# Contents

*Formaliz. Math.* 16 (**3**)

FORMALIZED MATHEMATICS
Vol. **16**, No. **3**, Pages 231–245, **2008**

# Model Checking. Part II

Kazuhisa Ishida
Shinshu University
Nagano, Japan

**Summary.** This article provides the definition of linear temporal logic (LTL) and its properties relevant to model checking based on [9]. Mizar formalization of LTL language and satisfiability is based on [2, 3].

MML identifier: MODELC_2, version: 7.9.01 4.101.1015

The articles [8], [11], [6], [5], [7], [1], [4], [12], and [10] provide the notation and terminology for this paper.

Let $x$ be a set. The functor $\mathrm{CastNat}\, x$ yielding a natural number is defined by:

(Def. 1) $\mathrm{CastNat}\, x = \begin{cases} x, & \text{if } x \text{ is a natural number,} \\ 0, & \text{otherwise.} \end{cases}$

Let $W_1$ be a set. A sequence of $W_1$ is a function from $\mathbb{N}$ into $W_1$.

For simplicity, we adopt the following rules: $k$, $n$ denote natural numbers, $a$ denotes a set, $D$, $S$ denote non empty sets, and $p$, $q$ denote finite sequences of elements of $\mathbb{N}$.

Let us consider $n$. The functor $\mathrm{atom.}\, n$ yielding a finite sequence of elements of $\mathbb{N}$ is defined as follows:

(Def. 2) $\mathrm{atom.}\, n = \langle 6 + n \rangle$.

Let us consider $p$. The functor $\neg p$ yielding a finite sequence of elements of $\mathbb{N}$ is defined by:

(Def. 3) $\neg p = \langle 0 \rangle ^\frown p$.

Let us consider $q$. The functor $p \wedge q$ yields a finite sequence of elements of $\mathbb{N}$ and is defined by:

(Def. 4) $p \wedge q = \langle 1 \rangle ^\frown p ^\frown q$.

The functor $p \vee q$ yielding a finite sequence of elements of $\mathbb{N}$ is defined by:




ISSN 1426–2630(p), 1898-9934(e)

(Def. 5) $p \vee q = \langle 2 \rangle \mathbin{^\frown} p \mathbin{^\frown} q$.

Let us consider $p$. The functor $\mathcal{X}\, p$ yielding a finite sequence of elements of $\mathbb{N}$ is defined as follows:

(Def. 6) $\mathcal{X}\, p = \langle 3 \rangle \mathbin{^\frown} p$.

Let us consider $q$. The functor $p\,\mathcal{U}\,q$ yielding a finite sequence of elements of $\mathbb{N}$ is defined by:

(Def. 7) $p\,\mathcal{U}\,q = \langle 4 \rangle \mathbin{^\frown} p \mathbin{^\frown} q$.

The functor $p\,\mathcal{R}\,q$ yields a finite sequence of elements of $\mathbb{N}$ and is defined as follows:

(Def. 8) $p\,\mathcal{R}\,q = \langle 5 \rangle \mathbin{^\frown} p \mathbin{^\frown} q$.

The non empty set $\mathrm{WFF}_{\mathrm{LTL}}$ is defined by the conditions (Def. 9).

(Def. 9) For every $a$ such that $a \in \mathrm{WFF}_{\mathrm{LTL}}$ holds $a$ is a finite sequence of elements of $\mathbb{N}$ and for every $n$ holds $\mathrm{atom.}\, n \in \mathrm{WFF}_{\mathrm{LTL}}$ and for every $p$ such that $p \in \mathrm{WFF}_{\mathrm{LTL}}$ holds $\neg p \in \mathrm{WFF}_{\mathrm{LTL}}$ and for all $p$, $q$ such that $p$, $q \in \mathrm{WFF}_{\mathrm{LTL}}$ holds $p \wedge q \in \mathrm{WFF}_{\mathrm{LTL}}$ and for all $p$, $q$ such that $p$, $q \in \mathrm{WFF}_{\mathrm{LTL}}$ holds $p \vee q \in \mathrm{WFF}_{\mathrm{LTL}}$ and for every $p$ such that $p \in \mathrm{WFF}_{\mathrm{LTL}}$ holds $\mathcal{X}\, p \in \mathrm{WFF}_{\mathrm{LTL}}$ and for all $p$, $q$ such that $p$, $q \in \mathrm{WFF}_{\mathrm{LTL}}$ holds $p\,\mathcal{U}\,q \in \mathrm{WFF}_{\mathrm{LTL}}$ and for all $p$, $q$ such that $p$, $q \in \mathrm{WFF}_{\mathrm{LTL}}$ holds $p\,\mathcal{R}\,q \in \mathrm{WFF}_{\mathrm{LTL}}$ and for every $D$ such that for every $a$ such that $a \in D$ holds $a$ is a finite sequence of elements of $\mathbb{N}$ and for every $n$ holds $\mathrm{atom.}\, n \in D$ and for every $p$ such that $p \in D$ holds $\neg p \in D$ and for all $p$, $q$ such that $p$, $q \in D$ holds $p \wedge q \in D$ and for all $p$, $q$ such that $p$, $q \in D$ holds $p \vee q \in D$ and for every $p$ such that $p \in D$ holds $\mathcal{X}\, p \in D$ and for all $p$, $q$ such that $p$, $q \in D$ holds $p\,\mathcal{U}\,q \in D$ and for all $p$, $q$ such that $p$, $q \in D$ holds $p\,\mathcal{R}\,q \in D$ holds $\mathrm{WFF}_{\mathrm{LTL}} \subseteq D$.

Let $I_1$ be a finite sequence of elements of $\mathbb{N}$. We say that $I_1$ is LTL-formula-like if and only if:

(Def. 10) $I_1$ is an element of $\mathrm{WFF}_{\mathrm{LTL}}$.

Let us observe that there exists a finite sequence of elements of $\mathbb{N}$ which is LTL-formula-like.

An LTL-formula is a LTL-formula-like finite sequence of elements of $\mathbb{N}$.

Next we state the proposition

(1) $a$ is an LTL-formula iff $a \in \mathrm{WFF}_{\mathrm{LTL}}$.

In the sequel $F$, $F_1$, $G$, $H$, $H_1$, $H_2$ denote LTL-formulae.

Let us consider $n$. Observe that $\mathrm{atom.}\, n$ is LTL-formula-like.

Let us consider $H$. Note that $\neg H$ is LTL-formula-like and $\mathcal{X}\, H$ is LTL-formula-like. Let us consider $G$. One can check the following observations:

* $H \wedge G$ is LTL-formula-like,
* $H \vee G$ is LTL-formula-like,
* $H\,\mathcal{U}\,G$ is LTL-formula-like, and

* $H \mathcal{R} G$ is LTL-formula-like.

Let us consider $H$. We say that $H$ is atomic if and only if:

(Def. 11) There exists $n$ such that $H = \mathrm{atom}.\, n$.

We say that $H$ is negative if and only if:

(Def. 12) There exists $H_1$ such that $H = \neg H_1$.

We say that $H$ is conjunctive if and only if:

(Def. 13) There exist $F$, $G$ such that $H = F \wedge G$.

We say that $H$ is disjunctive if and only if:

(Def. 14) There exist $F$, $G$ such that $H = F \vee G$.

We say that $H$ has *next* operator if and only if:

(Def. 15) There exists $H_1$ such that $H = \mathcal{X}\, H_1$.

We say that $H$ has *until* operator if and only if:

(Def. 16) There exist $F$, $G$ such that $H = F \,\mathcal{U}\, G$.

We say that $H$ has *release* operator if and only if:

(Def. 17) There exist $F$, $G$ such that $H = F \,\mathcal{R}\, G$.

Next we state two propositions:

(2) $H$ is either atomic, or negative, or conjunctive, or disjunctive, or has *next* operator, or *until* operator, or *release* operator.

(3) $1 \leq \mathrm{len}\, H$.

Let us consider $H$. Let us assume that $H$ is either negative or has *next* operator. The functor $\mathrm{Arg}(H)$ yields an LTL-formula and is defined by:

(Def. 18)(i) $\neg \mathrm{Arg}(H) = H$ if $H$ is negative,

(ii) $\mathcal{X}\, \mathrm{Arg}(H) = H$, otherwise.

Let us consider $H$. Let us assume that $H$ is either conjunctive or disjunctive or has *until* operator or *release* operator. The functor $\mathrm{LeftArg}(H)$ yielding an LTL-formula is defined as follows:

(Def. 19)(i) There exists $H_1$ such that $\mathrm{LeftArg}(H) \wedge H_1 = H$ if $H$ is conjunctive,

(ii) there exists $H_1$ such that $\mathrm{LeftArg}(H) \vee H_1 = H$ if $H$ is disjunctive,

(iii) there exists $H_1$ such that $\mathrm{LeftArg}(H) \mathcal{U} H_1 = H$ if $H$ has *until* operator,

(iv) there exists $H_1$ such that $\mathrm{LeftArg}(H)\, \mathcal{R}\, H_1 = H$, otherwise.

The functor $\mathrm{RightArg}(H)$ yields an LTL-formula and is defined by:

(Def. 20)(i) There exists $H_1$ such that $H_1 \wedge \mathrm{RightArg}(H) = H$ if $H$ is conjunctive,

(ii) there exists $H_1$ such that $H_1 \vee \mathrm{RightArg}(H) = H$ if $H$ is disjunctive,

(iii) there exists $H_1$ such that $H_1 \,\mathcal{U}\, \mathrm{RightArg}(H) = H$ if $H$ has *until* operator,

(iv) there exists $H_1$ such that $H_1 \,\mathcal{R}\, \mathrm{RightArg}(H) = H$, otherwise.

The following propositions are true:

(4) If $H$ is negative, then $H = \neg \mathrm{Arg}(H)$.

(5) If $H$ has *next* operator, then $H = \mathcal{X}\,\mathrm{Arg}(H)$.

(6) If $H$ is conjunctive, then $H = \mathrm{LeftArg}(H) \wedge \mathrm{RightArg}(H)$.

(7) If $H$ is disjunctive, then $H = \mathrm{LeftArg}(H) \vee \mathrm{RightArg}(H)$.

(8) If $H$ has *until* operator, then $H = \mathrm{LeftArg}(H)\,\mathcal{U}\,\mathrm{RightArg}(H)$.

(9) If $H$ has *release* operator, then $H = \mathrm{LeftArg}(H)\,\mathcal{R}\,\mathrm{RightArg}(H)$.

(10) If $H$ is either negative or has *next* operator, then $\mathrm{len}\,H = 1 + \mathrm{len}\,\mathrm{Arg}(H)$ and $\mathrm{len}\,\mathrm{Arg}(H) < \mathrm{len}\,H$.

(11) Suppose $H$ is either conjunctive or disjunctive or has *until* operator or *release* operator. Then $\mathrm{len}\,H = 1 + \mathrm{len}\,\mathrm{LeftArg}(H) + \mathrm{len}\,\mathrm{RightArg}(H)$ and $\mathrm{len}\,\mathrm{LeftArg}(H) < \mathrm{len}\,H$ and $\mathrm{len}\,\mathrm{RightArg}(H) < \mathrm{len}\,H$.

Let us consider $H$, $F$. We say that $H$ is an immediate constituent of $F$ if and only if:

(Def. 21) $F = \neg H$ or $F = \mathcal{X}\,H$ or there exists $H_1$ such that $F = H \wedge H_1$ or $F = H_1 \wedge H$ or $F = H \vee H_1$ or $F = H_1 \vee H$ or $F = H\,\mathcal{U}\,H_1$ or $F = H_1\,\mathcal{U}\,H$ or $F = H\,\mathcal{R}\,H_1$ or $F = H_1\,\mathcal{R}\,H$.

We now state a number of propositions:

(12) For all $F$, $G$ holds $(\neg F)(1) = 0$ and $(F \wedge G)(1) = 1$ and $(F \vee G)(1) = 2$ and $(\mathcal{X}\,F)(1) = 3$ and $(F\,\mathcal{U}\,G)(1) = 4$ and $(F\,\mathcal{R}\,G)(1) = 5$.

(13) $H$ is an immediate constituent of $\neg F$ iff $H = F$.

(14) $H$ is an immediate constituent of $\mathcal{X}\,F$ iff $H = F$.

(15) $H$ is an immediate constituent of $F \wedge G$ iff $H = F$ or $H = G$.

(16) $H$ is an immediate constituent of $F \vee G$ iff $H = F$ or $H = G$.

(17) $H$ is an immediate constituent of $F\,\mathcal{U}\,G$ iff $H = F$ or $H = G$.

(18) $H$ is an immediate constituent of $F\,\mathcal{R}\,G$ iff $H = F$ or $H = G$.

(19) If $F$ is atomic, then $H$ is not an immediate constituent of $F$.

(20) If $F$ is negative, then $H$ is an immediate constituent of $F$ iff $H = \mathrm{Arg}(F)$.

(21) If $F$ has *next* operator, then $H$ is an immediate constituent of $F$ iff $H = \mathrm{Arg}(F)$.

(22) If $F$ is conjunctive, then $H$ is an immediate constituent of $F$ iff $H = \mathrm{LeftArg}(F)$ or $H = \mathrm{RightArg}(F)$.

(23) If $F$ is disjunctive, then $H$ is an immediate constituent of $F$ iff $H = \mathrm{LeftArg}(F)$ or $H = \mathrm{RightArg}(F)$.

(24) If $F$ has *until* operator, then $H$ is an immediate constituent of $F$ iff $H = \mathrm{LeftArg}(F)$ or $H = \mathrm{RightArg}(F)$.

(25) If $F$ has *release* operator, then $H$ is an immediate constituent of $F$ iff $H = \mathrm{LeftArg}(F)$ or $H = \mathrm{RightArg}(F)$.

(26) Suppose $H$ is an immediate constituent of $F$. Then $F$ is either negative, or conjunctive, or disjunctive, or has *next* operator, or *until* operator, or

*release* operator.

In the sequel $L$ denotes a finite sequence.

Let us consider $H$, $F$. We say that $H$ is a subformula of $F$ if and only if the condition (Def. 22) is satisfied.

(Def. 22) There exist $n$, $L$ such that

(i) $1 \leq n$,

(ii) $\operatorname{len} L = n$,

(iii) $L(1) = H$,

(iv) $L(n) = F$, and

(v) for every $k$ such that $1 \leq k < n$ there exist $H_1$, $F_1$ such that $L(k) = H_1$ and $L(k+1) = F_1$ and $H_1$ is an immediate constituent of $F_1$.

We now state the proposition

(27) $H$ is a subformula of $H$.

Let us consider $H$, $F$. We say that $H$ is a proper subformula of $F$ if and only if:

(Def. 23) $H$ is a subformula of $F$ and $H \neq F$.

One can prove the following propositions:

(28) If $H$ is an immediate constituent of $F$, then $\operatorname{len} H < \operatorname{len} F$.

(29) If $H$ is an immediate constituent of $F$, then $H$ is a proper subformula of $F$.

(30) If $G$ is either negative or has *next* operator, then $\operatorname{Arg}(G)$ is a subformula of $G$.

(31) Suppose $G$ is either conjunctive or disjunctive or has *until* operator or *release* operator. Then $\operatorname{LeftArg}(G)$ is a subformula of $G$ and $\operatorname{RightArg}(G)$ is a subformula of $G$.

(32) If $H$ is a proper subformula of $F$, then $\operatorname{len} H < \operatorname{len} F$.

(33) If $H$ is a proper subformula of $F$, then there exists $G$ which is an immediate constituent of $F$.

(34) If $F$ is a proper subformula of $G$ and $G$ is a proper subformula of $H$, then $F$ is a proper subformula of $H$.

(35) If $F$ is a subformula of $G$ and $G$ is a subformula of $H$, then $F$ is a subformula of $H$.

(36) If $G$ is a subformula of $H$ and $H$ is a subformula of $G$, then $G = H$.

(37) If $G$ is either negative or has *next* operator and $F$ is a proper subformula of $G$, then $F$ is a subformula of $\operatorname{Arg}(G)$.

(38) Suppose that

(i) $G$ is either conjunctive or disjunctive or has *until* operator or *release* operator, and

(ii) $F$ is a proper subformula of $G$.

Then $F$ is a subformula of $\mathrm{LeftArg}(G)$ or a subformula of $\mathrm{RightArg}(G)$.

(39) If $F$ is a proper subformula of $\neg H$, then $F$ is a subformula of $H$.

(40) If $F$ is a proper subformula of $\mathcal{X}\,H$, then $F$ is a subformula of $H$.

(41) If $F$ is a proper subformula of $G \wedge H$, then $F$ is a subformula of $G$ or a subformula of $H$.

(42) If $F$ is a proper subformula of $G \vee H$, then $F$ is a subformula of $G$ or a subformula of $H$.

(43) If $F$ is a proper subformula of $G\,\mathcal{U}\,H$, then $F$ is a subformula of $G$ or a subformula of $H$.

(44) If $F$ is a proper subformula of $G\,\mathcal{R}\,H$, then $F$ is a subformula of $G$ or a subformula of $H$.

Let us consider $H$. The functor $\mathrm{Subformulae}\,H$ yields a set and is defined by:

(Def. 24) $a \in \mathrm{Subformulae}\,H$ iff there exists $F$ such that $F = a$ and $F$ is a subformula of $H$.

One can prove the following proposition

(45) $G \in \mathrm{Subformulae}\,H$ iff $G$ is a subformula of $H$.

Let us consider $H$. Observe that $\mathrm{Subformulae}\,H$ is non empty.

Next we state two propositions:

(46) If $F$ is a subformula of $H$, then $\mathrm{Subformulae}\,F \subseteq \mathrm{Subformulae}\,H$.

(47) If $a$ is a subset of $\mathrm{Subformulae}\,H$, then $a$ is a subset of $\mathrm{WFF}_{\mathrm{LTL}}$.

In this article we present several logical schemes. The scheme *LTLInd* concerns a unary predicate $\mathcal{P}$, and states that:

For every $H$ holds $\mathcal{P}[H]$

provided the following conditions are satisfied:

- For every $H$ such that $H$ is atomic holds $\mathcal{P}[H]$,
- For every $H$ such that $H$ is either negative or has *next* operator and $\mathcal{P}[\mathrm{Arg}(H)]$ holds $\mathcal{P}[H]$, and
- Let given $H$. Suppose $H$ is either conjunctive or disjunctive or has *until* operator or *release* operator and $\mathcal{P}[\mathrm{LeftArg}(H)]$ and $\mathcal{P}[\mathrm{RightArg}(H)]$. Then $\mathcal{P}[H]$.

The scheme *LTLCompInd* concerns a unary predicate $\mathcal{P}$, and states that:

For every $H$ holds $\mathcal{P}[H]$

provided the following condition is met:

- For every $H$ such that for every $F$ such that $F$ is a proper subformula of $H$ holds $\mathcal{P}[F]$ holds $\mathcal{P}[H]$.

