which is undefined consequently and has arrays of type 1 with connectives from 11 and integers at 1, integers with connectives from 4 and the sort at 1, division by 0 undefined, and index overflow undefined.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. Introduction to trees. *Formalized Mathematics*, 1(**2**):421–427, 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. Cartesian product of functions. *Formalized Mathematics*, 2(**4**):547–552, 1991.
[6] Grzegorz Bancerek. König's lemma. *Formalized Mathematics*, 2(**3**):397–402, 1991.
[7] Grzegorz Bancerek. Algebra of morphisms. *Formalized Mathematics*, 6(**2**):303–310, 1997.
[8] Grzegorz Bancerek. Institution of many sorted algebras. Part I: Signature reduct of an algebra. *Formalized Mathematics*, 6(**2**):279–287, 1997.
[9] Grzegorz Bancerek. Mizar analysis of algorithms: Preliminaries. *Formalized Mathematics*, 15(**3**):87–110, 2007, doi:10.2478/v10037-007-0011-x.
[10] Grzegorz Bancerek. Sorting by exchanging. *Formalized Mathematics*, 19(**2**):93–102, 2011, doi: 10.2478/v10037-011-0015-4.
[11] Grzegorz Bancerek. Free term algebras. *Formalized Mathematics*, 20(**3**):239–256, 2012, doi: 10.2478/v10037-012-0029-6.
[12] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[13] Grzegorz Bancerek and Piotr Rudnicki. The set of primitive recursive functions. *Formalized Mathematics*, 9(**4**):705–720, 2001.
[14] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.
[15] Ewa Burakowska. Subalgebras of the universal algebra. Lattices of subalgebras. *Formalized Mathematics*, 4(**1**):23–27, 1993.
[16] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[17] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[18] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[19] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[20] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.
[21] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[22] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[23] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[24] Artur Korniłowicz. On the group of automorphisms of universal algebra & many sorted algebra. *Formalized Mathematics*, 5(**2**):221–226, 1996.
[25] Artur Korniłowicz and Marco Riccardi. The Borsuk-Ulam theorem. *Formalized Mathematics*, 20(**2**):105–112, 2012, doi: 10.2478/v10037-012-0014-0.
[26] Małgorzata Korolkiewicz. Homomorphisms of many sorted algebras. *Formalized Mathematics*, 5(**1**):61–65, 1996.

[27] Jarosław Kotowicz, Beata Madras, and Małgorzata Korolkiewicz. Basic notation of universal algebra. *Formalized Mathematics*, 3(**2**):251–253, 1992.
[28] Yatsuka Nakamura and Grzegorz Bancerek. Combining of circuits. *Formalized Mathematics*, 5(**2**):283–295, 1996.
[29] Andrzej Nędzusiak. Probability. *Formalized Mathematics*, 1(**4**):745–749, 1990.
[30] Beata Perkowska. Free many sorted universal algebra. *Formalized Mathematics*, 5(**1**):67–74, 1996.
[31] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[32] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[33] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[34] Andrzej Trybulec. Many sorted algebras. *Formalized Mathematics*, 5(**1**):37–42, 1996.
[35] Andrzej Trybulec. A scheme for extensions of homomorphisms of many sorted algebras. *Formalized Mathematics*, 5(**2**):205–209, 1996.
[36] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[37] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[38] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[39] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[40] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.
[41] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.
[42] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received August 27, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 4, Pages 343–347, 2012
DOI: 10.2478/v10037-012-0038-5

VERSITA
versita.com/fm/

Isomorphisms of Direct Products of Finite Cyclic Groups

Kenichi Arai
Tokyo University of Science
Chiba, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize that every finite cyclic group is isomorphic to a direct product of finite cyclic groups which orders are relative prime. This theorem is closely related to the Chinese Remainder theorem ([18]) and is a useful lemma to prove the basis theorem for finite abelian groups and the fundamental theorem of finite abelian groups. Moreover, we formalize some facts about the product of a finite sequence of abelian groups.

MML identifier: GROUP_14, version: 8.0.01 5.4.1165

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

Let G be an Abelian add-associative right zeroed right complementable non empty additive loop structure. Note that $\langle G \rangle$ is non empty and Abelian group yielding as a finite sequence.

Let G, F be Abelian add-associative right zeroed right complementable non empty additive loop structures. Note that $\langle G, F \rangle$ is non empty and Abelian group yielding as a finite sequence.

We now state the proposition

(1) Let X be an Abelian group. Then there exists a homomorphism I from X to $\prod\langle X \rangle$ such that I is bijective and for every element x of X holds $I(x) = \langle x \rangle$.

ISSN 1426–2630(p), 1898-9934(e)

Let G, F be non empty Abelian group yielding finite sequences. Note that $G \frown F$ is Abelian group yielding.