Let $x$ be a set. The functor $\mathrm{Cast}_{\mathrm{LTL}}\,x$ yielding an LTL-formula is defined by:

(Def. 25) $$\mathrm{Cast}_{\mathrm{LTL}}\,x = \begin{cases} x, & \text{if } x \in \mathrm{WFF}_{\mathrm{LTL}}, \\ \mathrm{atom}.\,0, & \text{otherwise.} \end{cases}$$

We introduce LTL-model structures which are systems

⟨ assignations, basic assignations, a conjunction, a disjunction, a negation, a next-operation, an until-operation, a release-operation ⟩,

where the assignations constitute a non empty set, the basic assignations constitute a non empty subset of the assignations, the conjunction is a binary operation on the assignations, the disjunction is a binary operation on the assignations, the negation is a unary operation on the assignations, the next-operation is a unary operation on the assignations, the until-operation is a binary operation on the assignations, and the release-operation is a binary operation on the assignations.

Let $V$ be an LTL-model structure. An assignation of $V$ is an element of the assignations of $V$.

The subset $\mathrm{atomic}_{\mathrm{LTL}}$ of $\mathrm{WFF}_{\mathrm{LTL}}$ is defined by:

(Def. 26) $\mathrm{atomic}_{\mathrm{LTL}} = \{x; x$ ranges over LTL-formulae: $x$ is atomic$\}$.

Let $V$ be an LTL-model structure, let $K_1$ be a function from $\mathrm{atomic}_{\mathrm{LTL}}$ into the basic assignations of $V$, and let $f$ be a function from $\mathrm{WFF}_{\mathrm{LTL}}$ into the assignations of $V$. We say that $f$ is an evaluation for $K_1$ if and only if the condition (Def. 27) is satisfied.

(Def. 27) Let $H$ be an LTL-formula. Then

(i) if $H$ is atomic, then $f(H) = K_1(H)$,

(ii) if $H$ is negative, then $f(H) =$ (the negation of $V$)$(f(\mathrm{Arg}(H)))$,

(iii) if $H$ is conjunctive, then $f(H) =$ (the conjunction of $V$)$(f(\mathrm{LeftArg}(H)), f(\mathrm{RightArg}(H)))$,

(iv) if $H$ is disjunctive, then $f(H) =$ (the disjunction of $V$)$(f(\mathrm{LeftArg}(H)), f(\mathrm{RightArg}(H)))$,

(v) if $H$ has *next* operator, then $f(H) =$ (the next-operation of $V$)$(f(\mathrm{Arg}(H)))$,

(vi) if $H$ has *until* operator, then $f(H) =$ (the until-operation of $V$)$(f(\mathrm{LeftArg}(H)), f(\mathrm{RightArg}(H)))$, and

(vii) if $H$ has *release* operator, then $f(H) =$ (the release-operation of $V$)$(f(\mathrm{LeftArg}(H)), f(\mathrm{RightArg}(H)))$.

Let $V$ be an LTL-model structure, let $K_1$ be a function from $\mathrm{atomic}_{\mathrm{LTL}}$ into the basic assignations of $V$, let $f$ be a function from $\mathrm{WFF}_{\mathrm{LTL}}$ into the assignations of $V$, and let $n$ be a natural number. We say that $f$ is a $n$-pre-evaluation for $K_1$ if and only if the condition (Def. 28) is satisfied.

(Def. 28) Let $H$ be an LTL-formula such that $\mathrm{len}\, H \leq n$. Then

(i) if $H$ is atomic, then $f(H) = K_1(H)$,

(ii) if $H$ is negative, then $f(H) =$ (the negation of $V$)$(f(\mathrm{Arg}(H)))$,

(iii) if $H$ is conjunctive, then $f(H) =$ (the conjunction of $V$)$(f(\mathrm{LeftArg}(H)), f(\mathrm{RightArg}(H)))$,

(iv) if $H$ is disjunctive, then $f(H) =$ (the disjunction of $V$)($f(\mathrm{LeftArg}(H))$, $f(\mathrm{RightArg}(H))$),

(v) if $H$ has *next* operator, then $f(H) =$ (the next-operation of $V$)($f(\mathrm{Arg}(H))$),

(vi) if $H$ has *until* operator, then $f(H) =$ (the until-operation of $V$)($f(\mathrm{LeftArg}(H))$, $f(\mathrm{RightArg}(H))$), and

(vii) if $H$ has *release* operator, then $f(H) =$ (the release-operation of $V$)($f(\mathrm{LeftArg}(H))$, $f(\mathrm{RightArg}(H))$).

Let $V$ be an LTL-model structure, let $K_1$ be a function from $\mathrm{atomic}_{\mathrm{LTL}}$ into the basic assignations of $V$, let $f$, $h$ be functions from $\mathrm{WFF}_{\mathrm{LTL}}$ into the assignations of $V$, let $n$ be a natural number, and let $H$ be an LTL-formula. The functor $\mathrm{GraftEval}(V, K_1, f, h, n, H)$ yields a set and is defined by:

(Def. 29) $\mathrm{GraftEval}(V, K_1, f, h, n, H)$

$$= \begin{cases} f(H), \text{ if } \mathrm{len}\, H > n+1, \\ K_1(H), \text{ if } \mathrm{len}\, H = n+1 \text{ and } H \text{ is atomic}, \\ (\text{the negation of } V)(h(\mathrm{Arg}(H))), \text{ if } \mathrm{len}\, H = n+1 \text{ and } H \text{ is negative}, \\ (\text{the conjunction of } V)(h(\mathrm{LeftArg}(H)), h(\mathrm{RightArg}(H))), \\ \quad \text{if } \mathrm{len}\, H = n+1 \text{ and } H \text{ is conjunctive}, \\ (\text{the disjunction of } V)(h(\mathrm{LeftArg}(H)), h(\mathrm{RightArg}(H))), \\ \quad \text{if } \mathrm{len}\, H = n+1 \text{ and } H \text{ is disjunctive}, \\ (\text{the next-operation of } V)(h(\mathrm{Arg}(H))), \\ \quad \text{if } \mathrm{len}\, H = n+1 \text{ and } H \text{ has } \textit{next} \text{ operator}, \\ (\text{the until-operation of } V)(h(\mathrm{LeftArg}(H)), h(\mathrm{RightArg}(H))), \\ \quad \text{if } \mathrm{len}\, H = n+1 \text{ and } H \text{ has } \textit{until} \text{ operator}, \\ (\text{the release-operation of } V)(h(\mathrm{LeftArg}(H)), h(\mathrm{RightArg}(H))), \\ \quad \text{if } \mathrm{len}\, H = n+1 \text{ and } H \text{ has } \textit{release} \text{ operator}, \\ h(H), \text{ if } \mathrm{len}\, H < n+1, \\ \emptyset, \text{ otherwise.} \end{cases}$$

We adopt the following convention: $V$ denotes an LTL-model structure, $K_1$ denotes a function from $\mathrm{atomic}_{\mathrm{LTL}}$ into the basic assignations of $V$, and $f$, $f_1$, $f_2$ denote functions from $\mathrm{WFF}_{\mathrm{LTL}}$ into the assignations of $V$.

Let $V$ be an LTL-model structure, let $K_1$ be a function from $\mathrm{atomic}_{\mathrm{LTL}}$ into the basic assignations of $V$, and let $n$ be a natural number. The functor $\mathrm{EvalSet}(V, K_1, n)$ yields a non empty set and is defined by:

(Def. 30) $\mathrm{EvalSet}(V, K_1, n) = \{h; h$ ranges over functions from $\mathrm{WFF}_{\mathrm{LTL}}$ into the assignations of $V$: $h$ is a $n$-pre-evaluation for $K_1\}$.

Let $V$ be an LTL-model structure, let $v_0$ be an element of the assignations of $V$, and let $x$ be a set. The functor $\mathrm{CastEval}(V, x, v_0)$ yielding a function from $\mathrm{WFF}_{\mathrm{LTL}}$ into the assignations of $V$ is defined by:

(Def. 31) $\mathrm{CastEval}(V, x, v_0) = \begin{cases} x, \text{ if } x \in (\text{the assignations of } V)^{\mathrm{WFF}_{\mathrm{LTL}}}, \\ \mathrm{WFF}_{\mathrm{LTL}} \longmapsto v_0, \text{ otherwise.} \end{cases}$

Let $V$ be an LTL-model structure and let $K_1$ be a function from $\mathrm{atomic}_{\mathrm{LTL}}$ into the basic assignations of $V$. The functor $\mathrm{EvalFamily}(V, K_1)$ yielding a non empty set is defined by the condition (Def. 32).

(Def. 32) Let $p$ be a set. Then $p \in \mathrm{EvalFamily}(V, K_1)$ if and only if the following conditions are satisfied:

(i) $p \in 2^{(\text{the assignations of } V)^{\mathrm{WFF}_{\mathrm{LTL}}}}$, and

(ii) there exists a natural number $n$ such that $p = \mathrm{EvalSet}(V, K_1, n)$.

We now state two propositions:

(48) There exists $f$ which is an evaluation for $K_1$.

(49) If $f_1$ is an evaluation for $K_1$ and $f_2$ is an evaluation for $K_1$, then $f_1 = f_2$.

Let $V$ be an LTL-model structure, let $K_1$ be a function from $\mathrm{atomic}_{\mathrm{LTL}}$ into the basic assignations of $V$, and let $H$ be an LTL-formula. The functor $\mathrm{Evaluate}(H, K_1)$ yields an assignation of $V$ and is defined by:

(Def. 33) There exists a function $f$ from $\mathrm{WFF}_{\mathrm{LTL}}$ into the assignations of $V$ such that $f$ is an evaluation for $K_1$ and $\mathrm{Evaluate}(H, K_1) = f(H)$.

Let $V$ be an LTL-model structure and let $f$ be an assignation of $V$. The functor $\neg f$ yielding an assignation of $V$ is defined by:

(Def. 34) $\neg f = (\text{the negation of } V)(f)$.

Let $V$ be an LTL-model structure and let $f$, $g$ be assignations of $V$. The functor $f \wedge g$ yields an assignation of $V$ and is defined by:

(Def. 35) $f \wedge g = (\text{the conjunction of } V)(f, g)$.

The functor $f \vee g$ yields an assignation of $V$ and is defined as follows:

(Def. 36) $f \vee g = (\text{the disjunction of } V)(f, g)$.

Let $V$ be an LTL-model structure and let $f$ be an assignation of $V$. The functor $\mathcal{X} f$ yielding an assignation of $V$ is defined by:

(Def. 37) $\mathcal{X} f = (\text{the next-operation of } V)(f)$.

Let $V$ be an LTL-model structure and let $f$, $g$ be assignations of $V$. The functor $f \,\mathcal{U}\, g$ yielding an assignation of $V$ is defined by:

(Def. 38) $f \,\mathcal{U}\, g = (\text{the until-operation of } V)(f, g)$.

The functor $f \,\mathcal{R}\, g$ yields an assignation of $V$ and is defined as follows:

(Def. 39) $f \,\mathcal{R}\, g = (\text{the release-operation of } V)(f, g)$.

One can prove the following propositions:

(50) $\mathrm{Evaluate}(\neg H, K_1) = \neg\,\mathrm{Evaluate}(H, K_1)$.

(51) $\mathrm{Evaluate}(H_1 \wedge H_2, K_1) = \mathrm{Evaluate}(H_1, K_1) \wedge \mathrm{Evaluate}(H_2, K_1)$.

(52) $\mathrm{Evaluate}(H_1 \vee H_2, K_1) = \mathrm{Evaluate}(H_1, K_1) \vee \mathrm{Evaluate}(H_2, K_1)$.

(53) $\mathrm{Evaluate}(\mathcal{X} H, K_1) = \mathcal{X}\,\mathrm{Evaluate}(H, K_1)$.

(54) $\mathrm{Evaluate}(H_1 \,\mathcal{U}\, H_2, K_1) = \mathrm{Evaluate}(H_1, K_1) \,\mathcal{U}\, \mathrm{Evaluate}(H_2, K_1)$.

(55) $\mathrm{Evaluate}(H_1 \,\mathcal{R}\, H_2, K_1) = \mathrm{Evaluate}(H_1, K_1) \,\mathcal{R}\, \mathrm{Evaluate}(H_2, K_1)$.

Let $S$ be a non empty set. The infinite sequences of $S$ yielding a non empty set is defined by:

(Def. 40) The infinite sequences of $S = S^{\mathbb{N}}$.

Let $S$ be a non empty set and let $t$ be a sequence of $S$. The functor $\mathrm{CastSeq}\, t$ yields an element of the infinite sequences of $S$ and is defined by:

(Def. 41) $\mathrm{CastSeq}\, t = t$.

Let $S$ be a non empty set and let $t$ be a set. Let us assume that $t$ is an element of the infinite sequences of $S$. The functor $\mathrm{CastSeq}(t, S)$ yielding a sequence of $S$ is defined by:

(Def. 42) $\mathrm{CastSeq}(t, S) = t$.

Let $S$ be a non empty set, let $t$ be a sequence of $S$, and let $k$ be a natural number. The functor $\mathrm{Shift}(t, k)$ yielding a sequence of $S$ is defined as follows:

(Def. 43) For every natural number $n$ holds $(\mathrm{Shift}(t, k))(n) = t(n + k)$.

Let $S$ be a non empty set, let $t$ be a set, and let $k$ be a natural number. The functor $\mathrm{Shift}(t, k, S)$ yielding an element of the infinite sequences of $S$ is defined as follows:

(Def. 44) $\mathrm{Shift}(t, k, S) = \mathrm{CastSeq}\,\mathrm{Shift}(\mathrm{CastSeq}(t, S), k)$.

Let $S$ be a non empty set, let $t$ be an element of the infinite sequences of $S$, and let $k$ be a natural number. The functor $\mathrm{Shift}(t, k)$ yielding an element of the infinite sequences of $S$ is defined as follows:

(Def. 45) $\mathrm{Shift}(t, k) = \mathrm{Shift}(t, k, S)$.

Let $S$ be a non empty set and let $f$ be a set. The functor $\mathrm{Not}_0(f, S)$ yields an element of ModelSP (the infinite sequences of $S$) and is defined by the condition (Def. 46).

(Def. 46) Let $t$ be a set. Suppose $t \in$ the infinite sequences of $S$. Then $\neg\,\mathrm{Castboolean}(\mathrm{Fid}(f, \text{the infinite sequences of } S))(t) = \mathit{true}$ if and only if $(\mathrm{Fid}(\mathrm{Not}_0(f, S), \text{the infinite sequences of } S))(t) = \mathit{true}$.

Let $S$ be a non empty set. The functor $\mathrm{Not}\, S$ yielding a unary operation on ModelSP (the infinite sequences of $S$) is defined by:

(Def. 47) For every set $f$ such that $f \in$ ModelSP (the infinite sequences of $S$) holds $(\mathrm{Not}\, S)(f) = \mathrm{Not}_0(f, S)$.

Let $S$ be a non empty set, let $f$ be a function from the infinite sequences of $S$ into *Boolean*, and let $t$ be a set. The functor $\text{Next-univ}(t, f)$ yields an element of *Boolean* and is defined as follows:

(Def. 48) $$\text{Next-univ}(t, f) = \begin{cases} \mathit{true}, & \text{if } t \text{ is an element of the infinite sequences} \\ & \quad \text{of } S \text{ and } f(\mathrm{Shift}(t, 1, S)) = \mathit{true}, \\ \mathit{false}, & \text{otherwise.} \end{cases}$$

Let $S$ be a non empty set and let $f$ be a set. The functor $\mathrm{Next}_0(f, S)$ yielding an element of ModelSP (the infinite sequences of $S$) is defined by the condition

(Def. 49).

(Def. 49) Let $t$ be a set. Suppose $t \in$ the infinite sequences of $S$. Then $\text{Next-univ}(t, \text{Fid}(f, \text{the infinite sequences of } S)) = \mathit{true}$ if and only if $(\text{Fid}(\text{Next}_0(f, S), \text{the infinite sequences of } S))(t) = \mathit{true}$.

Let $S$ be a non empty set. The functor $\text{Next}\, S$ yields a unary operation on ModelSP (the infinite sequences of $S$) and is defined as follows:

(Def. 50) For every set $f$ such that $f \in$ ModelSP (the infinite sequences of $S$) holds $(\text{Next}\, S)(f) = \text{Next}_0(f, S)$.

Let $S$ be a non empty set and let $f$, $g$ be sets. The functor $\text{And}_0(f, g, S)$ yields an element of ModelSP (the infinite sequences of $S$) and is defined by the condition (Def. 51).

(Def. 51) Let $t$ be a set. Suppose $t \in$ the infinite sequences of $S$. Then $\text{Castboolean}(\text{Fid}(f, \text{the infinite sequences of } S))(t) \wedge \text{Castboolean}(\text{Fid}(g, \text{the infinite sequences of } S))(t) = \mathit{true}$ if and only if $(\text{Fid}(\text{And}_0(f, g, S), \text{the infinite sequences of } S))(t) = \mathit{true}$.

Let $S$ be a non empty set. The functor $\text{And}\, S$ yielding a binary operation on ModelSP (the infinite sequences of $S$) is defined by the condition (Def. 52).

(Def. 52) Let $f$, $g$ be sets. Suppose $f \in$ ModelSP (the infinite sequences of $S$) and $g \in$ ModelSP (the infinite sequences of $S$). Then $(\text{And}\, S)(f, g) = \text{And}_0(f, g, S)$.

Let $S$ be a non empty set, let $f$, $g$ be functions from the infinite sequences of $S$ into *Boolean*, and let $t$ be a set. The functor $\text{Until-univ}(t, f, g, S)$ yields an element of *Boolean* and is defined as follows:

(Def. 53) $$\text{Until-univ}(t, f, g, S) = \begin{cases} \mathit{true}, & \text{if } t \text{ is an element of the infinite sequences of } S \text{ and there exists a natural number } m \text{ such that for every natural number } j \text{ such that } j < m \text{ holds } f(\text{Shift}(t, j, S)) = \mathit{true} \text{ and } g(\text{Shift}(t, m, S)) = \mathit{true}, \\ \mathit{false}, & \text{otherwise.} \end{cases}$$

Let $S$ be a non empty set and let $f$, $g$ be sets. The functor $\text{Until}_0(f, g, S)$ yields an element of ModelSP (the infinite sequences of $S$) and is defined by the condition (Def. 54).

(Def. 54) Let $t$ be a set. Suppose $t \in$ the infinite sequences of $S$. Then $\text{Until-univ}(t, \text{Fid}(f, \text{the infinite sequences of } S), \text{Fid}(g, \text{the infinite sequences of } S), S) = \mathit{true}$ if and only if $(\text{Fid}(\text{Until}_0(f, g, S), \text{the infinite sequences of } S))(t) = \mathit{true}$.

Let $S$ be a non empty set. The functor $\text{Until}\, S$ yielding a binary operation on ModelSP (the infinite sequences of $S$) is defined by the condition (Def. 55).

(Def. 55) Let $f$, $g$ be sets. Suppose $f \in$ ModelSP (the infinite sequences of $S$) and $g \in$ ModelSP (the infinite sequences of $S$). Then $(\text{Until}\, S)(f, g) =$

$\mathrm{Until}_0(f, g, S)$.

Let $S$ be a non empty set. The functor $\vee_S$ yields a binary operation on ModelSP (the infinite sequences of $S$) and is defined by the condition (Def. 56).

(Def. 56) Let $f$, $g$ be sets. Suppose $f \in$ ModelSP (the infinite sequences of $S$) and $g \in$ ModelSP (the infinite sequences of $S$). Then $\vee_S(f, g) = (\mathrm{Not}\, S)((\mathrm{And}\, S)((\mathrm{Not}\, S)(f), (\mathrm{Not}\, S)(g)))$.

The functor Release $S$ yields a binary operation on ModelSP (the infinite sequences of $S$) and is defined by the condition (Def. 57).

(Def. 57) Let $f$, $g$ be sets. Suppose $f \in$ ModelSP (the infinite sequences of $S$) and $g \in$ ModelSP (the infinite sequences of $S$). Then $(\mathrm{Release}\, S)(f, g) = (\mathrm{Not}\, S)((\mathrm{Until}\, S)((\mathrm{Not}\, S)(f), (\mathrm{Not}\, S)(g)))$.

Let $S$ be a non empty set and let $B_1$ be a non empty subset of ModelSP (the infinite sequences of $S$). The functor $\mathrm{Model}_{\mathrm{LTL}}(S, B_1)$ yields an LTL-model structure and is defined as follows:

(Def. 58) $\mathrm{Model}_{\mathrm{LTL}}(S, B_1) = \langle$ModelSP (the infinite sequences of $S$), $B_1, \mathrm{And}\, S, \vee_S, \mathrm{Not}\, S, \mathrm{Next}\, S, \mathrm{Until}\, S, \mathrm{Release}\, S\rangle$.

In the sequel $B_1$ denotes a non empty subset of ModelSP (the infinite sequences of $S$), $t$ denotes an element of the infinite sequences of $S$, and $f$, $g$ denote assignations of $\mathrm{Model}_{\mathrm{LTL}}(S, B_1)$.

Let $S$ be a non empty set, let $B_1$ be a non empty subset of ModelSP (the infinite sequences of $S$), let $t$ be an element of the infinite sequences of $S$, and let $f$ be an assignation of $\mathrm{Model}_{\mathrm{LTL}}(S, B_1)$. The predicate $t \models f$ is defined by:

(Def. 59) $(\mathrm{Fid}(f, \text{the infinite sequences of } S))(t) = \mathit{true}$.

Let $S$ be a non empty set, let $B_1$ be a non empty subset of ModelSP (the infinite sequences of $S$), let $t$ be an element of the infinite sequences of $S$, and let $f$ be an assignation of $\mathrm{Model}_{\mathrm{LTL}}(S, B_1)$. We introduce $t \not\models f$ as an antonym of $t \models f$.

The following propositions are true:

(56) $f \vee g = \neg(\neg f \wedge \neg g)$ and $f \,\mathcal{R}\, g = \neg(\neg f \,\mathcal{U}\, \neg g)$.

(57) $t \models \neg f$ iff $t \not\models f$.

(58) $t \models f \wedge g$ iff $t \models f$ and $t \models g$.

(59) $t \models \mathcal{X} f$ iff $\mathrm{Shift}(t, 1) \models f$.

(60) $t \models f \,\mathcal{U}\, g$ if and only if there exists a natural number $m$ such that for every natural number $j$ such that $j < m$ holds $\mathrm{Shift}(t, j) \models f$ and $\mathrm{Shift}(t, m) \models g$.

(61) $t \models f \vee g$ iff $t \models f$ or $t \models g$.

(62) $t \models f \,\mathcal{R}\, g$ if and only if for every natural number $m$ such that for every natural number $j$ such that $j < m$ holds $\mathrm{Shift}(t, j) \models \neg f$ holds $\mathrm{Shift}(t, m) \models g$.

The non empty set AtomicFamily is defined as follows:

(Def. 60) AtomicFamily $= 2^{\mathrm{atomic}_{\mathrm{LTL}}}$.

Let $a$, $t$ be sets. The functor AtomicFunc$(a, t)$ yielding an element of *Boolean* is defined as follows:

(Def. 61) $\mathrm{AtomicFunc}(a, t) = \begin{cases} \mathit{true}, & \text{if } t \in \text{the infinite sequences of AtomicFamily} \\ & \text{and } a \in (\mathrm{CastSeq}(t, \mathrm{AtomicFamily}))(0), \\ \mathit{false}, & \text{otherwise.} \end{cases}$

Let $a$ be a set. The functor AtomicAsgn $a$ yields an element of ModelSP (the infinite sequences of AtomicFamily) and is defined by:

(Def. 62) For every set $t$ such that $t \in$ the infinite sequences of AtomicFamily holds (Fid(AtomicAsgn $a$, the infinite sequences of AtomicFamily))$(t) =$ AtomicFunc$(a, t)$.

The non empty subset AtomicBasicAsgn of ModelSP (the infinite sequences of AtomicFamily) is defined by:

(Def. 63) AtomicBasicAsgn $= \{x \in$ ModelSP (the infinite sequences of AtomicFamily): $\bigvee_{a\,:\,\mathrm{set}}\ x =$ AtomicAsgn $a\}$.

The function AtomicKai from $\mathrm{atomic}_{\mathrm{LTL}}$ into the basic assignations of $\mathrm{Model}_{\mathrm{LTL}}$(AtomicFamily, AtomicBasicAsgn) is defined as follows:

(Def. 64) For every set $a$ such that $a \in \mathrm{atomic}_{\mathrm{LTL}}$ holds (AtomicKai)$(a) =$ AtomicAsgn $a$.

Let $r$ be an element of the infinite sequences of AtomicFamily and let $H$ be an LTL-formula. The predicate $r \models H$ is defined by:

(Def. 65) $r \models$ Evaluate$(H$, AtomicKai$)$.

Let $r$ be an element of the infinite sequences of AtomicFamily and let $H$ be an LTL-formula. We introduce $r \not\models H$ as an antonym of $r \models H$.

Let $r$ be an element of the infinite sequences of AtomicFamily and let $W$ be a subset of $\mathrm{WFF}_{\mathrm{LTL}}$. The predicate $r \models W$ is defined by:

(Def. 66) For every LTL-formula $H$ such that $H \in W$ holds $r \models H$.

Let $r$ be an element of the infinite sequences of AtomicFamily and let $W$ be a subset of $\mathrm{WFF}_{\mathrm{LTL}}$. We introduce $r \not\models W$ as an antonym of $r \models W$.

Let $W$ be a subset of $\mathrm{WFF}_{\mathrm{LTL}}$. The functor $\mathcal{X}\,W$ yielding a subset of $\mathrm{WFF}_{\mathrm{LTL}}$ is defined as follows:

(Def. 67) $\mathcal{X}\,W = \{x; x$ ranges over LTL-formulae: $\bigvee_{u\,:\,\text{LTL-formula}}\ (u \in W \ \wedge\ x = \mathcal{X}\,u)\}$.

In the sequel $r$ denotes an element of the infinite sequences of AtomicFamily.

We now state a number of propositions:

(63) If $H$ is atomic, then $r \models H$ iff $H \in (\mathrm{CastSeq}(r, \mathrm{AtomicFamily}))(0)$.

(64) $r \models \neg H$ iff $r \not\models H$.

(65) $r \models H_1 \wedge H_2$ iff $r \models H_1$ and $r \models H_2$.

(66) $r \models H_1 \vee H_2$ iff $r \models H_1$ or $r \models H_2$.

(67) $r \models \mathcal{X}\, H$ iff $\mathrm{Shift}(r, 1) \models H$.

(68) $r \models H_1 \,\mathcal{U}\, H_2$ if and only if there exists a natural number $m$ such that for every natural number $j$ such that $j < m$ holds $\mathrm{Shift}(r, j) \models H_1$ and $\mathrm{Shift}(r, m) \models H_2$.

(69) $r \models H_1 \,\mathcal{R}\, H_2$ if and only if for every natural number $m$ such that for every natural number $j$ such that $j < m$ holds $\mathrm{Shift}(r, j) \models \neg H_1$ holds $\mathrm{Shift}(r, m) \models H_2$.

(70) $r \models \neg(H_1 \vee H_2)$ iff $r \models \neg H_1 \wedge \neg H_2$.

(71) $r \models \neg(H_1 \wedge H_2)$ iff $r \models \neg H_1 \vee \neg H_2$.

(72) $r \models H_1 \,\mathcal{R}\, H_2$ iff $r \models \neg(\neg H_1 \,\mathcal{U}\, \neg H_2)$.

(73) $r \not\models \neg H$ iff $r \models H$.

(74) $r \models \mathcal{X}\, \neg H$ iff $r \models \neg\, \mathcal{X}\, H$.

(75) $r \models H_1 \,\mathcal{U}\, H_2$ iff $r \models H_2 \vee H_1 \wedge \mathcal{X}(H_1 \,\mathcal{U}\, H_2)$.

(76) $r \models H_1 \,\mathcal{R}\, H_2$ iff $r \models H_1 \wedge H_2 \vee H_2 \wedge \mathcal{X}(H_1 \,\mathcal{R}\, H_2)$.

In the sequel $W$ is a subset of $\mathrm{WFF}_{\mathrm{LTL}}$.

One can prove the following propositions:

(77) $r \models \mathcal{X}\, W$ iff $\mathrm{Shift}(r, 1) \models W$.

(78)(i) If $H$ is atomic, then $H$ is not negative and $H$ is not conjunctive and $H$ is not disjunctive and $H$ does not have *next* operator and $H$ does not have *until* operator and $H$ does not have *release* operator,

(ii) if $H$ is negative, then $H$ is not atomic and $H$ is not conjunctive and $H$ is not disjunctive and $H$ does not have *next* operator and $H$ does not have *until* operator and $H$ does not have *release* operator,

(iii) if $H$ is conjunctive, then $H$ is not atomic and $H$ is not negative and $H$ is not disjunctive and $H$ does not have *next* operator and $H$ does not have *until* operator and $H$ does not have *release* operator,

(iv) if $H$ is disjunctive, then $H$ is not atomic and $H$ is not negative and $H$ is not conjunctive and $H$ does not have *next* operator and $H$ does not have *until* operator and $H$ does not have *release* operator,

(v) if $H$ has *next* operator, then $H$ is not atomic and $H$ is not negative and $H$ is not conjunctive and $H$ is not disjunctive and $H$ does not have *until* operator and $H$ does not have *release* operator,

(vi) if $H$ has *until* operator, then $H$ is not atomic and $H$ is not negative and $H$ is not conjunctive and $H$ is not disjunctive and $H$ does not have *next* operator and $H$ does not have *release* operator, and

(vii) if $H$ has *release* operator, then $H$ is not atomic and $H$ is not negative and $H$ is not conjunctive and $H$ is not disjunctive and $H$ does not have *next* operator and $H$ does not have *until* operator.

(79) For every element $t$ of the infinite sequences of $S$ holds $\mathrm{Shift}(t, 0) = t$.

(80) For every element $s_1$ of the infinite sequences of $S$ holds $\mathrm{Shift}(\mathrm{Shift}(s_1, k), n) = \mathrm{Shift}(s_1, n + k)$.

(81) For every sequence $s_1$ of $S$ holds $\mathrm{CastSeq}(\mathrm{CastSeq}\, s_1, S) = s_1$.

(82) For every element $s_1$ of the infinite sequences of $S$ holds $\mathrm{CastSeq}\,\mathrm{CastSeq}(s_1, S) = s_1$.

(83) If $H$, $\neg H \in W$, then $r \not\models W$.

## References


[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek. A model of ZF set theory language. *Formalized Mathematics*, 1(**1**):131–145, 1990.
[3] Grzegorz Bancerek. Models and satisfiability. *Formalized Mathematics*, 1(**1**):191–199, 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. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[9] E. M. Clarke, O. Grumberg, and D. Peled. *Model Checking*. MIT Press, 2000.
[10] Kazuhisa Ishida. Model checking. Part I. *Formalized Mathematics*, 14(**4**):171–186, 2006.
[11] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[12] Edmund Woronowicz. Many–argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.


*Received April 21, 2008*

FORMALIZED MATHEMATICS
Vol. **16**, No. **3**, Pages 247–252, **2008**

# Modular Integer Arithmetic[1]

Christoph Schwarzweller
Institute of Computer Science
University of Gdańsk
Wita Stwosza 57, 80-952 Gdańsk, Poland

**Summary.** In this article we show the correctness of integer arithmetic based on Chinese Remainder theorem as described e.g. in [11]: Integers are transformed to finite sequences of modular integers, on which the arithmetic operations are performed. Retransformation of the results to the integers is then accomplished by means of the Chinese Remainder theorem. The method presented is a typical example for computing in homomorphic images.

MML identifier: `INT_6`, version: `7.9.01 4.103.1019`

The terminology and notation used here are introduced in the following articles: [10], [9], [8], [2], [7], [5], [4], [3], [6], and [1].

## 1. Preliminaries

Let $f$ be a finite sequence. Note that $f{\restriction}0$ is empty.

Let $f$ be a complex-valued finite sequence and let $n$ be a natural number. Observe that $f{\restriction}n$ is complex-valued.

Let $f$ be an integer-valued finite sequence and let $n$ be a natural number. Note that $f{\restriction}n$ is integer-valued.

Let $f$ be an integer-valued finite sequence and let $n$ be a natural number. Observe that $f_{\lfloor n}$ is integer-valued.

Let $i$ be an integer. Observe that $\langle i \rangle$ is integer-valued.

Let $f$, $g$ be integer-valued finite sequences. Note that $f ^\frown g$ is integer-valued.

One can prove the following propositions:

[1]This work has been partially supported by grant BW 5100-5-0293-7.




ISSN 1426–2630(p), 1898-9934(e)

(1) For all complex-valued finite sequences $f_1$, $f_2$ holds $\operatorname{len}(f_1 + f_2) = \min(\operatorname{len} f_1, \operatorname{len} f_2)$.

(2) For all complex-valued finite sequences $f_1$, $f_2$ holds $\operatorname{len}(f_1 - f_2) = \min(\operatorname{len} f_1, \operatorname{len} f_2)$.

(3) For all complex-valued finite sequences $f_1$, $f_2$ holds $\operatorname{len}(f_1\, f_2) = \min(\operatorname{len} f_1, \operatorname{len} f_2)$.

(4) Let $m_1$, $m_2$ be complex-valued finite sequences. Suppose $\operatorname{len} m_1 = \operatorname{len} m_2$. Let $k$ be a natural number. If $k \leq \operatorname{len} m_1$, then $(m_1\, m_2){\restriction}k = (m_1{\restriction}k)\,(m_2{\restriction}k)$.

Let $F$ be an integer-valued finite sequence. Note that $\sum F$ is integer and $\prod F$ is integer.

Next we state several propositions:

(5) Let $f$ be a complex-valued finite sequence and $i$ be a natural number. If $i + 1 \leq \operatorname{len} f$, then $(f{\restriction}i) \frown \langle f(i+1) \rangle = f{\restriction}(i+1)$.

(6) For every complex-valued finite sequence $f$ such that there exists a natural number $i$ such that $i \in \operatorname{dom} f$ and $f(i) = 0$ holds $\prod f = 0$.

(7) For all integers $n$, $a$, $b$ holds $(a - b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n$.

(8) For all integers $i$, $j$, $k$ such that $i \mid j$ holds $k \cdot i \mid k \cdot j$.

(9) Let $m$ be an integer-valued finite sequence and $i$ be a natural number. If $i \in \operatorname{dom} m$ and $m_i \neq 0$, then $\frac{\prod m}{m_i}$ is an integer.

(10) Let $m$ be an integer-valued finite sequence and $i$ be a natural number. If $i \in \operatorname{dom} m$, then there exists an integer $z$ such that $z \cdot m_i = \prod m$.

(11) Let $m$ be an integer-valued finite sequence and $i$, $j$ be natural numbers. If $i, j \in \operatorname{dom} m$ and $j \neq i$ and $m_j \neq 0$, then $\frac{\prod m}{m_i \cdot m_j}$ is an integer.

(12) Let $m$ be an integer-valued finite sequence and $i$, $j$ be natural numbers. Suppose $i, j \in \operatorname{dom} m$ and $j \neq i$ and $m_j \neq 0$. Then there exists an integer $z$ such that $z \cdot m_i = \frac{\prod m}{m_j}$.

## 2. More on Greatest Common Divisors

Next we state a number of propositions:

(13) For every integer $i$ holds $|i| \mid i$ and $i \mid |i|$.

(14) For all integers $i$, $j$ holds $i \gcd j = i \gcd |j|$.

(15) For all integers $i$, $j$ such that $i$ and $j$ are relative prime holds $\operatorname{lcm}(i, j) = |i \cdot j|$.

(16) For all integers $i$, $j$, $k$ holds $i \cdot j \gcd i \cdot k = |i| \cdot (j \gcd k)$.

(17) For all integers $i$, $j$ holds $i \cdot j \gcd i = |i|$.

(18) For all integers $i$, $j$, $k$ holds $i \gcd j \gcd k = i \gcd j \gcd k$.

(19) For all integers $i$, $j$, $k$ such that $i$ and $j$ are relative prime holds $i \gcd j \cdot k = i \gcd k$.

(20) For all integers $i$, $j$ such that $i$ and $j$ are relative prime holds $i \cdot j \mid \mathrm{lcm}(i, j)$.

(21) For all integers $x$, $y$, $i$, $j$ such that $i$ and $j$ are relative prime holds if $x \equiv y \pmod{i}$ and $x \equiv y \pmod{j}$, then $x \equiv y \pmod{i \cdot j}$.

(22) For all integers $i$, $j$ such that $i$ and $j$ are relative prime there exists an integer $s$ such that $s \cdot i \equiv 1 \pmod{j}$.

## 3. Chinese Remainder Sequences

Let $f$ be an integer-valued finite sequence. We introduce $f$ is multiplicative-trivial as an antonym of $f$ is non-empty.

Let $f$ be an integer-valued finite sequence. Let us observe that $f$ is multiplicative-trivial if and only if:

(Def. 1) There exists a natural number $i$ such that $i \in \mathrm{dom}\, f$ and $f_i = 0$.

One can verify the following observations:

* there exists an integer-valued finite sequence which is multiplicative-trivial,
* there exists an integer-valued finite sequence which is non multiplicative-trivial, and
* there exists an integer-valued finite sequence which is non empty and positive yielding.

The following proposition is true

(23) For every multiplicative-trivial integer-valued finite sequence $m$ holds $\prod m = 0$.

Let $f$ be an integer-valued finite sequence. We say that $f$ is Chinese remainder if and only if:

(Def. 2) For all natural numbers $i$, $j$ such that $i$, $j \in \mathrm{dom}\, f$ and $i \neq j$ holds $f_i$ and $f_j$ are relative prime.

One can verify that there exists an integer-valued finite sequence which is non empty, positive yielding, and Chinese remainder.

A CR-sequence is a non empty positive yielding Chinese remainder integer-valued finite sequence.

Let us note that every CR-sequence is non multiplicative-trivial.

One can verify that every integer-valued finite sequence which is multiplicative-trivial is also non empty.

We now state the proposition

(24) For every CR-sequence $f$ and for every natural number $m$ such that $0 < m \leq \operatorname{len} f$ holds $f \restriction m$ is a CR-sequence.

Let $m$ be a CR-sequence. Observe that $\prod m$ is positive and natural.