One can prove the following propositions:

(2) Let X, Y be Abelian groups. Then there exists a homomorphism I from $X \times Y$ to $\prod\langle X, Y\rangle$ such that I is bijective and for every element x of X and for every element y of Y holds $I(x, y) = \langle x, y\rangle$.

(3) Let X, Y be sequences of groups. Then there exists a homomorphism I from $\prod X \times \prod Y$ to $\prod(X \frown Y)$ such that

(i) I is bijective, and

(ii) for every element x of $\prod X$ and for every element y of $\prod Y$ there exist finite sequences x_1, y_1 such that $x = x_1$ and $y = y_1$ and $I(x, y) = x_1 \frown y_1$.

(4) Let G, F be Abelian groups. Then

(i) for every set x holds x is an element of $\prod\langle G, F\rangle$ iff there exists an element x_1 of G and there exists an element x_2 of F such that $x = \langle x_1, x_2\rangle$,

(ii) for all elements x, y of $\prod\langle G, F\rangle$ and for all elements x_1, y_1 of G and for all elements x_2, y_2 of F such that $x = \langle x_1, x_2\rangle$ and $y = \langle y_1, y_2\rangle$ holds $x + y = \langle x_1 + y_1, x_2 + y_2\rangle$,

(iii) $0_{\prod\langle G,F\rangle} = \langle 0_G, 0_F\rangle$, and

(iv) for every element x of $\prod\langle G, F\rangle$ and for every element x_1 of G and for every element x_2 of F such that $x = \langle x_1, x_2\rangle$ holds $-x = \langle -x_1, -x_2\rangle$.

(5) Let G, F be Abelian groups. Then

(i) for every set x holds x is an element of $G \times F$ iff there exists an element x_1 of G and there exists an element x_2 of F such that $x = \langle x_1, x_2\rangle$,

(ii) for all elements x, y of $G \times F$ and for all elements x_1, y_1 of G and for all elements x_2, y_2 of F such that $x = \langle x_1, x_2\rangle$ and $y = \langle y_1, y_2\rangle$ holds $x + y = \langle x_1 + y_1, x_2 + y_2\rangle$,

(iii) $0_{G \times F} = \langle 0_G, 0_F\rangle$, and

(iv) for every element x of $G \times F$ and for every element x_1 of G and for every element x_2 of F such that $x = \langle x_1, x_2\rangle$ holds $-x = \langle -x_1, -x_2\rangle$.

(6) Let G, H, I be groups, h be a homomorphism from G to H, and h_1 be a homomorphism from H to I. Then $h_1 \cdot h$ is a homomorphism from G to I.

Let G, H, I be groups, let h be a homomorphism from G to H, and let h_1 be a homomorphism from H to I. Then $h_1 \cdot h$ is a homomorphism from G to I.

One can prove the following propositions:

(7) Let G, H be groups and h be a homomorphism from G to H. If h is bijective, then h^{-1} is a homomorphism from H to G.

(8) Let X, Y be sequences of groups. Then there exists a homomorphism I from $\prod\langle\prod X, \prod Y\rangle$ to $\prod(X \frown Y)$ such that

(i) I is bijective, and

(ii) for every element x of $\prod X$ and for every element y of $\prod Y$ there exist finite sequences x_1, y_1 such that $x = x_1$ and $y = y_1$ and $I(\langle x, y\rangle) = x_1 \frown y_1$.

(9) Let X, Y be Abelian groups. Then there exists a homomorphism I from $X \times Y$ to $X \times \prod\langle Y\rangle$ such that I is bijective and for every element x of X and for every element y of Y holds $I(x, y) = \langle x, \langle y\rangle\rangle$.

(10) Let X be a sequence of groups and Y be an Abelian group. Then there exists a homomorphism I from $\prod X \times Y$ to $\prod(X \frown \langle Y\rangle)$ such that

(i) I is bijective, and

(ii) for every element x of $\prod X$ and for every element y of Y there exist finite sequences x_1, y_1 such that $x = x_1$ and $\langle y\rangle = y_1$ and $I(x, y) = x_1 \frown y_1$.

(11) Let n be a non zero natural number. Then the additive loop structure of $(\mathbb{Z}_n^{\mathrm{R}})$ is non empty, Abelian, right complementable, add-associative, and right zeroed.

Let n be a natural number. The functor $\mathbb{Z}/n\mathbb{Z}$ yields an additive loop structure and is defined by:

(Def. 1) $\mathbb{Z}/n\mathbb{Z} =$ the additive loop structure of $(\mathbb{Z}_n^{\mathrm{R}})$.

Let n be a non zero natural number. Observe that $\mathbb{Z}/n\mathbb{Z}$ is non empty and strict.

Let n be a non zero natural number. Note that $\mathbb{Z}/n\mathbb{Z}$ is Abelian, right complementable, add-associative, and right zeroed.