Next we state the proposition

(25) Let $m$ be a CR-sequence and $i$ be a natural number. If $i \in \operatorname{dom} m$, then for every integer $m_3$ such that $m_3 = \frac{\prod m}{m_i}$ holds

## 4. Integer Arithmetic based on CRT

let $u$ be an integer and let $m$ be an integer-valued finite sequence. The functor $\operatorname{mod}(u, m)$ yields a finite sequence and is defined as follows:

(Def. 3) $\operatorname{len} \operatorname{mod}(u, m) = \operatorname{len} m$ and for every natural number $i$ such that $i \in \operatorname{dom} \operatorname{mod}(u, m)$ holds $(\operatorname{mod}(u, m))_i = u \bmod m_i$.

Let $u$ be an integer and let $m$ be an integer-valued finite sequence. Observe that $\operatorname{mod}(u, m)$ is integer-valued.

Let $m$ be a CR-sequence. A finite sequence is called a CR-coefficient sequence for $m$ if it satisfies the conditions (Def. 4).

(Def. 4)(i) $\operatorname{len} \mathrm{it} = \operatorname{len} m$, and

(ii) for every natural number $i$ such that $i \in \operatorname{dom} \mathrm{it}$ there exists an integer $s$ and there exists an integer $m_3$ such that $m_3 = \frac{\prod m}{m_i}$ and $s \cdot m_3 \equiv 1 \pmod{m_i}$ and $\mathrm{it}_i = s \cdot \frac{\prod m}{m_i}$.

Let $m$ be a CR-sequence. Note that every CR-coefficient sequence for $m$ is integer-valued.

Next we state several propositions:

(26) Let $m$ be a CR-sequence, $c$ be a CR-coefficient sequence for $m$, and $i$ be a natural number. If $i \in \operatorname{dom} c$, then $c_i \equiv 1 \pmod{m_i}$.

(27) Let $m$ be a CR-sequence, $c$ be a CR-coefficient sequence for $m$, and $i$, $j$ be natural numbers. If $i$, $j \in \operatorname{dom} c$ and $i \neq j$, then $c_i \equiv 0 \pmod{m_j}$.

(28) Let $m$ be a CR-sequence, $c_1$, $c_2$ be CR-coefficient sequences for $m$, and $i$ be a natural number. If $i \in \operatorname{dom} c_1$, then $(c_1)_i \equiv (c_2)_i \pmod{m_i}$.

(29) Let $u$ be an integer-valued finite sequence and $m$ be a CR-sequence. Suppose $\operatorname{len} m = \operatorname{len} u$. Let $c$ be a CR-coefficient sequence for $m$ and $i$ be a natural number. If $i \in \operatorname{dom} m$, then $\sum u\, c \equiv u_i \pmod{m_i}$.

(30) Let $u$ be an integer-valued finite sequence and $m$ be a CR-sequence. Suppose $\operatorname{len} m = \operatorname{len} u$. Let $c_1$, $c_2$ be CR-coefficient sequences for $m$. Then $\sum u\, c_1 \equiv \sum u\, c_2 \pmod{\prod m}$.

Let $u$ be an integer-valued finite sequence and let $m$ be a CR-sequence. Let us assume that $\operatorname{len} m = \operatorname{len} u$. The functor $\mathbb{Z}(u, m)$ yields an integer and is defined as follows:

(Def. 5) For every CR-coefficient sequence $c$ for $m$ holds $\mathbb{Z}(u,m) = (\sum u\,c) \bmod \prod m$.

We now state a number of propositions:

(31) For every integer-valued finite sequence $u$ and for every CR-sequence $m$ such that $\operatorname{len} m = \operatorname{len} u$ holds $0 \leq \mathbb{Z}(u,m) < \prod m$.

(32) For every integer $u$ and for every CR-sequence $m$ and for every natural number $i$ such that $i \in \operatorname{dom} m$ holds $u \equiv (\operatorname{mod}(u,m))_i \pmod{m_i}$.

(33) Let $u$, $v$ be integers, $m$ be a CR-sequence, and $i$ be a natural number. If $i \in \operatorname{dom} m$, then $(\operatorname{mod}(u,m) + \operatorname{mod}(v,m))_i \equiv u + v \pmod{m_i}$.

(34) Let $u$, $v$ be integers, $m$ be a CR-sequence, and $i$ be a natural number. If $i \in \operatorname{dom} m$, then $(\operatorname{mod}(u,m)\ \operatorname{mod}(v,m))_i \equiv u \cdot v \pmod{m_i}$.

(35) Let $u$, $v$ be integers, $m$ be a CR-sequence, and $i$ be a natural number. If $i \in \operatorname{dom} m$, then $\mathbb{Z}(\operatorname{mod}(u,m) + \operatorname{mod}(v,m), m) \equiv u + v \pmod{m_i}$.

(36) Let $u$, $v$ be integers, $m$ be a CR-sequence, and $i$ be a natural number. If $i \in \operatorname{dom} m$, then $\mathbb{Z}(\operatorname{mod}(u,m) - \operatorname{mod}(v,m), m) \equiv u - v \pmod{m_i}$.

(37) Let $u$, $v$ be integers, $m$ be a CR-sequence, and $i$ be a natural number. If $i \in \operatorname{dom} m$, then $\mathbb{Z}(\operatorname{mod}(u,m)\ \operatorname{mod}(v,m), m) \equiv u \cdot v \pmod{m_i}$.

(38) For all integers $u$, $v$ and for every CR-sequence $m$ such that $0 \leq u + v < \prod m$ holds $\mathbb{Z}(\operatorname{mod}(u,m) + \operatorname{mod}(v,m), m) = u + v$.

(39) For all integers $u$, $v$ and for every CR-sequence $m$ such that $0 \leq u - v < \prod m$ holds $\mathbb{Z}(\operatorname{mod}(u,m) - \operatorname{mod}(v,m), m) = u - v$.

(40) For all integers $u$, $v$ and for every CR-sequence $m$ such that $0 \leq u \cdot v < \prod m$ holds $\mathbb{Z}(\operatorname{mod}(u,m)\ \operatorname{mod}(v,m), m) = u \cdot v$.

## 5. Chinese Remainder Theorem Revisited

We now state two propositions:

(41) Let $u$ be an integer-valued finite sequence and $m$ be a CR-sequence. Suppose $\operatorname{len} u = \operatorname{len} m$. Then there exists an integer $z$ such that $0 \leq z < \prod m$ and for every natural number $i$ such that $i \in \operatorname{dom} u$ holds $z \equiv u_i \pmod{m_i}$.

(42) Let $u$ be an integer-valued finite sequence, $m$ be a CR-sequence, and $z_1$, $z_2$ be integers. Suppose that

(i) $0 \leq z_1$,

(ii) $z_1 < \prod m$,

(iii) for every natural number $i$ such that $i \in \operatorname{dom} m$ holds $z_1 \equiv u_i \pmod{m_i}$,

(iv) $0 \leq z_2$,

(v) $z_2 < \prod m$, and

(vi) for every natural number $i$ such that $i \in \operatorname{dom} m$ holds $z_2 \equiv u_i \pmod{m_i}$.

Then $z_1 = z_2$.

## References


[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[6] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[7] Artur Korniłowicz. On the real valued functions. *Formalized Mathematics*, 13(**1**):181–187, 2005.
[8] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[9] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[10] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[11] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.


*Received May 13, 2008*

FORMALIZED MATHEMATICS
Vol. **16**, No. **3**, Pages 253–258, **2008**

# General Theory of Quasi-Commutative BCI-algebras

Tao Sun
Qingdao University of Science and Technology
China

Weibo Pan
Qingdao University of Science and Technology
China

Chenglong Wu
Qingdao University of Science and Technology
China

Xiquan Liang
Qingdao University of Science and Technology
China

**Summary.** It is known that commutative BCK-algebras form a variety, but BCK-algebras do not [4]. Therefore H. Yutani introduced the notion of quasi-commutative BCK-algebras. In this article we first present the notion and general theory of quasi-commutative BCI-algebras. Then we discuss the reduction of the type of quasi-commutative BCK-algebras and some special classes of quasi-commutative BCI-algebras.

MML identifier: `BCIALG_5`, version: `7.9.01 4.103.1019`

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

Let $X$ be a BCI-algebra, let $x$, $y$ be elements of $X$, and let $m$, $n$ be elements of $\mathbb{N}$. The functor Polynom$(m,n,x,y)$ yields an element of $X$ and is defined as follows:

(Def. 1) Polynom$(m,n,x,y) = ((x \setminus (x \setminus y))^{m+1} \setminus (y \setminus x))^n$.

We adopt the following convention: $X$ denotes a BCI-algebra, $x$, $y$, $z$ denote elements of $X$, and $i$, $j$, $k$, $l$, $m$, $n$ denote elements of $\mathbb{N}$.

One can prove the following propositions:

(1) If $x \leq y \leq z$, then $x \leq z$.

(2) If $x \leq y \leq x$, then $x = y$.




ISSN 1426–2630(p), 1898-9934(e)

(3) For every BCK-algebra $X$ and for all elements $x$, $y$ of $X$ holds $x \setminus y \leq x$ and $(x \setminus y)^{n+1} \leq (x \setminus y)^n$.

(4) For every BCK-algebra $X$ and for every element $x$ of $X$ holds $(0_X \setminus x)^n = 0_X$.

(5) For every BCK-algebra $X$ and for all elements $x$, $y$ of $X$ such that $m \geq n$ holds $(x \setminus y)^m \leq (x \setminus y)^n$.

(6) Let $X$ be a BCK-algebra and $x$, $y$ be elements of $X$. Suppose $m > n$ and $(x \setminus y)^n = (x \setminus y)^m$. Let $k$ be an element of $\mathbb{N}$. If $k \geq n$, then $(x \setminus y)^n = (x \setminus y)^k$.

(7) $\mathrm{Polynom}(0, 0, x, y) = x \setminus (x \setminus y)$.

(8) $\mathrm{Polynom}(m, n, x, y) = ((\mathrm{Polynom}(0, 0, x, y) \setminus (x \setminus y))^m \setminus (y \setminus x))^n$.

(9) $\mathrm{Polynom}(m + 1, n, x, y) = \mathrm{Polynom}(m, n, x, y) \setminus (x \setminus y)$.

(10) $\mathrm{Polynom}(m, n + 1, x, y) = \mathrm{Polynom}(m, n, x, y) \setminus (y \setminus x)$.

(11) $\mathrm{Polynom}(n + 1, n + 1, y, x) \leq \mathrm{Polynom}(n, n + 1, x, y)$.

(12) $\mathrm{Polynom}(n, n + 1, x, y) \leq \mathrm{Polynom}(n, n, y, x)$.

Let $X$ be a BCI-algebra. We say that $X$ is quasi-commutative if and only if:

(Def. 2) There exist elements $i$, $j$, $m$, $n$ of $\mathbb{N}$ such that for all elements $x$, $y$ of $X$ holds $\mathrm{Polynom}(i, j, x, y) = \mathrm{Polynom}(m, n, y, x)$.

Let us observe that BCI-EXAMPLE is quasi-commutative.

One can check that there exists a BCI-algebra which is quasi-commutative.

Let $i$, $j$, $m$, $n$ be elements of $\mathbb{N}$. A BCI-algebra is called a BCI-algebra commutating with $i$, $j$ and $m$, $n$ if:

(Def. 3) For all elements $x$, $y$ of it holds $\mathrm{Polynom}(i, j, x, y) = \mathrm{Polynom}(m, n, y, x)$.

One can prove the following propositions:

(13) $X$ is a BCI-algebra commutating with $i$, $j$ and $m$, $n$ if and only if $X$ is a BCI-algebra commutating with $m$, $n$ and $i$, $j$.

(14) Let $X$ be a BCI-algebra commutating with $i$, $j$ and $m$, $n$ and $k$ be an element of $\mathbb{N}$. Then $X$ is a BCI-algebra commutating with $i + k$, $j$ and $m$, $n + k$.

(15) Let $X$ be a BCI-algebra commutating with $i$, $j$ and $m$, $n$ and $k$ be an element of $\mathbb{N}$. Then $X$ is a BCI-algebra commutating with $i$, $j + k$ and $m + k$, $n$.

One can verify that there exists a BCK-algebra which is quasi-commutative.

Let $i$, $j$, $m$, $n$ be elements of $\mathbb{N}$. One can check that there exists a BCI-algebra commutating with $i$, $j$ and $m$, $n$ which is BCK-5.

Let $i$, $j$, $m$, $n$ be elements of $\mathbb{N}$. A BCK-algebra commutating with $i$, $j$ and $m$, $n$ is BCK-5 BCI-algebra commutating with $i$, $j$ and $m$, $n$.

One can prove the following propositions:

(16) $X$ is a BCK-algebra commutating with $i$, $j$ and $m$, $n$ if and only if $X$ is a BCK-algebra commutating with $m$, $n$ and $i$, $j$.

(17) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$ and $k$ be an element of $\mathbb{N}$. Then $X$ is a BCK-algebra commutating with $i + k$, $j$ and $m$, $n + k$.

(18) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$ and $k$ be an element of $\mathbb{N}$. Then $X$ is a BCK-algebra commutating with $i$, $j + k$ and $m + k$, $n$.

(19) For every BCK-algebra $X$ commutating with $i$, $j$ and $m$, $n$ and for all elements $x$, $y$ of $X$ holds $(x \setminus y)^{i+1} = (x \setminus y)^{n+1}$.

(20) For every BCK-algebra $X$ commutating with $i$, $j$ and $m$, $n$ and for all elements $x$, $y$ of $X$ holds $(x \setminus y)^{j+1} = (x \setminus y)^{m+1}$.

(21) Every BCK-algebra commutating with $i$, $j$ and $m$, $n$ is a BCK-algebra commutating with $i$, $j$ and $j$, $n$.

(22) Every BCK-algebra commutating with $i$, $j$ and $m$, $n$ is a BCK-algebra commutating with $n$, $j$ and $m$, $n$.

Let us consider $i$, $j$, $m$, $n$. The functor $\min(i, j, m, n)$ yielding an extended real number is defined as follows:

(Def. 4) $\min(i, j, m, n) = \min(\min(i, j), \min(m, n))$.

The functor $\max(i, j, m, n)$ yielding an extended real number is defined by:

(Def. 5) $\max(i, j, m, n) = \max(\max(i, j), \max(m, n))$.

Next we state a number of propositions:

(23) $\min(i, j, m, n) = i$ or $\min(i, j, m, n) = j$ or $\min(i, j, m, n) = m$ or $\min(i, j, m, n) = n$.

(24) $\max(i, j, m, n) = i$ or $\max(i, j, m, n) = j$ or $\max(i, j, m, n) = m$ or $\max(i, j, m, n) = n$.

(25) If $i = \min(i, j, m, n)$, then $i \leq j$ and $i \leq m$ and $i \leq n$.

(26) $\max(i, j, m, n) \geq i$ and $\max(i, j, m, n) \geq j$ and $\max(i, j, m, n) \geq m$ and $\max(i, j, m, n) \geq n$.

(27) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $i = \min(i, j, m, n)$. If $i = j$, then $X$ is a BCK-algebra commutating with $i$, $i$ and $i$, $i$.

(28) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $i = \min(i, j, m, n)$. Suppose $i < j$ and $i < n$. Then $X$ is a BCK-algebra commutating with $i$, $i + 1$ and $i$, $i + 1$.

(29) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $i = \min(i, j, m, n)$. Suppose $i < j$ and $i = n$ and $i = m$. Then $X$ is a BCK-algebra commutating with $i$, $i$ and $i$, $i$.

(30) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $i = \min(i, j, m, n)$. Suppose $i < j$ and $i = n$ and $i < m < j$. Then $X$ is a BCK-algebra commutating with $i$, $m + 1$ and $m$, $i$.

(31) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $i = \min(i, j, m, n)$. Suppose $i < j$ and $i = n$ and $j \leq m$. Then $X$ is a BCK-algebra commutating with $i$, $j$ and $j$, $i$.

(32) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $l \geq j$ and $k \geq n$. Then $X$ is a BCK-algebra commutating with $k$, $l$ and $l$, $k$.

(33) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $k \geq \max(i, j, m, n)$. Then $X$ is a BCK-algebra commutating with $k$, $k$ and $k$, $k$.

(34) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $i \leq m$ and $j \leq n$. Then $X$ is a BCK-algebra commutating with $i$, $j$ and $i$, $j$.

(35) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $i \leq m$ and $i < n$. Then $X$ is a BCK-algebra commutating with $i$, $j$ and $i$, $i + 1$.

(36) If $X$ is a BCI-algebra commutating with $i$, $j$ and $j + k$, $i + k$, then $X$ is a BCK-algebra.

(37) $X$ is a BCI-algebra commutating with 0, 0 and 0, 0 if and only if $X$ is a BCK-algebra commutating with 0, 0 and 0, 0.

(38) $X$ is a commutative BCK-algebra iff $X$ is a BCI-algebra commutating with 0, 0 and 0, 0.

Let $X$ be a BCI-algebra. We introduce $p$-Semisimple-part $X$ as a synonym of AtomSet $X$.

In the sequel $B$, $P$ are non empty subsets of $X$.

One can prove the following propositions:

(39) For every BCI-algebra $X$ such that $B =$ BCK-part $X$ and $P =$ $p$-Semisimple-part $X$ holds $B \cap P = \{0_X\}$.

(40) For every BCI-algebra $X$ such that $P = p$-Semisimple-part $X$ holds $X$ is a BCK-algebra iff $P = \{0_X\}$.

(41) For every BCI-algebra $X$ such that $B =$ BCK-part $X$ holds $X$ is a $p$-semisimple BCI-algebra iff $B = \{0_X\}$.

(42) If $X$ is a $p$-semisimple BCI-algebra, then $X$ is a BCI-algebra commutating with 0, 1 and 0, 0.

(43) Suppose $X$ is a $p$-semisimple BCI-algebra. Then $X$ is a BCI-algebra commutating with $n + j$, $n$ and $m$, $m + j + 1$.

(44) Suppose $X$ is an associative BCI-algebra. Then $X$ is a BCI-algebra commutating with 0, 1 and 0, 0 and a BCI-algebra commutating with 1, 0 and 0, 0.

(45) Suppose $X$ is a weakly-positive-implicative BCI-algebra. Then $X$ is a BCI-algebra commutating with 0, 1 and 1, 1.

(46) If $X$ is a positive-implicative BCI-algebra, then $X$ is a BCI-algebra commutating with 0, 1 and 1, 1.

(47) If $X$ is an implicative BCI-algebra, then $X$ is a BCI-algebra commutating with 0, 1 and 0, 0.

(48) If $X$ is an alternative BCI-algebra, then $X$ is a BCI-algebra commutating with 0, 1 and 0, 0.

(49) $X$ is a BCK-positive-implicative BCK-algebra if and only if $X$ is a BCK-algebra commutating with 0, 1 and 0, 1.

(50) $X$ is a BCK-implicative BCK-algebra iff $X$ is a BCK-algebra commutating with 1, 0 and 0, 0.

One can check that every BCK-algebra which is BCK-implicative is also commutative and every BCK-algebra which is BCK-implicative is also BCK-positive-implicative.

The following propositions are true:

(51) $X$ is a BCK-algebra commutating with 1, 0 and 0, 0 if and only if $X$ is a BCK-algebra commutating with 0, 0 and 0, 0 and a BCK-algebra commutating with 0, 1 and 0, 1.