Next we state a number of propositions:

(12) Let X be a sequence of groups, x, y, z be elements of $\prod X$, and x_1, y_1, z_1 be finite sequences. Suppose $x = x_1$ and $y = y_1$ and $z = z_1$. Then $z = x + y$ if and only if for every element j of $\mathrm{dom}\,\overline{X}$ holds $z_1(j) =$ (the addition of $X(j))(x_1(j), y_1(j))$.

(13) For every CR-sequence m and for every natural number j and for every integer x such that $j \in \mathrm{dom}\, m$ holds $x \bmod \prod m \bmod m(j) = x \bmod m(j)$.

(14) Let m be a CR-sequence and X be a sequence of groups. Suppose $\mathrm{len}\, m = \mathrm{len}\, X$ and for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, X$ there exists a non zero natural number m_1 such that $m_1 = m(i)$ and $X(i) = \mathbb{Z}/m_1\mathbb{Z}$. Then there exists a homomorphism I from $\mathbb{Z}/(\prod m)\mathbb{Z}$ to $\prod X$ such that for every integer x if $x \in$ the carrier of $\mathbb{Z}/(\prod m)\mathbb{Z}$, then $I(x) = \mathrm{mod}(x, m)$.

(15) Let X, Y be non empty sets. Then there exists a function I from $X \times Y$ into $X \times \prod\langle Y\rangle$ such that I is one-to-one and onto and for all sets x, y such that $x \in X$ and $y \in Y$ holds $I(x, y) = \langle x, \langle y\rangle\rangle$.

(16) For every non empty set X holds $\overline{\overline{\prod\langle X\rangle}} = \overline{\overline{X}}$.

(17) Let X be a non-empty non empty finite sequence and Y be a non empty set. Then there exists a function I from $\prod X \times Y$ into $\prod(X \frown \langle Y\rangle)$ such that

(i) I is one-to-one and onto, and

(ii) for all sets x, y such that $x \in \prod X$ and $y \in Y$ there exist finite sequences x_1, y_1 such that $x = x_1$ and $\langle y \rangle = y_1$ and $I(x, y) = x_1 \frown y_1$.

(18) Let m be a finite sequence of elements of $\mathbb{N}$ and X be a non-empty non empty finite sequence. Suppose $\operatorname{len} m = \operatorname{len} X$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} X$ holds $\overline{\overline{X(i)}} = m(i)$. Then $\overline{\overline{\prod X}} = \prod m$.

(19) Let m be a CR-sequence and X be a sequence of groups. Suppose $\operatorname{len} m = \operatorname{len} X$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} X$ there exists a non zero natural number m_1 such that $m_1 = m(i)$ and $X(i) = \mathbb{Z}/m_1\mathbb{Z}$. Then $\overline{\overline{\text{the carrier of } \prod X}} = \prod m$.

(20) Let m be a CR-sequence, X be a sequence of groups, and I be a function from $\mathbb{Z}/(\prod m)\mathbb{Z}$ into $\prod X$. Suppose that

(i) $\operatorname{len} m = \operatorname{len} X$,

(ii) for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} X$ there exists a non zero natural number m_1 such that $m_1 = m(i)$ and $X(i) = \mathbb{Z}/m_1\mathbb{Z}$, and

(iii) for every integer x such that $x \in$ the carrier of $\mathbb{Z}/(\prod m)\mathbb{Z}$ holds $I(x) = \operatorname{mod}(x, m)$.

Then I is one-to-one.

(21) Let m be a CR-sequence and X be a sequence of groups. Suppose $\operatorname{len} m = \operatorname{len} X$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} X$ there exists a non zero natural number m_1 such that $m_1 = m(i)$ and $X(i) = \mathbb{Z}/m_1\mathbb{Z}$. Then there exists a homomorphism I from $\mathbb{Z}/(\prod m)\mathbb{Z}$ to $\prod X$ such that I is bijective and for every integer x such that $x \in$ the carrier of $\mathbb{Z}/(\prod m)\mathbb{Z}$ holds $I(x) = \operatorname{mod}(x, m)$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 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] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

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

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

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

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

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

[10] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

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

[12] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**):841–845, 1990.

[13] Artur Korniłowicz. On the real valued functions. *Formalized Mathematics*, 13(**1**):181–187, 2005.

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

[15] Anna Lango and Grzegorz Bancerek. Product of families of groups and vector spaces. *Formalized Mathematics*, 3(**2**):235–240, 1992.
[16] Hiroyuki Okazaki, Noboru Endou, and Yasunari Shidama. Cartesian products of family of real linear spaces. *Formalized Mathematics*, 19(**1**):51–59, 2011, doi: 10.2478/v10037-011-0009-2.
[17] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[18] Christoph Schwarzweller. Modular integer arithmetic. *Formalized Mathematics*, 16(**3**):247–252, 2008, doi:10.2478/v10037-008-0029-8.
[19] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[20] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[21] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[22] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[23] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received August 27, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 4, Pages 349–357, 2012
DOI: 10.2478/v10037-012-0039-4

VERSITA
versita.com/fm/

On L^1 Space Formed by Complex-Valued Partial Functions

Yasushige Watase
3-21-6 Suginami
Tokyo, Japan

Noboru Endou
Gifu National College of Technology
Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalized L^1 space formed by complex-valued partial functions [11], [15]. The real-valued case was formalized in [22] and this article is its generalization.

MML identifier: LPSPACC1, version: 8.0.01 5.4.1165

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

1. Preliminaries of Complex Linear Space

Let D be a non empty set and let E be a complex-membered set. One can verify that every element of $D \dot{\rightarrow} E$ is complex-valued.

Let D be a non empty set, let E be a complex-membered set, and let F_1, F_2 be elements of $D \dot{\rightarrow} E$. Then $F_1 + F_2$ is an element of $D \dot{\rightarrow} \mathbb{C}$. Then $F_1 - F_2$ is an element of $D \dot{\rightarrow} \mathbb{C}$. Then $F_1 \cdot F_2$ is an element of $D \dot{\rightarrow} \mathbb{C}$. Then F_1 / F_2 is an element of $D \dot{\rightarrow} \mathbb{C}$.

Let D be a non empty set, let E be a complex-membered set, let F be an element of $D \dot{\rightarrow} E$, and let a be a complex number. Then $a \cdot F$ is an element of $D \dot{\rightarrow} \mathbb{C}$.

Let V be a non empty CLS structure and let V_1 be a subset of V. We say that V_1 is multiplicatively closed if and only if:

ISSN 1426–2630(p), 1898-9934(e)

(Def. 1) For every complex number a and for every vector v of V such that $v \in V_1$ holds $a \cdot v \in V_1$.

Next we state the proposition

(1) Let V be a complex linear space and V_1 be a subset of V. Then V_1 is linearly closed if and only if V_1 is add closed and multiplicatively closed.

Let V be a non empty CLS structure. One can verify that there exists a non empty subset of V which is add closed and multiplicatively closed.

Let X be a non empty CLS structure and let X_1 be a multiplicatively closed non empty subset of X. The functor $\cdot_{(X_1)}$ yields a function from $\mathbb{C} \times X_1$ into X_1 and is defined by:

(Def. 2) $\cdot_{(X_1)} =$ (the external multiplication of $X) \restriction (\mathbb{C} \times X_1)$.

In the sequel a, b, r denote complex numbers and V denotes a complex linear space.

We now state two propositions:

(2) Let V be an Abelian add-associative right zeroed vector distributive scalar distributive scalar associative scalar unital non empty CLS structure, V_1 be a non empty subset of V, d_1 be an element of V_1, A be a binary operation on V_1, and M be a function from $\mathbb{C} \times V_1$ into V_1. Suppose $d_1 = 0_V$ and $A =$ (the addition of $V) \restriction (V_1)$ and $M =$ (the external multiplication of $V) \restriction (\mathbb{C} \times V_1)$. Then $\langle V_1, d_1, A, M \rangle$ is Abelian, add-associative, right zeroed, vector distributive, scalar distributive, scalar associative, and scalar unital.

(3) Let V be an Abelian add-associative right zeroed vector distributive scalar distributive scalar associative scalar unital non empty CLS structure and V_1 be an add closed multiplicatively closed non empty subset of V. Suppose $0_V \in V_1$. Then $\langle V_1, 0_V(\in V_1), \mathrm{add}\,|(V_1, V), \cdot_{(V_1)} \rangle$ is Abelian, add-associative, right zeroed, vector distributive, scalar distributive, scalar associative, and scalar unital.

2. Quasi-Complex Linear Space of Partial Functions

We follow the rules: A, B are non empty sets and f, g, h are elements of $A \dot{\to} \mathbb{C}$.

Let us consider A. The functor multcpfunc A yielding a binary operation on $A \dot{\to} \mathbb{C}$ is defined as follows:

(Def. 3) For all elements f, g of $A \dot{\to} \mathbb{C}$ holds $(\mathrm{multcpfunc}\, A)(f, g) = f \cdot g$.

Let us consider A. The functor multcomplexcpfunc A yielding a function from $\mathbb{C} \times (A \dot{\to} \mathbb{C})$ into $A \dot{\to} \mathbb{C}$ is defined by:

(Def. 4) For every complex number a and for every element f of $A \dot{\to} \mathbb{C}$ holds $(\mathrm{multcomplexcpfunc}\, A)(a, f) = a \cdot f$.