(52) Let $X$ be a quasi-commutative BCK-algebra. Then $X$ is a BCK-algebra commutating with 0, 1 and 0, 1 if and only if for all elements $x$, $y$ of $X$ holds $x \setminus y = x \setminus y \setminus y$.

(53) Let $X$ be a quasi-commutative BCK-algebra. Then $X$ is a BCK-algebra commutating with $n$, $n + 1$ and $n$, $n + 1$ if and only if for all elements $x$, $y$ of $X$ holds $(x \setminus y)^{n+1} = (x \setminus y)^{n+2}$.

(54) If $X$ is a BCI-algebra commutating with 0, 1 and 0, 0, then $X$ is a BCI-commutative BCI-algebra.

(55) If $X$ is a BCI-algebra commutating with $n$, 0 and $m$, $m$, then $X$ is a BCI-commutative BCI-algebra.

(56) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $j = 0$ and $m > 0$. Then $X$ is a BCK-algebra commutating with 0, 0 and 0, 0.

(57) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $m = 0$ and $j > 0$. Then $X$ is a BCK-algebra commutating with 0, 1 and 0, 1.

(58) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $n = 0$ and $i \neq 0$. Then $X$ is a BCK-algebra commutating with 0, 0 and 0, 0.

(59) Let $X$ be a BCK-algebra commutating with $i$, $j$ and $m$, $n$. Suppose $i = 0$ and $n \neq 0$. Then $X$ is a BCK-algebra commutating with 0, 1 and 0, 1.

## References


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

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

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

[4] Jie Meng and YoungLin Liu. *An Introduction to BCI-algebras*. Shaanxi Scientific and Technological Press, 2001.

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

[6] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.

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


*Received May 13, 2008*

FORMALIZED MATHEMATICS
Vol. **16**, No. **3**, Pages 259–267, **2008**

# Block Diagonal Matrices

Karol Pąk
Institute of Computer Science
University of Białystok
Poland

**Summary.** In this paper I present basic properties of block diagonal matrices over a set. In my approach the finite sequence of matrices in a block diagonal matrix is not restricted to square matrices. Moreover, the off-diagonal blocks need not be zero matrices, but also with another arbitrary fixed value.

MML identifier: `MATRIXJ1`, version: `7.9.01 4.103.1019`

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

## 1. Preliminaries

For simplicity, we adopt the following rules: $i$, $j$, $m$, $n$, $k$ denote natural numbers, $x$ denotes a set, $K$ denotes a field, $a$, $a_1$, $a_2$ denote elements of $K$, $D$ denotes a non empty set, $d$, $d_1$, $d_2$ denote elements of $D$, $M$, $M_1$, $M_2$ denote matrices over $D$, $A$, $A_1$, $A_2$, $B_1$, $B_2$ denote matrices over $K$, and $f$, $g$ denote finite sequences of elements of $\mathbb{N}$.

One can prove the following propositions:

(1) Let $K$ be a non empty additive loop structure and $f_1$, $f_2$, $g_1$, $g_2$ be finite sequences of elements of $K$. If $\operatorname{len} f_1 = \operatorname{len} f_2$, then $(f_1 + f_2) ^\frown (g_1 + g_2) = f_1 ^\frown g_1 + f_2 ^\frown g_2$.

(2) For all finite sequences $f$, $g$ of elements of $D$ such that $i \in \operatorname{dom} f$ holds $(f ^\frown g)_{\restriction i} = (f_{\restriction i}) ^\frown g$.

(3) For all finite sequences $f$, $g$ of elements of $D$ such that $i \in \operatorname{dom} g$ holds $(f ^\frown g)_{\restriction i + \operatorname{len} f} = f ^\frown (g_{\restriction i})$.




ISSN 1426–2630(p), 1898-9934(e)

(4) If $i \in \mathrm{Seg}(n+1)$, then $((n+1) \mapsto d)_{\restriction i} = n \mapsto d$.

(5) $\prod(n \mapsto a) = \mathrm{power}_K(a, n)$.

Let us consider $f$ and let $i$ be a natural number. Let us assume that $i \in \mathrm{Seg}(\sum f)$. The functor $\min(f, i)$ yielding an element of $\mathbb{N}$ is defined by:

(Def. 1) $i \leq \sum f \restriction \min(f, i)$ and $\min(f, i) \in \mathrm{dom}\, f$ and for every $j$ such that $i \leq \sum f \restriction j$ holds $\min(f, i) \leq j$.

One can prove the following propositions:

(6) If $i \in \mathrm{dom}\, f$ and $f(i) \neq 0$, then $\min(f, \sum f \restriction i) = i$.

(7) If $i \in \mathrm{Seg}(\sum f)$, then $\min(f, i) -' 1 = \min(f, i) - 1$ and $\sum f \restriction (\min(f, i) -' 1) < i$.

(8) If $i \in \mathrm{Seg}(\sum f)$, then $\min(f \frown g, i) = \min(f, i)$.

(9) If $i \in \mathrm{Seg}((\sum f) + \sum g) \setminus \mathrm{Seg}(\sum f)$, then $\min(f \frown g, i) = \min(g, i -' \sum f) + \mathrm{len}\, f$ and $i -' \sum f = i - \sum f$.

(10) If $i \in \mathrm{dom}\, f$ and $j \in \mathrm{Seg}(f_i)$, then $j + \sum f \restriction (i -' 1) \in \mathrm{Seg}(\sum f \restriction i)$ and $\min(f, j + \sum f \restriction (i -' 1)) = i$.

(11) For all $i$, $j$ such that $i \leq \mathrm{len}\, f$ and $j \leq \mathrm{len}\, f$ and $\sum f \restriction i = \sum f \restriction j$ and if $i \in \mathrm{dom}\, f$, then $f(i) \neq 0$ and if $j \in \mathrm{dom}\, f$, then $f(j) \neq 0$ holds $i = j$.

## 2. Finite Sequences of Matrices

Let us consider $D$ and let $F$ be a finite sequence of elements of $(D^*)^*$. We say that $F$ is matrix-yielding if and only if:

(Def. 2) For every $i$ such that $i \in \mathrm{dom}\, F$ holds $F(i)$ is a matrix over $D$.

Let us consider $D$. Observe that there exists a finite sequence of elements of $(D^*)^*$ which is matrix-yielding.

Let us consider $D$. A finite sequence of matrices over $D$ is a matrix-yielding finite sequence of elements of $(D^*)^*$.

Let us consider $K$. A finite sequence of matrices over $K$ is a matrix-yielding finite sequence of elements of ((the carrier of $K)^*)^*$.

We now state the proposition

(12) $\emptyset$ is a finite sequence of matrices over $D$.

We adopt the following rules: $F$, $F_1$, $F_2$ are finite sequences of matrices over $D$ and $G$, $G'$, $G_1$, $G_2$ are finite sequences of matrices over $K$.

Let us consider $D$, $F$, $x$. Then $F(x)$ is a matrix over $D$.

Let us consider $D$, $F_1$, $F_2$. Then $F_1 \frown F_2$ is a finite sequence of matrices over $D$.

Let us consider $D$, $M_1$. Then $\langle M_1 \rangle$ is a finite sequence of matrices over $D$. Let us consider $M_2$. Then $\langle M_1, M_2 \rangle$ is a finite sequence of matrices over $D$.

Let us consider $D$, $F$, $n$. Then $F{\restriction}n$ is a finite sequence of matrices over $D$. Then $F_{\downharpoonright n}$ is a finite sequence of matrices over $D$.

## 3. Sequences of Sizes of Matrices in a Finite Sequence

Let us consider $D$, $F$. The functor $\operatorname{Len} F$ yielding a finite sequence of elements of $\mathbb{N}$ is defined as follows:

(Def. 3) $\operatorname{dom} \operatorname{Len} F = \operatorname{dom} F$ and for every $i$ such that $i \in \operatorname{dom} \operatorname{Len} F$ holds $(\operatorname{Len} F)(i) = \operatorname{len} F(i)$.

The functor $\operatorname{Width} F$ yields a finite sequence of elements of $\mathbb{N}$ and is defined by:

(Def. 4) $\operatorname{dom} \operatorname{Width} F = \operatorname{dom} F$ and for every $i$ such that $i \in \operatorname{dom} \operatorname{Width} F$ holds $(\operatorname{Width} F)(i) = \operatorname{width} F(i)$.

Let us consider $D$, $F$. Then $\operatorname{Len} F$ is an element of $\mathbb{N}^{\operatorname{len} F}$. Then $\operatorname{Width} F$ is an element of $\mathbb{N}^{\operatorname{len} F}$.

The following propositions are true:

(13) If $\sum \operatorname{Len} F = 0$, then $\sum \operatorname{Width} F = 0$.

(14) $\operatorname{Len}(F_1 \frown F_2) = (\operatorname{Len} F_1) \frown \operatorname{Len} F_2$.

(15) $\operatorname{Len}\langle M \rangle = \langle \operatorname{len} M \rangle$.

(16) $\sum \operatorname{Len}\langle M_1, M_2 \rangle = \operatorname{len} M_1 + \operatorname{len} M_2$.

(17) $\operatorname{Len}(F_1{\restriction}n) = \operatorname{Len} F_1{\restriction}n$.

(18) $\operatorname{Width}(F_1 \frown F_2) = (\operatorname{Width} F_1) \frown \operatorname{Width} F_2$.

(19) $\operatorname{Width}\langle M \rangle = \langle \operatorname{width} M \rangle$.

(20) $\sum \operatorname{Width}\langle M_1, M_2 \rangle = \operatorname{width} M_1 + \operatorname{width} M_2$.

(21) $\operatorname{Width}(F_1{\restriction}n) = \operatorname{Width} F_1{\restriction}n$.

## 4. Block Diagonal Matrices

Let us consider $D$, let $d$ be an element of $D$, and let $F$ be a finite sequence of matrices over $D$. The $d$-block diagonal of $F$ is a matrix over $D$ and is defined by the conditions (Def. 5).

(Def. 5)(i) len (the $d$-block diagonal of $F$) $= \sum \operatorname{Len} F$,

(ii) width (the $d$-block diagonal of $F$) $= \sum \operatorname{Width} F$, and

(iii) for all $i$, $j$ such that $\langle i, j \rangle \in$ the indices of the $d$-block diagonal of $F$ holds if $j \leq \sum \operatorname{Width} F{\restriction}(\min(\operatorname{Len} F, i) -' 1)$ or $j > \sum \operatorname{Width} F{\restriction}\min(\operatorname{Len} F, i)$, then (the $d$-block diagonal of $F)_{i,j} = d$ and if $\sum \operatorname{Width} F{\restriction}(\min(\operatorname{Len} F, i) -' 1) < j \leq \sum \operatorname{Width} F{\restriction}\min(\operatorname{Len} F, i)$, then (the $d$-block diagonal of $F)_{i,j} = F(\min(\operatorname{Len} F, i))_{i -' \sum \operatorname{Len} F{\restriction}(\min(\operatorname{Len} F, i) -' 1),\, j -' \sum \operatorname{Width} F{\restriction}(\min(\operatorname{Len} F, i) -' 1)}$.

Let us consider $D$, let $d$ be an element of $D$, and let $F$ be a finite sequence of matrices over $D$. Then the $d$-block diagonal of $F$ is a matrix over $D$ of dimension $\sum \mathrm{Len}\, F \times \sum \mathrm{Width}\, F$.

Next we state a number of propositions:

(22) For every finite sequence $F$ of matrices over $D$ such that $F = \emptyset$ holds the $d$-block diagonal of $F = \emptyset$.

(23) Let $M$ be a matrix over $D$ of dimension $\sum \mathrm{Len}\langle M_1, M_2\rangle \times \sum \mathrm{Width}\langle M_1, M_2\rangle$. Then $M =$ the $d$-block diagonal of $\langle M_1, M_2\rangle$ if and only if for every $i$ holds if $i \in \mathrm{dom}\, M_1$, then $\mathrm{Line}(M, i) = \mathrm{Line}(M_1, i) \frown (\mathrm{width}\, M_2 \mapsto d)$ and if $i \in \mathrm{dom}\, M_2$, then $\mathrm{Line}(M, i + \mathrm{len}\, M_1) = (\mathrm{width}\, M_1 \mapsto d) \frown \mathrm{Line}(M_2, i)$.

(24) Let $M$ be a matrix over $D$ of dimension $\sum \mathrm{Len}\langle M_1, M_2\rangle \times \sum \mathrm{Width}\langle M_1, M_2\rangle$. Then $M =$ the $d$-block diagonal of $\langle M_1, M_2\rangle$ if and only if for every $i$ holds if $i \in \mathrm{Seg\,width}\, M_1$, then $M_{\square,i} = ((M_1)_{\square,i}) \frown (\mathrm{len}\, M_2 \mapsto d)$ and if $i \in \mathrm{Seg\,width}\, M_2$, then $M_{\square,i+\mathrm{width}\, M_1} = (\mathrm{len}\, M_1 \mapsto d) \frown ((M_2)_{\square,i})$.

(25) The indices of the $d_1$-block diagonal of $F_1$ is a subset of the indices of the $d_2$-block diagonal of $F_1 \frown F_2$.

(26) Suppose $\langle i, j\rangle \in$ the indices of the $d$-block diagonal of $F_1$. Then (the $d$-block diagonal of $F_1)_{i,j} =$ (the $d$-block diagonal of $F_1 \frown F_2)_{i,j}$.

(27) $\langle i, j\rangle \in$ the indices of the $d_1$-block diagonal of $F_2$ if and only if $i > 0$ and $j > 0$ and $\langle i + \sum \mathrm{Len}\, F_1, j + \sum \mathrm{Width}\, F_1\rangle \in$ the indices of the $d_2$-block diagonal of $F_1 \frown F_2$.

(28) Suppose $\langle i, j\rangle \in$ the indices of the $d$-block diagonal of $F_2$. Then (the $d$-block diagonal of $F_2)_{i,j} =$ (the $d$-block diagonal of $F_1 \frown F_2)_{i+\sum \mathrm{Len}\, F_1, j+\sum \mathrm{Width}\, F_1}$.

(29) Suppose $\langle i, j\rangle \in$ the indices of the $d$-block diagonal of $F_1 \frown F_2$ but $i \leq \sum \mathrm{Len}\, F_1$ and $j > \sum \mathrm{Width}\, F_1$ or $i > \sum \mathrm{Len}\, F_1$ and $j \leq \sum \mathrm{Width}\, F_1$. Then (the $d$-block diagonal of $F_1 \frown F_2)_{i,j} = d$.

(30) Let given $i$, $j$, $k$. Suppose $i \in \mathrm{dom}\, F$ and $\langle j, k\rangle \in$ the indices of $F(i)$. Then

(i) $\langle j + \sum \mathrm{Len}\, F{\restriction}(i -' 1), k + \sum \mathrm{Width}\, F{\restriction}(i -' 1)\rangle \in$ the indices of the $d$-block diagonal of $F$, and

(ii) $F(i)_{j,k} =$ (the $d$-block diagonal of $F)_{j+\sum \mathrm{Len}\, F\restriction(i-'1), k+\sum \mathrm{Width}\, F\restriction(i-'1)}$.

(31) If $i \in \mathrm{dom}\, F$, then $F(i) = \mathrm{Segm}($the $d$-block diagonal of $F$, $\mathrm{Seg}(\sum \mathrm{Len}\, F{\restriction}i) \setminus \mathrm{Seg}(\sum \mathrm{Len}\, F{\restriction}(i -' 1)), \mathrm{Seg}(\sum \mathrm{Width}\, F{\restriction}i) \setminus \mathrm{Seg}(\sum \mathrm{Width}\, F{\restriction}(i -' 1)))$.

(32) $M = \mathrm{Segm}($the $d$-block diagonal of $\langle M\rangle \frown F, \mathrm{Seg\,len}\, M, \mathrm{Seg\,width}\, M)$.

(33) $M = \mathrm{Segm}($the $d$-block diagonal of $F \frown \langle M\rangle, \mathrm{Seg}(\mathrm{len}\, M + \sum \mathrm{Len}\, F) \setminus \mathrm{Seg}(\sum \mathrm{Len}\, F), \mathrm{Seg}(\mathrm{width}\, M + \sum \mathrm{Width}\, F) \setminus \mathrm{Seg}(\sum \mathrm{Width}\, F))$.

(34) The $d$-block diagonal of $\langle M\rangle = M$.

(35) The $d$-block diagonal of $F_1 \frown F_2 =$ the $d$-block diagonal of $\langle$the $d$-block diagonal of $F_1\rangle \frown F_2$.

(36) The $d$-block diagonal of $F_1 \frown F_2 =$ the $d$-block diagonal of $F_1 \frown \langle$the $d$-block diagonal of $F_2\rangle$.

(37) If $i \in \mathrm{Seg}(\sum \mathrm{Len}\, F)$ and $m = \min(\mathrm{Len}\, F, i)$, then Line(the $d$-block diagonal of $F$, $i$) $= ((\sum \mathrm{Width}(F{\restriction}(m -' 1))) \mapsto d) \frown \mathrm{Line}(F(m), i -' \sum \mathrm{Len}(F{\restriction}(m -' 1))) \frown (((\sum \mathrm{Width}\, F) -' \sum \mathrm{Width}(F{\restriction}m)) \mapsto d)$.

(38) If $i \in \mathrm{Seg}(\sum \mathrm{Width}\, F)$ and $m = \min(\mathrm{Width}\, F, i)$, then (the $d$-block diagonal of $F)_{\square,i} = ((\sum \mathrm{Len}(F{\restriction}(m -' 1))) \mapsto d) \frown (F(m)_{\square,i-'\sum \mathrm{Width}(F{\restriction}(m-'1))}) \frown (((\sum \mathrm{Len}\, F) -' \sum \mathrm{Len}(F{\restriction}m)) \mapsto d)$.

(39) Let $M_1$, $M_2$, $N_1$, $N_2$ be matrices over $D$. Suppose $\mathrm{len}\, M_1 = \mathrm{len}\, N_1$ and $\mathrm{width}\, M_1 = \mathrm{width}\, N_1$ and $\mathrm{len}\, M_2 = \mathrm{len}\, N_2$ and $\mathrm{width}\, M_2 = \mathrm{width}\, N_2$ and the $d_1$-block diagonal of $\langle M_1, M_2\rangle =$ the $d_2$-block diagonal of $\langle N_1, N_2\rangle$. Then $M_1 = N_1$ and $M_2 = N_2$.

(40) Suppose $M = \emptyset$. Then

(i) the $d$-block diagonal of $F \frown \langle M\rangle =$ the $d$-block diagonal of $F$, and

(ii) the $d$-block diagonal of $\langle M\rangle \frown F =$ the $d$-block diagonal of $F$.

(41) Suppose $i \in \mathrm{dom}\, A$ and $\mathrm{width}\, A = \mathrm{width}$ (the deleting of $i$-row in $A$). Then the deleting of $i$-row in the $a$-block diagonal of $\langle A\rangle \frown G =$ the $a$-block diagonal of $\langle$the deleting of $i$-row in $A\rangle \frown G$.