Let D be a non empty set. The functor addcpfunc D yields a binary operation on $D \dot{\to} \mathbb{C}$ and is defined as follows:

(Def. 5) For all elements F_1, F_2 of $D \dot{\to} \mathbb{C}$ holds $(\text{addcpfunc}\, D)(F_1, F_2) = F_1 + F_2$.

Let A be a set. The functor CPFuncZero A yields an element of $A \dot{\to} \mathbb{C}$ and is defined by:

(Def. 6) $\text{CPFuncZero}\, A = A \longmapsto 0_{\mathbb{C}}$.

Let A be a set. The functor CPFuncUnit A yielding an element of $A \dot{\to} \mathbb{C}$ is defined as follows:

(Def. 7) $\text{CPFuncUnit}\, A = A \longmapsto 1_{\mathbb{C}}$.

The following propositions are true:

(4) $h = (\text{addcpfunc}\, A)(f, g)$ iff $\text{dom}\, h = \text{dom}\, f \cap \text{dom}\, g$ and for every element x of A such that $x \in \text{dom}\, h$ holds $h(x) = f(x) + g(x)$.

(5) $h = (\text{multcpfunc}\, A)(f, g)$ iff $\text{dom}\, h = \text{dom}\, f \cap \text{dom}\, g$ and for every element x of A such that $x \in \text{dom}\, h$ holds $h(x) = f(x) \cdot g(x)$.

(6) $\text{CPFuncZero}\, A \neq \text{CPFuncUnit}\, A$.

(7) $h = (\text{multcomplexcpfunc}\, A)(a, f)$ iff $\text{dom}\, h = \text{dom}\, f$ and for every element x of A such that $x \in \text{dom}\, f$ holds $h(x) = a \cdot f(x)$.

Let us consider A. Note that addcpfunc A is commutative and associative.

Observe that multcpfunc A is commutative and associative.

One can prove the following propositions:

(8) CPFuncUnit A is a unity w.r.t. multcpfunc A.

(9) CPFuncZero A is a unity w.r.t. addcpfunc A.

(10) $(\text{addcpfunc}\, A)(f, (\text{multcomplexcpfunc}\, A)(-1_{\mathbb{C}}, f)) = \text{CPFuncZero}\, A \restriction \text{dom}\, f$.

(11) $(\text{multcomplexcpfunc}\, A)(1_{\mathbb{C}}, f) = f$.

(12) $(\text{multcomplexcpfunc}\, A)(a, (\text{multcomplexcpfunc}\, A)(b, f)) = (\text{multcomplexcpfunc}\, A)(a \cdot b, f)$.

(13) $(\text{addcpfunc}\, A)((\text{multcomplexcpfunc}\, A)(a, f), (\text{multcomplexcpfunc}\, A)(b, f)) = (\text{multcomplexcpfunc}\, A)(a + b, f)$.

(14) $(\text{multcpfunc}\, A)(f, (\text{addcpfunc}\, A)(g, h)) = (\text{addcpfunc}\, A)((\text{multcpfunc}\, A)(f, g), (\text{multcpfunc}\, A)(f, h))$.

(15) $(\text{multcpfunc}\, A)((\text{multcomplexcpfunc}\, A)(a, f), g) = (\text{multcomplexcpfunc}\, A)(a, (\text{multcpfunc}\, A)(f, g))$.

Let us consider A. The functor CLSp PFunct A yields a non empty CLS structure and is defined as follows:

(Def. 8) $\text{CLSp PFunct}\, A = \langle A \dot{\to} \mathbb{C}, \text{CPFuncZero}\, A, \text{addcpfunc}\, A, \text{multcomplexcpfunc}\, A \rangle$.

In the sequel u, v, w are vectors of CLSp PFunct A.

Note that CLSp PFunct A is strict, Abelian, add-associative, right zeroed, vector distributive, scalar distributive, scalar associative, and scalar unital.

3. Quasi-Complex Linear Space of Integrable Functions

For simplicity, we use the following convention: X is a non empty set, x is an element of X, S is a σ-field of subsets of X, M is a σ-measure on S, E, A are elements of S, and f, g, h, f_1, g_1 are partial functions from X to $\mathbb{C}$.

Let us consider X and let f be a partial function from X to $\mathbb{C}$. Note that $|f|$ is non-negative.

Next we state the proposition

(16) Let f be a partial function from X to $\mathbb{C}$. Suppose $\operatorname{dom} f \in S$ and for every x such that $x \in \operatorname{dom} f$ holds $0 = f(x)$. Then f is integrable on M and $\int f \, \mathrm{d}M = 0$.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. The functor L_1CFunctions M yielding a non empty subset of CLSp PFunct X is defined by the condition (Def. 9).

(Def. 9) $\mathrm{L}_1\mathrm{CFunctions}\, M = \{f; f$ ranges over partial functions from X to $\mathbb{C}$: $\bigvee_{N_1 : \text{element of } S} (M(N_1) = 0 \ \wedge \ \operatorname{dom} f = {N_1}^{\mathrm{c}} \ \wedge \ f$ is integrable on $M)\}$.

The following propositions are true:

(17) If f, $g \in \mathrm{L}_1\mathrm{CFunctions}\, M$, then $f + g \in \mathrm{L}_1\mathrm{CFunctions}\, M$.

(18) If $f \in \mathrm{L}_1\mathrm{CFunctions}\, M$, then $a \cdot f \in \mathrm{L}_1\mathrm{CFunctions}\, M$.

Note that L_1CFunctions M is multiplicatively closed and add closed.

The functor CLSp L_1Funct M yielding a non empty CLS structure is defined by:

(Def. 10) $\mathrm{CLSp}\ \mathrm{L}_1\mathrm{Funct}\, M = \langle \mathrm{L}_1\mathrm{CFunctions}\, M, 0_{\mathrm{CLSp\ PFunct}\, X} (\in \mathrm{L}_1\mathrm{CFunctions}\, M),$ $\mathrm{add} \restriction (\mathrm{L}_1\mathrm{CFunctions}\, M, \mathrm{CLSp\ PFunct}\, X), \cdot_{\mathrm{L}_1\mathrm{CFunctions}\, M} \rangle$.

One can verify that CLSp L_1Funct M is strict, Abelian, add-associative, right zeroed, vector distributive, scalar distributive, scalar associative, and scalar unital.

4. Quotient Space of Quasi-Complex Linear Space of Integrable Functions

In the sequel v, u are vectors of CLSp L_1Funct M.

Next we state two propositions:

(19) If $f = v$ and $g = u$, then $f + g = v + u$.

(20) If $f = u$, then $a \cdot f = a \cdot u$.

Let X be a non empty set, let S be a σ-field of subsets of X, let M be a σ-measure on S, and let f, g be partial functions from X to $\mathbb{C}$. We say that f a.e.cpfunc $= g$ and M if and only if:

(Def. 11) There exists an element E of S such that $M(E) = 0$ and $f \restriction E^{\rm c} = g \restriction E^{\rm c}$.

We now state several propositions:

(21) Suppose $f = u$. Then
 (i) $u + (-1_{\mathbb{C}}) \cdot u = (X \longmapsto 0_{\mathbb{C}}) \restriction \operatorname{dom} f$, and
 (ii) there exist partial functions v, g from X to $\mathbb{C}$ such that $v, g \in$ $\mathrm{L_1CFunctions}\, M$ and $v = u + (-1_{\mathbb{C}}) \cdot u$ and $g = X \longmapsto 0_{\mathbb{C}}$ and v a.e.cpfunc $= g$ and M.

(22) f a.e.cpfunc $= f$ and M.

(23) If f a.e.cpfunc $= g$ and M, then g a.e.cpfunc $= f$ and M.

(24) If f a.e.cpfunc $= g$ and M and g a.e.cpfunc $= h$ and M, then f a.e.cpfunc $= h$ and M.

(25) If f a.e.cpfunc $= f_1$ and M and g a.e.cpfunc $= g_1$ and M, then $f + g$ a.e.cpfunc $= f_1 + g_1$ and M.

(26) If f a.e.cpfunc $= g$ and M, then $a \cdot f$ a.e.cpfunc $= a \cdot g$ and M.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. The almost zero cfunctions of M yields a non empty subset of CLSp $\mathrm{L_1Funct}\, M$ and is defined by the condition (Def. 12).

(Def. 12) The almost zero cfunctions of $M = \{f; f$ ranges over partial functions from X to $\mathbb{C}$: $f \in \mathrm{L_1CFunctions}\, M \ \wedge\ f$ a.e.cpfunc $= X \longmapsto 0_{\mathbb{C}}$ and $M\}$.

One can prove the following proposition

(27) $(X \longmapsto 0_{\mathbb{C}}) + (X \longmapsto 0_{\mathbb{C}}) = X \longmapsto 0_{\mathbb{C}}$ and $a \cdot (X \longmapsto 0_{\mathbb{C}}) = X \longmapsto 0_{\mathbb{C}}$.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. One can check that the almost zero cfunctions of M is add closed and multiplicatively closed.

One can prove the following proposition

(28) $0_{\mathrm{CLSp\ L_1Funct}\, M} = X \longmapsto 0_{\mathbb{C}}$ and $0_{\mathrm{CLSp\ L_1Funct}\, M} \in$ the almost zero cfunctions of M.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. The clsp almost zero functions of M yields a non empty CLS structure and is defined by the condition (Def. 13).