(42) Suppose $i \in \mathrm{dom}\, A$ and $\mathrm{width}\, A = \mathrm{width}$ (the deleting of $i$-row in $A$). Then the deleting of $(\sum \mathrm{Len}\, G)+i$-row in the $a$-block diagonal of $G \frown \langle A\rangle =$ the $a$-block diagonal of $G \frown \langle$the deleting of $i$-row in $A\rangle$.

(43) Suppose $i \in \mathrm{Seg}\,\mathrm{width}\, A$. Then the deleting of $i$-column in the $a$-block diagonal of $\langle A\rangle \frown G =$ the $a$-block diagonal of $\langle$the deleting of $i$-column in $A\rangle \frown G$.

(44) Suppose $i \in \mathrm{Seg}\,\mathrm{width}\, A$. Then the deleting of $i + \sum \mathrm{Width}\, G$-column in the $a$-block diagonal of $G \frown \langle A\rangle =$ the $a$-block diagonal of $G \frown \langle$the deleting of $i$-column in $A\rangle$.

Let us consider $D$ and let $F$ be a finite sequence of elements of $(D^*)^*$. We say that $F$ is square-matrix-yielding if and only if:

(Def. 6) For every $i$ such that $i \in \mathrm{dom}\, F$ there exists $n$ such that $F(i)$ is a square matrix over $D$ of dimension $n$.

Let us consider $D$. One can verify that there exists a finite sequence of elements of $(D^*)^*$ which is square-matrix-yielding.

Let us consider $D$. Observe that every finite sequence of elements of $(D^*)^*$ which is square-matrix-yielding is also matrix-yielding.

Let us consider $D$. A finite sequence of square-matrices over $D$ is a square-matrix-yielding finite sequence of elements of $(D^*)^*$.

Let us consider $K$. A finite sequence of square-matrices over $K$ is a square-matrix-yielding finite sequence of elements of ((the carrier of $K)^*)^*$.

We use the following convention: $S$, $S_1$, $S_2$ denote finite sequences of square-matrices over $D$ and $R$, $R_1$, $R_2$ denote finite sequences of square-matrices over $K$.

One can prove the following proposition

(45) $\emptyset$ is a finite sequence of square-matrices over $D$.

Let us consider $D$, $S$, $x$. Then $S(x)$ is a square matrix over $D$ of dimension $\operatorname{len} S(x)$.

Let us consider $D$, $S_1$, $S_2$. Then $S_1 \frown S_2$ is a finite sequence of square-matrices over $D$.

Let us consider $D$, $n$ and let $M_1$ be a square matrix over $D$ of dimension $n$. Then $\langle M_1 \rangle$ is a finite sequence of square-matrices over $D$.

Let us consider $D$, $n$, $m$, let $M_1$ be a square matrix over $D$ of dimension $n$, and let $M_2$ be a square matrix over $D$ of dimension $m$. Then $\langle M_1, M_2 \rangle$ is a finite sequence of square-matrices over $D$.

Let us consider $D$, $S$, $n$. Then $S \restriction n$ is a finite sequence of square-matrices over $D$. Then $S_{\lfloor n}$ is a finite sequence of square-matrices over $D$.

The following proposition is true

(46) $\operatorname{Len} S = \operatorname{Width} S$.

Let us consider $D$, let $d$ be an element of $D$, and let $S$ be a finite sequence of square-matrices over $D$. Then the $d$-block diagonal of $S$ is a square matrix over $D$ of dimension $\sum \operatorname{Len} S$.

One can prove the following propositions:

(47) Let $A$ be a square matrix over $K$ of dimension $n$. Suppose $i \in \operatorname{dom} A$ and $j \in \operatorname{Seg} n$. Then the deleting of $i$-row and $j$-column in the $a$-block diagonal of $\langle A \rangle \frown R =$ the $a$-block diagonal of $\langle$the deleting of $i$-row and $j$-column in $A\rangle \frown R$.

(48) Let $A$ be a square matrix over $K$ of dimension $n$. Suppose $i \in \operatorname{dom} A$ and $j \in \operatorname{Seg} n$. Then the deleting of $i + \sum \operatorname{Len} R$-row and $j + \sum \operatorname{Len} R$-column in the $a$-block diagonal of $R \frown \langle A \rangle =$ the $a$-block diagonal of $R \frown \langle$the deleting of $i$-row and $j$-column in $A\rangle$.

Let us consider $K$, $R$. The functor $\operatorname{Det} R$ yielding a finite sequence of elements of $K$ is defined as follows:

(Def. 7) $\operatorname{dom} \operatorname{Det} R = \operatorname{dom} R$ and for every $i$ such that $i \in \operatorname{dom} \operatorname{Det} R$ holds $(\operatorname{Det} R)(i) = \operatorname{Det} R(i)$.

Let us consider $K$, $R$. Then $\operatorname{Det} R$ is an element of (the carrier of $K)^{\operatorname{len} R}$.

In the sequel $N$ denotes a square matrix over $K$ of dimension $n$ and $N_1$ denotes a square matrix over $K$ of dimension $m$.

The following propositions are true:

(49) $\mathrm{Det}\langle N\rangle = \langle \mathrm{Det}\,N\rangle$.

(50) $\mathrm{Det}(R_1 \frown R_2) = (\mathrm{Det}\,R_1) \frown \mathrm{Det}\,R_2$.

(51) $\mathrm{Det}(R{\restriction}n) = \mathrm{Det}\,R{\restriction}n$.

(52) Det (the $0_K$-block diagonal of $\langle N, N_1\rangle$) $= \mathrm{Det}\,N \cdot \mathrm{Det}\,N_1$.

(53) Det (the $0_K$-block diagonal of $R$) $= \prod \mathrm{Det}\,R$.

(54) If $\mathrm{len}\,A_1 \neq \mathrm{width}\,A_1$ and $N =$ the $0_K$-block diagonal of $\langle A_1, A_2\rangle$, then $\mathrm{Det}\,N = 0_K$.

(55) Suppose $\mathrm{Len}\,G \neq \mathrm{Width}\,G$. Let $M$ be a square matrix over $K$ of dimension $n$. If $M =$ the $0_K$-block diagonal of $G$, then $\mathrm{Det}\,M = 0_K$.

## 5. An Example of a Finite Sequence of Matrices

Let us consider $K$ and let $f$ be a finite sequence of elements of $\mathbb{N}$. The functor $I_K^{f\times f}$ yielding a finite sequence of square-matrices over $K$ is defined by:

(Def. 8) $\mathrm{dom}(I_K^{f\times f}) = \mathrm{dom}\,f$ and for every $i$ such that $i \in \mathrm{dom}(I_K^{f\times f})$ holds $I_K^{f\times f}(i) = I_K^{f(i)\times f(i)}$.

The following propositions are true:

(56) $\mathrm{Len}(I_K^{f\times f}) = f$ and $\mathrm{Width}(I_K^{f\times f}) = f$.

(57) For every element $i$ of $\mathbb{N}$ holds $I_K^{\langle i\rangle\times\langle i\rangle} = \langle I_K^{i\times i}\rangle$.

(58) $I_K^{(f\frown g)\times(f\frown g)} = (I_K^{f\times f}) \frown I_K^{g\times g}$.

(59) $I_K^{(f\restriction n)\times(f\restriction n)} = I_K^{f\times f}{\restriction}n$.

(60) The $0_K$-block diagonal of $\langle I_K^{i\times i}, I_K^{j\times j}\rangle = I_K^{(i+j)\times(i+j)}$.

(61) The $0_K$-block diagonal of $I_K^{f\times f} = I_K^{(\sum f)\times(\sum f)}$.

In the sequel $p$, $p_1$ are finite sequences of elements of $K$.

## 6. Operations on a Finite Sequence of Matrices

Let us consider $K$, $G$, $p$. The functor $p \bullet G$ yielding a finite sequence of matrices over $K$ is defined as follows:

(Def. 9) $\mathrm{dom}(p \bullet G) = \mathrm{dom}\,G$ and for every $i$ such that $i \in \mathrm{dom}(p \bullet G)$ holds $(p \bullet G)(i) = p_i \cdot G(i)$.

Let us consider $K$ and let us consider $R$, $p$. Then $p \bullet R$ is a finite sequence of square-matrices over $K$.

The following propositions are true:

(62) $\mathrm{Len}(p \bullet G) = \mathrm{Len}\,G$ and $\mathrm{Width}(p \bullet G) = \mathrm{Width}\,G$.

(63) $p \bullet \langle A\rangle = \langle p_1 \cdot A\rangle$.

(64) If $\mathrm{len}\,G = \mathrm{len}\,p$ and $\mathrm{len}\,G_1 \leq \mathrm{len}\,p_1$, then $p{\frown}p_1 \bullet G{\frown}G_1 = (p\bullet G){\frown}(p_1\bullet G_1)$.

(65) $a\cdot$the $a_1$-block diagonal of $G =$ the $(a\cdot a_1)$-block diagonal of $\operatorname{len} G \mapsto a \bullet G$.

Let us consider $K$ and let $G_1$, $G_2$ be finite sequences of matrices over $K$. The functor $G_1 \oplus G_2$ yields a finite sequence of matrices over $K$ and is defined by:

(Def. 10) $\operatorname{dom}(G_1 \oplus G_2) = \operatorname{dom} G_1$ and for every $i$ such that $i \in \operatorname{dom}(G_1 \oplus G_2)$ holds $(G_1 \oplus G_2)(i) = G_1(i) + G_2(i)$.

Let us consider $K$ and let us consider $R$, $G$. Then $R \oplus G$ is a finite sequence of square-matrices over $K$.

The following propositions are true:

(66) $\operatorname{Len}(G_1 \oplus G_2) = \operatorname{Len} G_1$ and $\operatorname{Width}(G_1 \oplus G_2) = \operatorname{Width} G_1$.

(67) If $\operatorname{len} G = \operatorname{len} G'$, then $G \frown G_1 \oplus G' \frown G_2 = (G \oplus G') \frown (G_1 \oplus G_2)$.

(68) $\langle A \rangle \oplus G = \langle A + G(1) \rangle$.

(69) $\langle A_1 \rangle \oplus \langle A_2 \rangle = \langle A_1 + A_2 \rangle$.

(70) $\langle A_1, B_1 \rangle \oplus \langle A_2, B_2 \rangle = \langle A_1 + A_2, B_1 + B_2 \rangle$.

(71) Suppose $\operatorname{len} A_1 = \operatorname{len} B_1$ and $\operatorname{len} A_2 = \operatorname{len} B_2$ and $\operatorname{width} A_1 = \operatorname{width} B_1$ and $\operatorname{width} A_2 = \operatorname{width} B_2$. Then (the $a_1$-block diagonal of $\langle A_1, A_2 \rangle$) $+$ (the $a_2$-block diagonal of $\langle B_1, B_2 \rangle$) $=$ the $(a_1 + a_2)$-block diagonal of $\langle A_1, A_2 \rangle \oplus \langle B_1, B_2 \rangle$.

(72) Suppose $\operatorname{Len} R_1 = \operatorname{Len} R_2$ and $\operatorname{Width} R_1 = \operatorname{Width} R_2$. Then (the $a_1$-block diagonal of $R_1$) $+$ (the $a_2$-block diagonal of $R_2$) $=$ the $(a_1 + a_2)$-block diagonal of $R_1 \oplus R_2$.

Let us consider $K$ and let $G_1$, $G_2$ be finite sequences of matrices over $K$. The functor $G_1\, G_2$ yielding a finite sequence of matrices over $K$ is defined by:

(Def. 11) $\operatorname{dom}(G_1\, G_2) = \operatorname{dom} G_1$ and for every $i$ such that $i \in \operatorname{dom}(G_1\, G_2)$ holds $(G_1\, G_2)(i) = G_1(i) \cdot G_2(i)$.

Next we state several propositions:

(73) If $\operatorname{Width} G_1 = \operatorname{Len} G_2$, then $\operatorname{Len}(G_1\, G_2) = \operatorname{Len} G_1$ and $\operatorname{Width}(G_1\, G_2) = \operatorname{Width} G_2$.

(74) If $\operatorname{len} G = \operatorname{len} G'$, then $(G \frown G_1)\,(G' \frown G_2) = (G\, G') \frown (G_1\, G_2)$.

(75) $\langle A \rangle\, G = \langle A \cdot G(1) \rangle$.

(76) $\langle A_1 \rangle\, \langle A_2 \rangle = \langle A_1 \cdot A_2 \rangle$.

(77) $\langle A_1, B_1 \rangle\, \langle A_2, B_2 \rangle = \langle A_1 \cdot A_2, B_1 \cdot B_2 \rangle$.

(78) Suppose $\operatorname{width} A_1 = \operatorname{len} B_1$ and $\operatorname{width} A_2 = \operatorname{len} B_2$. Then (the $0_K$-block diagonal of $\langle A_1, A_2 \rangle$) $\cdot$ (the $0_K$-block diagonal of $\langle B_1, B_2 \rangle$) $=$ the $0_K$-block diagonal of $\langle A_1, A_2 \rangle\, \langle B_1, B_2 \rangle$.

(79) If $\operatorname{Width} R_1 = \operatorname{Len} R_2$, then (the $0_K$-block diagonal of $R_1$) $\cdot$ (the $0_K$-block diagonal of $R_2$) $=$ the $0_K$-block diagonal of $R_1\, R_2$.

## References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.
[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[8] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.
[9] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Formalized Mathematics*, 2(**5**):711–717, 1991.
[10] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.
[11] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.
[12] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[13] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[14] Karol Pąk. Basic properties of the rank of matrices over a field. *Formalized Mathematics*, 15(**4**):199–211, 2007.
[15] Karol Pąk and Andrzej Trybulec. Laplace expansion. *Formalized Mathematics*, 15(**3**):143–150, 2007.
[16] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[17] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[18] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[20] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.
[21] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

*Received May 13, 2008*

FORMALIZED MATHEMATICS
Vol. **16**, No. **3**, Pages 269–275, **2008**

# Linear Map of Matrices

Karol Pąk
Institute of Computer Science
University of Białystok
Poland

**Summary.** The paper is concerned with a generalization of concepts introduced in [13], i.e. introduced are matrices of linear transformations over a finite-dimensional vector space. Introduced are linear transformations over a finite-dimensional vector space depending on a given matrix of the transformation. Finally, I prove that the rank of linear transformations over a finite-dimensional vector space is the same as the rank of the matrix of that transformation.

MML identifier: `MATRLIN2`, version: `7.9.03 4.104.1021`

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

## 1. Preliminaries

We adopt the following rules: $i$, $j$, $m$, $n$ are natural numbers, $K$ is a field, and $a$ is an element of $K$.

One can prove the following propositions:

(1) Let $V$ be a vector space over $K$, $W_1$, $W_2$, $W_{12}$ be subspaces of $V$, and $U_1$, $U_2$ be subspaces of $W_{12}$. If $U_1 = W_1$ and $U_2 = W_2$, then $W_1 \cap W_2 = U_1 \cap U_2$ and $W_1 + W_2 = U_1 + U_2$.

(2) Let $V$ be a vector space over $K$ and $W_1$, $W_2$ be subspaces of $V$. Suppose $W_1 \cap W_2 = \mathbf{0}_V$. Let $B_1$ be a linearly independent subset of $W_1$ and $B_2$ be a linearly independent subset of $W_2$. Then $B_1 \cup B_2$ is a linearly independent subset of $W_1 + W_2$.




ISSN 1426–2630(p), 1898-9934(e)

(3) Let $V$ be a vector space over $K$ and $W_1$, $W_2$ be subspaces of $V$. Suppose $W_1 \cap W_2 = \mathbf{0}_V$. Let $B_1$ be a basis of $W_1$ and $B_2$ be a basis of $W_2$. Then $B_1 \cup B_2$ is a basis of $W_1 + W_2$.

(4) For every finite dimensional vector space $V$ over $K$ holds every ordered basis of $\Omega_V$ is an ordered basis of $V$.

(5) Let $V_1$ be a vector space over $K$ and $A$ be a finite subset of $V_1$. If $\dim(\mathrm{Lin}(A)) = \mathrm{card}\, A$, then $A$ is linearly independent.

(6) For every vector space $V$ over $K$ and for every finite subset $A$ of $V$ holds $\dim(\mathrm{Lin}(A)) \leq \mathrm{card}\, A$.

## 2. More on the Product of Finite Sequence of Scalars and Vectors

For simplicity, we follow the rules: $V_1$, $V_2$, $V_3$ are finite dimensional vector spaces over $K$, $f$ is a function from $V_1$ into $V_2$, $b_1$, $b_1'$ are ordered bases of $V_1$, $B_1$ is a finite sequence of elements of $V_1$, $b_2$ is an ordered basis of $V_2$, $B_2$ is a finite sequence of elements of $V_2$, $B_3$ is a finite sequence of elements of $V_3$, $v_1$, $w_1$ are elements of $V_1$, $R$, $R_1$, $R_2$ are finite sequences of elements of $V_1$, and $p$, $p_1$, $p_2$ are finite sequences of elements of $K$.

We now state a number of propositions:

(7) $\mathrm{lmlt}(p_1 + p_2, R) = \mathrm{lmlt}(p_1, R) + \mathrm{lmlt}(p_2, R)$.

(8) $\mathrm{lmlt}(p, R_1 + R_2) = \mathrm{lmlt}(p, R_1) + \mathrm{lmlt}(p, R_2)$.

(9) If $\mathrm{len}\, p_1 = \mathrm{len}\, R_1$ and $\mathrm{len}\, p_2 = \mathrm{len}\, R_2$, then $\mathrm{lmlt}(p_1 ^\frown p_2, R_1 ^\frown R_2) = (\mathrm{lmlt}(p_1, R_1)) ^\frown \mathrm{lmlt}(p_2, R_2)$.

(10) If $\mathrm{len}\, R_1 = \mathrm{len}\, R_2$, then $\sum(R_1 + R_2) = (\sum R_1) + \sum R_2$.

(11) $\sum \mathrm{lmlt}(\mathrm{len}\, R \mapsto a, R) = a \cdot \sum R$.

(12) $\sum \mathrm{lmlt}(p, \mathrm{len}\, p \mapsto v_1) = (\sum p) \cdot v_1$.

(13) $\sum \mathrm{lmlt}(a \cdot p, R) = a \cdot \sum \mathrm{lmlt}(p, R)$.

(14) Let $B_1$ be a finite sequence of elements of $V_1$, $W_1$ be a subspace of $V_1$, and $B_2$ be a finite sequence of elements of $W_1$. If $B_1 = B_2$, then $\mathrm{lmlt}(p, B_1) = \mathrm{lmlt}(p, B_2)$.

(15) Let $B_1$ be a finite sequence of elements of $V_1$, $W_1$ be a subspace of $V_1$, and $B_2$ be a finite sequence of elements of $W_1$. If $B_1 = B_2$, then $\sum B_1 = \sum B_2$.

(16) If $i \in \mathrm{dom}\, R$, then $\sum \mathrm{lmlt}(\mathrm{Line}(I_K^{\mathrm{len}\, R \times \mathrm{len}\, R}, i), R) = R_i$.

## 3. More on the Decomposition of a Vector in a Basis

We now state a number of propositions:

(17) $v_1 + w_1 \rightarrow b_1 = (v_1 \rightarrow b_1) + (w_1 \rightarrow b_1)$.