(Def. 13) The clsp almost zero functions of $M = \langle$the almost zero cfunctions of M, $0_{\mathrm{CLSp\ L_1Funct}\, M}(\in$ the almost zero cfunctions of $M)$, add $|$(the almost zero cfunctions of M, CLSp $\mathrm{L_1Funct}\, M)$, $\cdot_{\text{the almost zero cfunctions of } M}\rangle$.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. One can check that CLSp $\mathrm{L_1Funct}\, M$ is strict, Abelian, add-associative, right zeroed, vector distributive, scalar distributive, scalar associative, and scalar unital.

In the sequel v, u are vectors of the clsp almost zero functions of M.

One can prove the following proposition

(29) If $f = v$ and $g = u$, then $f + g = v + u$.

Let X be a non empty set, let S be a σ-field of subsets of X, let M be a σ-measure on S, and let f be a partial function from X to $\mathbb{C}$. The functor a.e-Ceq-class(f, M) yields a subset of L_1CFunctions M and is defined as follows:

(Def. 14) a.e-Ceq-class$(f, M) = \{g; g$ ranges over partial functions from X to $\mathbb{C}$: $g \in \mathrm{L}_1$CFunctions $M \wedge f \in \mathrm{L}_1$CFunctions $M \wedge f$ a.e.cpfunc $= g$ and $M\}$.

Next we state several propositions:

(30) If f, $g \in \mathrm{L}_1$CFunctions M, then g a.e.cpfunc $= f$ and M iff $g \in$ a.e-Ceq-class(f, M).

(31) If $f \in \mathrm{L}_1$CFunctions M, then $f \in$ a.e-Ceq-class(f, M).

(32) If $f, g \in \mathrm{L}_1$CFunctions M, then a.e-Ceq-class$(f, M) =$ a.e-Ceq-class(g, M) iff f a.e.cpfunc $= g$ and M.

(33) If $f, g \in \mathrm{L}_1$CFunctions M, then a.e-Ceq-class$(f, M) =$ a.e-Ceq-class(g, M) iff $g \in$ a.e-Ceq-class(f, M).

(34) If f, f_1, g, $g_1 \in \mathrm{L}_1$CFunctions M and a.e-Ceq-class$(f, M) =$ a.e-Ceq-class(f_1, M) and a.e-Ceq-class$(g, M) =$ a.e-Ceq-class(g_1, M), then a.e-Ceq-class$(f + g, M) =$ a.e-Ceq-class$(f_1 + g_1, M)$.

(35) If $f, g \in \mathrm{L}_1$CFunctions M and a.e-Ceq-class$(f, M) =$ a.e-Ceq-class(g, M), then a.e-Ceq-class$(a \cdot f, M) =$ a.e-Ceq-class$(a \cdot g, M)$.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. The functor CCosetSet M yields a non empty family of subsets of L_1CFunctions M and is defined by:

(Def. 15) CCosetSet $M = \{$a.e-Ceq-class$(f, M); f$ ranges over partial functions from X to $\mathbb{C}$: $f \in \mathrm{L}_1$CFunctions $M\}$.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. The functor addCCoset M yields a binary operation on CCosetSet M and is defined by the condition (Def. 16).

(Def. 16) Let A, B be elements of CCosetSet M and a, b be partial functions from X to $\mathbb{C}$. If $a \in A$ and $b \in B$, then (addCCoset M)$(A, B) =$ a.e-Ceq-class$(a + b, M)$.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. The functor zeroCCoset M yielding an element of CCosetSet M is defined by:

(Def. 17) zeroCCoset $M =$ a.e-Ceq-class$(X \longmapsto 0_{\mathbb{C}}, M)$.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. The functor lmultCCoset M yields a function from $\mathbb{C} \times$ CCosetSet M into CCosetSet M and is defined by the condition (Def. 18).

(Def. 18) Let z be a complex number, A be an element of CCosetSet M, and f be a partial function from X to $\mathbb{C}$. If $f \in A$, then $(\text{lmultCCoset}\,M)(z, A) =$ a.e-Ceq-class$(z \cdot f, M)$.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. The functor Pre-L-CSpace M yields a strict Abelian add-associative right zeroed right complementable vector distributive scalar distributive scalar associative scalar unital non empty CLS structure and is defined by the conditions (Def. 19).

(Def. 19)(i) The carrier of Pre-L-CSpace M = CCosetSet M,

(ii) the addition of Pre-L-CSpace M = addCCoset M,

(iii) $0_{\text{Pre-L-CSpace}\,M}$ = zeroCCoset M, and

(iv) the external multiplication of Pre-L-CSpace M = lmultCCoset M.

5. Complex Normed Space of Integrable Functions

Next we state several propositions:

(36) If f, $g \in \mathrm{L}_1$CFunctions M and f a.e.cpfunc $= g$ and M, then $\int f\,\mathrm{d}M = \int g\,\mathrm{d}M$.

(37) If f is integrable on M, then $\int f\,\mathrm{d}M \in \mathbb{C}$ and $\int |f|\,\mathrm{d}M \in \mathbb{R}$ and $|f|$ is integrable on M.

(38) If f, $g \in \mathrm{L}_1$CFunctions M and f a.e.cpfunc $= g$ and M, then $|f| =_{\text{a.e.}}^{M} |g|$ and $\int |f|\,\mathrm{d}M = \int |g|\,\mathrm{d}M$.

(39) If there exists a vector x of Pre-L-CSpace M such that f, $g \in x$, then f a.e.cpfunc $= g$ and M and f, $g \in \mathrm{L}_1$CFunctions M.

(40) There exists a function N_2 from the carrier of Pre-L-CSpace M into $\mathbb{R}$ such that for every point x of Pre-L-CSpace M holds there exists a partial function f from X to $\mathbb{C}$ such that $f \in x$ and $N_2(x) = \int |f|\,\mathrm{d}M$.

In the sequel x is a point of Pre-L-CSpace M.

The following two propositions are true:

(41) If $f \in x$, then f is integrable on M and $f \in \mathrm{L}_1$CFunctions M and $|f|$ is integrable on M.

(42) If f, $g \in x$, then f a.e.cpfunc $= g$ and M and $\int f\,\mathrm{d}M = \int g\,\mathrm{d}M$ and $\int |f|\,\mathrm{d}M = \int |g|\,\mathrm{d}M$.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. The functor L-1-CNorm M yields a function from the carrier of Pre-L-CSpace M into $\mathbb{R}$ and is defined by:

(Def. 20) For every point x of Pre-L-CSpace M there exists a partial function f from X to $\mathbb{C}$ such that $f \in x$ and (L-1-CNorm $M)(x) = \int |f| \, \mathrm{d}M$.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. The functor L-1-CSpace M yields a non empty complex normed space structure and is defined as follows:

(Def. 21) L-1-CSpace M = $\langle$the carrier of Pre-L-CSpace M, the zero of Pre-L-CSpace M, the addition of Pre-L-CSpace M, the external multiplication of Pre-L-CSpace M, L-1-CNorm $M\rangle$.

In the sequel x denotes a point of L-1-CSpace M.

Next we state several propositions:

(43)(i) There exists a partial function f from X to $\mathbb{C}$ such that $f \in$ L_1CFunctions M and $x =$ a.e-Ceq-class(f, M) and $\|x\| = \int |f| \, \mathrm{d}M$, and

(ii) for every partial function f from X to $\mathbb{C}$ such that $f \in x$ holds $\int |f| \, \mathrm{d}M = \|x\|$.

(44) If $f \in x$, then $x =$ a.e-Ceq-class(f, M) and $\|x\| = \int |f| \, \mathrm{d}M$.

(45) If $f \in x$ and $g \in y$, then $f + g \in x + y$ and if $f \in x$, then $a \cdot f \in a \cdot x$.

(46) If $f \in \mathrm{L}_1$CFunctions M and $\int |f| \, \mathrm{d}M = 0$, then f a.e.cpfunc $= X \longmapsto 0_{\mathbb{C}}$ and M.

(47) If f, $g \in \mathrm{L}_1$CFunctions M, then $\int |f + g| \, \mathrm{d}M \leq \int |f| \, \mathrm{d}M + \int |g| \, \mathrm{d}M$.

Let X be a non empty set, let S be a σ-field of subsets of X, and let M be a σ-measure on S. One can check that L-1-CSpace M is complex normed space-like, vector distributive, scalar distributive, scalar associative, scalar unital, Abelian, add-associative, right zeroed, and right complementable.

References

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

[2] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.

[3] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.

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

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

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

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

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

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

[10] Noboru Endou. Complex linear space and complex normed space. *Formalized Mathematics*, 12(**2**):93–102, 2004.

[11] P. R. Halmos. *Measure Theory*. Springer-Verlag, 1974.

[12] 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.

[13] Keiko Narita, Noboru Endou, and Yasunari Shidama. Integral of complex-valued measurable function. *Formalized Mathematics*, 16(**4**):319–324, 2008, doi:10.2478/v10037-008-0039-6.
[14] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.
[15] Walter Rudin. *Real and Complex Analysis*. Mc Graw-Hill, Inc., 1974.
[16] Yasunari Shidama and Noboru Endou. Integral of real-valued measurable function. *Formalized Mathematics*, 14(**4**):143–152, 2006, doi:10.2478/v10037-006-0018-8.
[17] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[18] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[19] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.
[20] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[22] Yasushige Watase, Noboru Endou, and Yasunari Shidama. On L^1 space formed by real-valued partial functions. *Formalized Mathematics*, 16(**4**):361–369, 2008, doi:10.2478/v10037-008-0044-9.
[23] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[24] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received August 27, 2012