(18) $a \cdot v_1 \to b_1 = a \cdot (v_1 \to b_1)$.

(19) If $i \in \operatorname{dom} b_1$, then $(b_1)_i \to b_1 = \operatorname{Line}(I_K^{\operatorname{len} b_1 \times \operatorname{len} b_1}, i)$.

(20) $0_{(V_1)} \to b_1 = \operatorname{len} b_1 \mapsto 0_K$.

(21) $\operatorname{len} b_1 = \dim(V_1)$.

(22)(i) $\operatorname{rng}(b_1 \restriction m)$ is a linearly independent subset of $V_1$, and

(ii) for every subset $A$ of $V_1$ such that $A = \operatorname{rng}(b_1 \restriction m)$ holds $b_1 \restriction m$ is an ordered basis of $\operatorname{Lin}(A)$.

(23)(i) $\operatorname{rng}((b_1)_{\lfloor m})$ is a linearly independent subset of $V_1$, and

(ii) for every subset $A$ of $V_1$ such that $A = \operatorname{rng}((b_1)_{\lfloor m})$ holds $(b_1)_{\lfloor m}$ is an ordered basis of $\operatorname{Lin}(A)$.

(24) Let $W_1$, $W_2$ be subspaces of $V_1$. Suppose $W_1 \cap W_2 = \mathbf{0}_{(V_1)}$. Let $b_1$ be an ordered basis of $W_1$, $b_2$ be an ordered basis of $W_2$, and $b$ be an ordered basis of $W_1 + W_2$. Suppose $b = b_1 \frown b_2$. Let $v$, $v_1$, $v_2$ be vectors of $W_1 + W_2$, $w_1$ be a vector of $W_1$, and $w_2$ be a vector of $W_2$. If $v = v_1 + v_2$ and $v_1 = w_1$ and $v_2 = w_2$, then $v \to b = (w_1 \to b_1) \frown (w_2 \to b_2)$.

(25) Let $W_1$ be a subspace of $V_1$. Suppose $W_1 = \Omega_{(V_1)}$. Let $w$ be a vector of $W_1$, $v$ be a vector of $V_1$, and $w_1$ be an ordered basis of $W_1$. If $v = w$ and $b_1 = w_1$, then $v \to b_1 = w \to w_1$.

(26) Let $W_1$, $W_2$ be subspaces of $V_1$. Suppose $W_1 \cap W_2 = \mathbf{0}_{(V_1)}$. Let $w_1$ be an ordered basis of $W_1$ and $w_2$ be an ordered basis of $W_2$. Then $w_1 \frown w_2$ is an ordered basis of $W_1 + W_2$.

## 4. Properties of Matrices of Linear Transformations

Let us consider $K$, $V_1$, $V_2$, $f$, $B_1$, $b_2$. Then $\operatorname{AutMt}(f, B_1, b_2)$ is a matrix over $K$ of dimension $\operatorname{len} B_1 \times \operatorname{len} b_2$.

Let $S$ be a 1-sorted structure and let $R$ be a binary relation. The functor $R \restriction S$ is defined as follows:

(Def. 1) $R \restriction S = R \restriction$the carrier of $S$.

The following proposition is true

(27) Let $f$ be a linear transformation from $V_1$ to $V_2$, $W_1$, $W_2$ be subspaces of $V_1$, and $U_1$, $U_2$ be subspaces of $V_2$. Suppose if $\dim(W_1) = 0$, then $\dim(U_1) = 0$ and if $\dim(W_2) = 0$, then $\dim(U_2) = 0$ and $V_2$ is the direct sum of $U_1$ and $U_2$. Let $f_1$ be a linear transformation from $W_1$ to $U_1$ and $f_2$ be a linear transformation from $W_2$ to $U_2$. Suppose $f_1 = f \restriction W_1$ and $f_2 = f \restriction W_2$. Let $w_1$ be an ordered basis of $W_1$, $w_2$ be an ordered basis of $W_2$, $u_1$ be an ordered basis of $U_1$, and $u_2$ be an ordered basis of $U_2$. Suppose $w_1 \frown w_2 = b_1$ and $u_1 \frown u_2 = b_2$. Then $\operatorname{AutMt}(f, b_1, b_2) =$ the $0_K$-block diagonal of $\langle \operatorname{AutMt}(f_1, w_1, u_1), \operatorname{AutMt}(f_2, w_2, u_2) \rangle$.

Let us consider $K$, $V_1$, $V_2$, let $f$ be a function from $V_1$ into $V_2$, let $B_1$ be a finite sequence of elements of $V_1$, and let $b_2$ be an ordered basis of $V_2$. Let us assume that $\operatorname{len} B_1 = \operatorname{len} b_2$. The functor $\operatorname{AutEqMt}(f, B_1, b_2)$ yielding a matrix over $K$ of dimension $\operatorname{len} B_1 \times \operatorname{len} B_1$ is defined by:

(Def. 2) $\operatorname{AutEqMt}(f, B_1, b_2) = \operatorname{AutMt}(f, B_1, b_2)$.

The following propositions are true:

(28) $\operatorname{AutMt}(\operatorname{id}_{(V_1)}, b_1, b_1) = I_K^{\operatorname{len} b_1 \times \operatorname{len} b_1}$.

(29) $\operatorname{AutEqMt}(\operatorname{id}_{(V_1)}, b_1, b_1')$ is invertible and $\operatorname{AutEqMt}(\operatorname{id}_{(V_1)}, b_1', b_1) = (\operatorname{AutEqMt}(\operatorname{id}_{(V_1)}, b_1, b_1'))^{\smile}$.

(30) If $\operatorname{len} p_1 = \operatorname{len} p_2$ and $\operatorname{len} p_1 = \operatorname{len} B_1$ and $\operatorname{len} p_1 > 0$ and $j \in \operatorname{dom} b_1$ and for every $i$ such that $i \in \operatorname{dom} p_2$ holds $p_2(i) = ((B_1)_i \rightarrow b_1)(j)$, then $p_1 \cdot p_2 = (\sum \operatorname{lmlt}(p_1, B_1) \rightarrow b_1)(j)$.

(31) If $\operatorname{len} b_1 > 0$ and $f$ is linear, then $\operatorname{LineVec2Mx}(v_1 \rightarrow b_1) \cdot \operatorname{AutMt}(f, b_1, b_2) = \operatorname{LineVec2Mx}(f(v_1) \rightarrow b_2)$.

## 5. Linear Transformations of Matrices

Let us consider $K$, $V_1$, $V_2$, $b_1$, $B_2$ and let $M$ be a matrix over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} B_2$. The functor $\operatorname{Mx2Tran}(M, b_1, B_2)$ yielding a function from $V_1$ into $V_2$ is defined by:

(Def. 3) For every vector $v$ of $V_1$ holds $(\operatorname{Mx2Tran}(M, b_1, B_2))(v) = \sum \operatorname{lmlt}(\operatorname{Line}(\operatorname{LineVec2Mx}(v \rightarrow b_1) \cdot M, 1), B_2)$.

Next we state two propositions:

(32) For every matrix $M$ over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} b_2$ such that $\operatorname{len} b_1 > 0$ holds $\operatorname{LineVec2Mx}((\operatorname{Mx2Tran}(M, b_1, b_2))(v_1) \rightarrow b_2) = \operatorname{LineVec2Mx}(v_1 \rightarrow b_1) \cdot M$.

(33) For every matrix $M$ over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} B_2$ such that $\operatorname{len} b_1 = 0$ holds $(\operatorname{Mx2Tran}(M, b_1, B_2))(v_1) = 0_{(V_2)}$.

Let us consider $K$, $V_1$, $V_2$, $b_1$, $B_2$ and let $M$ be a matrix over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} B_2$. Then $\operatorname{Mx2Tran}(M, b_1, B_2)$ is a linear transformation from $V_1$ to $V_2$.

Next we state three propositions:

(34) If $f$ is linear, then $\operatorname{Mx2Tran}(\operatorname{AutMt}(f, b_1, b_2), b_1, b_2) = f$.

(35) For all matrices $A$, $B$ over $K$ such that $i \in \operatorname{dom} A$ and $\operatorname{width} A = \operatorname{len} B$ holds $\operatorname{LineVec2Mx} \operatorname{Line}(A, i) \cdot B = \operatorname{LineVec2Mx} \operatorname{Line}(A \cdot B, i)$.

(36) For every matrix $M$ over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} b_2$ holds $\operatorname{AutMt}(\operatorname{Mx2Tran}(M, b_1, b_2), b_1, b_2) = M$.

Let us consider $n$, $m$, $K$, let $A$ be a matrix over $K$ of dimension $n \times m$, and let $B$ be a matrix over $K$. Then $A + B$ is a matrix over $K$ of dimension $n \times m$.

The following propositions are true:

(37) For all matrices $A$, $B$ over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} B_2$ holds $\mathrm{Mx2Tran}(A+B, b_1, B_2) = \mathrm{Mx2Tran}(A, b_1, B_2) + \mathrm{Mx2Tran}(B, b_1, B_2)$.

(38) For every matrix $A$ over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} B_2$ holds $a \cdot \mathrm{Mx2Tran}(A, b_1, B_2) = \mathrm{Mx2Tran}(a \cdot A, b_1, B_2)$.

(39) For all matrices $A$, $B$ over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} b_2$ such that $\mathrm{Mx2Tran}(A, b_1, b_2) = \mathrm{Mx2Tran}(B, b_1, b_2)$ holds $A = B$.

(40) Let $A$ be a matrix over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} b_2$ and $B$ be a matrix over $K$ of dimension $\operatorname{len} b_2 \times \operatorname{len} B_3$. Suppose width $A = \operatorname{len} B$. Let $A_1$ be a matrix over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} B_3$. If $A_1 = A \cdot B$, then $\mathrm{Mx2Tran}(A_1, b_1, B_3) = \mathrm{Mx2Tran}(B, b_2, B_3) \cdot \mathrm{Mx2Tran}(A, b_1, b_2)$.

(41) Let $A$ be a matrix over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} b_2$. Suppose $\operatorname{len} b_1 > 0$ and $\operatorname{len} b_2 > 0$. Then $v_1 \in \ker \mathrm{Mx2Tran}(A, b_1, b_2)$ if and only if $v_1 \rightarrow b_1 \in$ the space of solutions of $A^{\mathrm{T}}$.

(42) $V_1$ is trivial iff $\dim(V_1) = 0$.

(43) Let $V_1$, $V_2$ be vector spaces over $K$ and $f$ be a linear transformation from $V_1$ to $V_2$. Then $f$ is one-to-one if and only if $\ker f = \mathbf{0}_{(V_1)}$.

Let us consider $K$ and let $V_1$ be a vector space over $K$. Then $\mathrm{id}_{(V_1)}$ is a linear transformation from $V_1$ to $V_1$.

Let us consider $K$, let $V_1$, $V_2$ be vector spaces over $K$, and let $f$, $g$ be linear transformations from $V_1$ to $V_2$. Then $f + g$ is a linear transformation from $V_1$ to $V_2$.

Let us consider $K$, let $V_1$, $V_2$ be vector spaces over $K$, let $f$ be a linear transformation from $V_1$ to $V_2$, and let us consider $a$. Then $a \cdot f$ is a linear transformation from $V_1$ to $V_2$.

Let us consider $K$, let $V_1$, $V_2$, $V_3$ be vector spaces over $K$, let $f_3$ be a linear transformation from $V_1$ to $V_2$, and let $f_4$ be a linear transformation from $V_2$ to $V_3$. Then $f_4 \cdot f_3$ is a linear transformation from $V_1$ to $V_3$.

One can prove the following propositions:

(44) For every matrix $A$ over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} b_2$ such that $\operatorname{rk}(A) = \operatorname{len} b_1$ holds $\mathrm{Mx2Tran}(A, b_1, b_2)$ is one-to-one.

(45) $\mathrm{MX2FinS}(I_K^{n \times n})$ is an ordered basis of the $n$-dimension vector space over $K$.

(46) Let $M$ be an ordered basis of the $\operatorname{len} b_2$-dimension vector space over $K$. Suppose $M = \mathrm{MX2FinS}(I_K^{\operatorname{len} b_2 \times \operatorname{len} b_2})$. Let $v_1$ be a vector of the $\operatorname{len} b_2$-dimension vector space over $K$. Then $v_1 \rightarrow M = v_1$.

(47) Let $M$ be an ordered basis of the $\operatorname{len} b_2$-dimension vector space over $K$. Suppose $M = \mathrm{MX2FinS}(I_K^{\operatorname{len} b_2 \times \operatorname{len} b_2})$. Let $A$ be a matrix over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} M$. If $A = \mathrm{AutMt}(f, b_1, b_2)$ and $f$ is linear, then $(\mathrm{Mx2Tran}(A, b_1, M))(v_1) = f(v_1) \rightarrow b_2$.

Let $K$ be an add-associative right zeroed right complementable Abelian associative well unital distributive non empty double loop structure, let $V_1$, $V_2$ be Abelian add-associative right zeroed right complementable vector space-like non empty vector space structures over $K$, let $W$ be a subspace of $V_1$, and let $f$ be a function from $V_1$ into $V_2$. Then $f \restriction W$ is a function from $W$ into $V_2$.

Let $K$ be a field, let $V_1$, $V_2$ be vector spaces over $K$, let $W$ be a subspace of $V_1$, and let $f$ be a linear transformation from $V_1$ to $V_2$. Then $f \restriction W$ is a linear transformation from $W$ to $V_2$.

## 6. The Main Theorems

The following propositions are true:

(48) For every linear transformation $f$ from $V_1$ to $V_2$ holds $\operatorname{rank} f = \operatorname{rk}(\operatorname{AutMt}(f, b_1, b_2))$.

(49) For every matrix $M$ over $K$ of dimension $\operatorname{len} b_1 \times \operatorname{len} b_2$ holds $\operatorname{rank} \operatorname{Mx2Tran}(M, b_1, b_2) = \operatorname{rk}(M)$.

(50) For every linear transformation $f$ from $V_1$ to $V_2$ such that $\dim(V_1) = \dim(V_2)$ holds $\ker f$ is non trivial iff $\operatorname{Det} \operatorname{AutEqMt}(f, b_1, b_2) = 0_K$.

(51) Let $f$ be a linear transformation from $V_1$ to $V_2$ and $g$ be a linear transformation from $V_2$ to $V_3$. If $g \restriction \operatorname{im} f$ is one-to-one, then $\operatorname{rank}(g \cdot f) = \operatorname{rank} f$ and $\operatorname{nullity}(g \cdot f) = \operatorname{nullity} f$.

## References

[1] Jesse Alama. The rank+nullity theorem. *Formalized Mathematics*, 15(**3**):137–142, 2007.
[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 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 applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 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] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[10] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.
[11] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.
[12] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[13] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(**3**):339–345, 1996.
[14] Michał Muzalewski. Rings and modules – part II. *Formalized Mathematics*, 2(**4**):579–585, 1991.

[15] Karol Pąk. Basic properties of the rank of matrices over a field. *Formalized Mathematics*, 15(**4**):199–211, 2007.
[16] Karol Pąk. Block diagonal matrices. *Formalized Mathematics*, 16(**3**):259–267, 2008.
[17] Karol Pąk. Solutions of linear equations. *Formalized Mathematics*, 16(**1**):81–90, 2008.
[18] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 1990.
[19] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[20] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1(**5**):877–882, 1990.
[21] Wojciech A. Trybulec. Operations on subspaces in vector space. *Formalized Mathematics*, 1(**5**):871–876, 1990.
[22] Wojciech A. Trybulec. Subspaces and cosets of subspaces in vector space. *Formalized Mathematics*, 1(**5**):865–870, 1990.
[23] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[24] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[25] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[26] Xiaopeng Yue, Xiquan Liang, and Zhongpin Sun. Some properties of some special matrices. *Formalized Mathematics*, 13(**4**):541–547, 2005.
[27] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.
[28] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.
[29] Mariusz Żynel. The Steinitz theorem and the dimension of a vector space. *Formalized Mathematics*, 5(**3**):423–428, 1996.

*Received May 13, 2008*

FORMALIZED MATHEMATICS
Vol. **16**, No. **3**, Pages 277–282, **2008**

# Orthomodular Lattices

Elżbieta Mądra
Institute of Mathematics
University of Białystok
Akademicka 2, 15-267 Białystok
Poland

Adam Grabowski
Institute of Mathematics
University of Białystok
Akademicka 2, 15-267 Białystok
Poland

**Summary.** The main result of the article is the solution to the problem of short axiomatizations of orthomodular ortholattices. Based on EQP/Otter results [10], we gave a set of three equations which is equivalent to the classical, much longer equational basis of such a class. Also the basic example of the lattice which is not orthomodular, i.e. benzene (or $B_6$) is defined in two settings – as a relational structure (poset) and as a lattice.

As a preliminary work, we present the proofs of the dependence of other axiomatizations of ortholattices. The formalization of the properties of orthomodular lattices follows [4].

MML identifier: `ROBBINS4`, version: `7.9.03 4.104.1021`

The articles [6], [11], [13], [5], [2], [1], [3], [14], [12], [7], [8], and [9] provide the terminology and notation for this paper.

## 1. Preliminaries

Let $L$ be a lattice. One can verify that the lattice structure of $L$ is lattice-like.

Next we state the proposition

(1) For all lattices $K$, $L$ such that the lattice structure of $K$ = the lattice structure of $L$ holds $\mathrm{Poset}(K) = \mathrm{Poset}(L)$.

Let us note that every non empty ortholattice structure which is trivial is also quasi-meet-absorbing.

One can check that every ortholattice is lower-bounded and every ortholattice is upper-bounded.




ISSN 1426–2630(p), 1898-9934(e)

In the sequel $L$ denotes an ortholattice and $a$, $b$, $c$ denote elements of $L$.

We now state three propositions:

(2) $a \sqcup a^{\mathrm{c}} = \top_L$ and $a \sqcap a^{\mathrm{c}} = \bot_L$.

(3) Let $L$ be a non empty ortholattice structure. Then $L$ is an ortholattice if and only if the following conditions are satisfied:

(i) for all elements $a$, $b$, $c$ of $L$ holds $a \sqcup b \sqcup c = (c^{\mathrm{c}} \sqcap b^{\mathrm{c}})^{\mathrm{c}} \sqcup a$,

(ii) for all elements $a$, $b$ of $L$ holds $a = a \sqcap (a \sqcup b)$, and

(iii) for all elements $a$, $b$ of $L$ holds $a = a \sqcup (b \sqcap b^{\mathrm{c}})$.

(4) Let $L$ be an involutive lattice-like non empty ortholattice structure. Then $L$ is de Morgan if and only if for all elements $a$, $b$ of $L$ such that $a \sqsubseteq b$ holds $b^{\mathrm{c}} \sqsubseteq a^{\mathrm{c}}$.

## 2. Orthomodularity

Let $L$ be a non empty ortholattice structure. We say that $L$ is orthomodular if and only if:

(Def. 1) For all elements $x$, $y$ of $L$ such that $x \sqsubseteq y$ holds $y = x \sqcup (x^{\mathrm{c}} \sqcap y)$.

Let us observe that there exists an ortholattice which is trivial, orthomodular, modular, and Boolean.

Next we state the proposition

(5) Every modular ortholattice is orthomodular.

An orthomodular lattice is an orthomodular ortholattice.

One can prove the following proposition

(6) Let $L$ be an orthomodular meet-absorbing join-absorbing join-associative meet-commutative non empty ortholattice structure and $x$, $y$ be elements of $L$. Then $x \sqcup (x^{\mathrm{c}} \sqcap (x \sqcup y)) = x \sqcup y$.

Let $L$ be a non empty ortholattice structure. We say that $L$ satisfies OM if and only if:

(Def. 2) For all elements $x$, $y$ of $L$ holds $x \sqcup (x^{\mathrm{c}} \sqcap (x \sqcup y)) = x \sqcup y$.

Let us observe that every meet-absorbing join-absorbing join-associative meet-commutative non empty ortholattice structure which satisfies OM is also orthomodular and every meet-absorbing join-absorbing join-associative meet-commutative non empty ortholattice structure which is orthomodular satisfies also OM.

Let us observe that every ortholattice which is modular is also orthomodular.

Let us mention that there exists an ortholattice which is quasi-join-associative, quasi-meet-absorbing, de Morgan, and orthomodular.

## 3. Examples: The Benzene Ring

The relational structure $B_6$ is defined by:

(Def. 3) $B_6 = \langle\{0, 1, 3 \setminus 1, 2, 3 \setminus 2, 3\}, \subseteq\rangle$.

Let us note that $B_6$ is non empty and $B_6$ is reflexive, transitive, and antisymmetric.

Let us note that $B_6$ has l.u.b.'s and g.l.b.'s.

One can prove the following propositions:

(7) The carrier of $\mathbb{L}_{B_6} = \{0, 1, 3 \setminus 1, 2, 3 \setminus 2, 3\}$.

(8) For every set $a$ such that $a \in$ the carrier of $\mathbb{L}_{B_6}$ holds $a \subseteq 3$.

The strict ortholattice structure Benzene is defined by the conditions (Def. 4).

(Def. 4)(i) The lattice structure of Benzene $= \mathbb{L}_{B_6}$, and

(ii) for every element $x$ of the carrier of Benzene and for every subset $y$ of 3 such that $x = y$ holds (the complement operation of Benzene)$(x) = y^{\mathrm{c}}$.

The following three propositions are true:

(9) The carrier of Benzene $= \{0, 1, 3 \setminus 1, 2, 3 \setminus 2, 3\}$.

(10) The carrier of Benzene $\subseteq 2^3$.

(11) For every set $a$ such that $a \in$ the carrier of Benzene holds $a \subseteq \{0, 1, 2\}$.

Let us note that Benzene is non empty and Benzene is lattice-like.

The following propositions are true:

(12) Poset(the lattice structure of Benzene) $= B_6$.

(13) For all elements $a$, $b$ of $B_6$ and for all elements $x$, $y$ of Benzene such that $a = x$ and $b = y$ holds $a \leq b$ iff $x \sqsubseteq y$.

(14) For all elements $a$, $b$ of $B_6$ and for all elements $x$, $y$ of Benzene such that $a = x$ and $b = y$ holds $a \sqcup b = x \sqcup y$ and $a \sqcap b = x \sqcap y$.

(15) For all elements $a$, $b$ of $B_6$ such that $a = 3 \setminus 1$ and $b = 2$ holds $a \sqcup b = 3$ and $a \sqcap b = 0$.

(16) For all elements $a$, $b$ of $B_6$ such that $a = 3 \setminus 2$ and $b = 1$ holds $a \sqcup b = 3$ and $a \sqcap b = 0$.

(17) For all elements $a$, $b$ of $B_6$ such that $a = 3 \setminus 1$ and $b = 1$ holds $a \sqcup b = 3$ and $a \sqcap b = 0$.

(18) For all elements $a$, $b$ of $B_6$ such that $a = 3 \setminus 2$ and $b = 2$ holds $a \sqcup b = 3$ and $a \sqcap b = 0$.

(19) For all elements $a$, $b$ of Benzene such that $a = 3 \setminus 1$ and $b = 2$ holds $a \sqcup b = 3$ and $a \sqcap b = 0$.

(20) For all elements $a$, $b$ of Benzene such that $a = 3 \setminus 2$ and $b = 1$ holds $a \sqcup b = 3$.

(21) For all elements $a$, $b$ of Benzene such that $a = 3 \setminus 1$ and $b = 1$ holds $a \sqcup b = 3$.

(22) For all elements $a$, $b$ of Benzene such that $a = 3 \setminus 2$ and $b = 2$ holds $a \sqcup b = 3$.

(23) Let $a$ be an element of Benzene. Then

(i) if $a = 0$, then $a^{\mathrm{c}} = 3$,

(ii) if $a = 3$, then $a^{\mathrm{c}} = 0$,

(iii) if $a = 1$, then $a^{\mathrm{c}} = 3 \setminus 1$,

(iv) if $a = 3 \setminus 1$, then $a^{\mathrm{c}} = 1$,

(v) if $a = 2$, then $a^{\mathrm{c}} = 3 \setminus 2$, and

(vi) if $a = 3 \setminus 2$, then $a^{\mathrm{c}} = 2$.

(24) For all elements $a$, $b$ of Benzene holds $a \sqsubseteq b$ iff $a \subseteq b$.

(25) For all elements $a$, $x$ of Benzene such that $a = 0$ holds $a \sqcap x = a$.

(26) For all elements $a$, $x$ of Benzene such that $a = 0$ holds $a \sqcup x = x$.

(27) For all elements $a$, $x$ of Benzene such that $a = 3$ holds $a \sqcup x = a$.

One can check that Benzene is lower-bounded and Benzene is upper-bounded.

We now state two propositions:

(28) $\top_{\mathrm{Benzene}} = 3$.

(29) $\perp_{\mathrm{Benzene}} = 0$.

Let us note that Benzene is involutive and de Morgan and has top and Benzene is non orthomodular.

## 4. Orthogonality

Let $L$ be an ortholattice and let $a$, $b$ be elements of $L$. We say that $a$, $b$ are orthogonal if and only if:

(Def. 5) $a \sqsubseteq b^{\mathrm{c}}$.

Let $L$ be an ortholattice and let $a$, $b$ be elements of $L$. We introduce $a \perp b$ as a synonym of $a$, $b$ are orthogonal.

Next we state the proposition

(30) $a \perp a$ iff $a = \perp_L$.

Let $L$ be an ortholattice and let $a$, $b$ be elements of $L$. Let us note that the predicate $a$, $b$ are orthogonal is symmetric.

The following proposition is true

(31) If $a \perp b$ and $a \perp c$, then $a \perp b \sqcap c$ and $a \perp b \sqcup c$.

## 5. Orthomodularity Conditions

One can prove the following propositions:

(32) $L$ is orthomodular iff for all elements $a$, $b$ of $L$ such that $b^{\rm c} \sqsubseteq a$ and $a \sqcap b = \bot_L$ holds $a = b^{\rm c}$.

(33) $L$ is orthomodular iff for all elements $a$, $b$ of $L$ such that $a \perp b$ and $a \sqcup b = \top_L$ holds $a = b^{\rm c}$.

(34) $L$ is orthomodular iff for all elements $a$, $b$ of $L$ such that $b \sqsubseteq a$ holds $a \sqcap (a^{\rm c} \sqcup b) = b$.

(35) $L$ is orthomodular iff for all $a$, $b$ holds $a \sqcap (a^{\rm c} \sqcup (a \sqcap b)) = a \sqcap b$.

(36) $L$ is orthomodular iff for all elements $a$, $b$ of $L$ holds $a \sqcup b = ((a \sqcup b) \sqcap a) \sqcup ((a \sqcup b) \sqcap a^{\rm c})$.

(37) $L$ is orthomodular iff for all $a$, $b$ such that $a \sqsubseteq b$ holds $(a \sqcup b) \sqcap (b \sqcup a^{\rm c}) = (a \sqcap b) \sqcup (b \sqcap a^{\rm c})$.

(38) Let $L$ be a non empty ortholattice structure. Then $L$ is an orthomodular lattice if and only if the following conditions are satisfied:

(i) for all elements $a$, $b$, $c$ of $L$ holds $a \sqcup b \sqcup c = (c^{\rm c} \sqcap b^{\rm c})^{\rm c} \sqcup a$,

(ii) for all elements $a$, $b$, $c$ of $L$ holds $a \sqcup b = ((a \sqcup b) \sqcap (a \sqcup c)) \sqcup ((a \sqcup b) \sqcap a^{\rm c})$, and

(iii) for all elements $a$, $b$ of $L$ holds $a = a \sqcup (b \sqcap b^{\rm c})$.

One can verify that every quasi-join-associative quasi-meet-absorbing de Morgan orthomodular lattice-like non empty ortholattice structure has top.

Next we state the proposition

(39) Let $L$ be a non empty ortholattice structure. Then $L$ is an orthomodular lattice if and only if $L$ is quasi-join-associative, quasi-meet-absorbing, and de Morgan and satisfies OM.

## 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. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.
[4] Ladislav Beran. *Orthomodular Lattices. Algebraic Approach.* Academiai Kiado, 1984.
[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] Adam Grabowski. Robbins algebras vs. Boolean algebras. *Formalized Mathematics*, 9(**4**):681–690, 2001.
[8] Adam Grabowski and Robert Milewski. Boolean posets, posets under inclusion and products of relational structures. *Formalized Mathematics*, 6(**1**):117–121, 1997.
[9] Adam Grabowski and Markus Moschner. Formalization of ortholattices via orthoposets. *Formalized Mathematics*, 13(**1**):189–197, 2005.
[10] W. McCune, R. Padmanabhan, M. A. Rose, and R. Veroff. Automated discovery of single axioms for ortholattices. *Algebra Universalis*, 52(4):541–549, 2005.
[11] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

[12] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski – Zorn lemma. *Formalized Mathematics*, 1(**2**):387–393, 1990.
[13] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[14] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

*Received June 27, 2008*

FORMALIZED MATHEMATICS
Vol. 16, No. 3, Pages 283–288, 2008

# Basic Properties and Concept of Selected Subsequence of Zero Based Finite Sequences

Yatsuka Nakamura
Shinshu University
Nagano, Japan

Hisashi Ito
Shinshu University
Nagano, Japan

**Summary.** Here, we develop the theory of zero based finite sequences, which are sometimes, more useful in applications than normal one based finite sequences. The fundamental function Sgm is introduced as well as in case of normal finite sequences and other notions are also introduced. However, many theorems are a modification of old theorems of normal finite sequences, they are basically important and are necessary for applications. A new concept of selected subsequence is introduced. This concept came from the individual Ergodic theorem (see [7]) and it is the preparation for its proof.

MML identifier: `AFINSQ_2`, version: `7.9.03 4.104.1021`

The articles [12], [1], [14], [5], [8], [2], [6], [4], [3], [13], [10], [9], and [11] provide the notation and terminology for this paper.

## 1. Preliminaries

In this paper $D$ is a set.

One can prove the following proposition

(1) For every set $x$ and for every natural number $i$ such that $x \in i$ holds $x$ is an element of $\mathbb{N}$.

Let us observe that every natural number is natural-membered.




ISSN 1426–2630(p), 1898-9934(e)

## 2. Additional Properties of Zero Based Finite Sequence

One can prove the following propositions:

(2) For every finite natural-membered set $X_0$ there exists a natural number $m$ such that $X_0 \subseteq m$.

(3) Let $p$ be a finite 0-sequence and $b$ be a set. If $b \in \operatorname{rng} p$, then there exists an element $i$ of $\mathbb{N}$ such that $i \in \operatorname{dom} p$ and $p(i) = b$.

(4) Let $D$ be a set and $p$ be a finite 0-sequence. Suppose that for every natural number $i$ such that $i \in \operatorname{dom} p$ holds $p(i) \in D$. Then $p$ is a finite 0-sequence of $D$.

The scheme *XSeqLambdaD* deals with a natural number $\mathcal{A}$, a non empty set $\mathcal{B}$, and a unary functor $\mathcal{F}$ yielding an element of $\mathcal{B}$, and states that:

There exists a finite 0-sequence $z$ of $\mathcal{B}$ such that $\operatorname{len} z = \mathcal{A}$ and for every natural number $j$ such that $j \in \mathcal{A}$ holds $z(j) = \mathcal{F}(j)$

for all values of the parameters.

One can prove the following proposition

(5) Let $p$, $q$ be finite 0-sequences. Suppose $\operatorname{len} p = \operatorname{len} q$ and for every natural number $j$ such that $j \in \operatorname{dom} p$ holds $p(j) = q(j)$. Then $p = q$.

Let $f$ be a finite 0-sequence of $\mathbb{R}$ and let $a$ be an element of $\mathbb{R}$. Then $f + a$ is a finite 0-sequence of $\mathbb{R}$.

We now state two propositions:

(6) Let $f$ be a finite 0-sequence of $\mathbb{R}$ and $a$ be an element of $\mathbb{R}$. Then $\operatorname{len}(f + a) = \operatorname{len} f$ and for every natural number $i$ such that $i < \operatorname{len} f$ holds $(f + a)(i) = f(i) + a$.

(7) For all finite 0-sequences $f_1$, $f_2$ and for every natural number $i$ such that $i < \operatorname{len} f_1$ holds $(f_1 \frown f_2)(i) = f_1(i)$.

Let $f$ be a finite 0-sequence. The functor $\operatorname{Rev}(f)$ yielding a finite 0-sequence is defined as follows:

(Def. 1) $\operatorname{len} \operatorname{Rev}(f) = \operatorname{len} f$ and for every element $i$ of $\mathbb{N}$ such that $i \in \operatorname{dom} \operatorname{Rev}(f)$ holds $(\operatorname{Rev}(f))(i) = f(\operatorname{len} f - (i + 1))$.

We now state the proposition

(8) For every finite 0-sequence $f$ holds $\operatorname{dom} f = \operatorname{dom} \operatorname{Rev}(f)$ and $\operatorname{rng} f = \operatorname{rng} \operatorname{Rev}(f)$.

Let $D$ be a set and let $f$ be a finite 0-sequence of $D$. Then $\operatorname{Rev}(f)$ is a finite 0-sequence of $D$.

We now state several propositions:

(9) For every finite 0-sequence $p$ such that $p \neq \emptyset$ there exists a finite 0-sequence $q$ and there exists a set $x$ such that $p = q \frown \langle x \rangle$.

(10) For every natural number $n$ and for every finite 0-sequence $f$ such that $\operatorname{len} f \leq n$ holds $f \restriction n = f$.

(11) For every finite 0-sequence $f$ and for all natural numbers $n$, $m$ such that $n \leq \operatorname{len} f$ and $m \in n$ holds $(f \restriction n)(m) = f(m)$ and $m \in \operatorname{dom} f$.

(12) For every element $i$ of $\mathbb{N}$ and for every finite 0-sequence $q$ such that $i \leq \operatorname{len} q$ holds $\operatorname{len}(q \restriction i) = i$.

(13) For every element $i$ of $\mathbb{N}$ and for every finite 0-sequence $q$ holds $\operatorname{len}(q \restriction i) \leq i$.

(14) For every finite 0-sequence $f$ and for every element $n$ of $\mathbb{N}$ such that $\operatorname{len} f = n + 1$ holds $f = (f \restriction n) \frown \langle f(n) \rangle$.

Let $f$ be a finite 0-sequence and let $n$ be a natural number. The functor $f_{\lfloor n}$ yielding a finite 0-sequence is defined by:

(Def. 2) $\operatorname{len}(f_{\lfloor n}) = \operatorname{len} f -' n$ and for every natural number $m$ such that $m \in \operatorname{dom}(f_{\lfloor n})$ holds $f_{\lfloor n}(m) = f(m + n)$.

One can prove the following three propositions:

(15) For every finite 0-sequence $f$ and for every natural number $n$ such that $n \geq \operatorname{len} f$ holds $f_{\lfloor n} = \emptyset$.

(16) For every finite 0-sequence $f$ and for every natural number $n$ such that $n < \operatorname{len} f$ holds $\operatorname{len}(f_{\lfloor n}) = \operatorname{len} f - n$.

(17) For every finite 0-sequence $f$ and for all natural numbers $n$, $m$ such that $m + n < \operatorname{len} f$ holds $f_{\lfloor n}(m) = f(m + n)$.

Let $f$ be an one-to-one finite 0-sequence and let $n$ be a natural number. Note that $f_{\lfloor n}$ is one-to-one.

We now state several propositions:

(18) For every finite 0-sequence $f$ and for every natural number $n$ holds $\operatorname{rng}(f_{\lfloor n}) \subseteq \operatorname{rng} f$.

(19) For every finite 0-sequence $f$ holds $f_{\lfloor 0} = f$.

(20) For every natural number $i$ and for all finite 0-sequences $f$, $g$ holds $(f \frown g)_{\lfloor \operatorname{len} f + i} = g_{\lfloor i}$.

(21) For all finite 0-sequences $f$, $g$ holds $(f \frown g)_{\lfloor \operatorname{len} f} = g$.

(22) For every finite 0-sequence $f$ and for every element $n$ of $\mathbb{N}$ holds $(f \restriction n) \frown (f_{\lfloor n}) = f$.

Let $D$ be a set, let $f$ be a finite 0-sequence of $D$, and let $n$ be a natural number. Then $f_{\lfloor n}$ is a finite 0-sequence of $D$.

Let $f$ be a finite 0-sequence and let $k_1$, $k_2$ be natural numbers. The functor $\operatorname{mid}(f, k_1, k_2)$ yields a finite 0-sequence and is defined as follows:

(Def. 3) For all elements $k_{11}$, $k_{21}$ of $\mathbb{N}$ such that $k_{11} = k_1$ and $k_{21} = k_2$ holds $\operatorname{mid}(f, k_1, k_2) = (f \restriction k_{21})_{\lfloor k_{11} -' 1}$.

We now state several propositions:

(23) For every finite 0-sequence $f$ and for all natural numbers $k_1$, $k_2$ such that $k_1 > k_2$ holds $\operatorname{mid}(f, k_1, k_2) = \emptyset$.

(24) For every finite 0-sequence $f$ and for all natural numbers $k_1$, $k_2$ such that $1 \leq k_1$ and $k_2 \leq \operatorname{len} f$ holds $\operatorname{mid}(f, k_1, k_2) = f_{\lfloor k_1 -' 1} \restriction ((k_2 + 1) -' k_1)$.

(25) For every finite 0-sequence $f$ and for every natural number $k_2$ holds $\operatorname{mid}(f, 1, k_2) = f \restriction k_2$.

(26) For every finite 0-sequence $f$ of $D$ and for every natural number $k_2$ such that $\operatorname{len} f \leq k_2$ holds $\operatorname{mid}(f, 1, k_2) = f$.

(27) For every finite 0-sequence $f$ and for every element $k_2$ of $\mathbb{N}$ holds $\operatorname{mid}(f, 0, k_2) = \operatorname{mid}(f, 1, k_2)$.

(28) For all finite 0-sequences $f$, $g$ holds $\operatorname{mid}(f \frown g, \operatorname{len} f + 1, \operatorname{len} f + \operatorname{len} g) = g$.

Let $D$ be a set, let $f$ be a finite 0-sequence of $D$, and let $k_1$, $k_2$ be natural numbers. Then $\operatorname{mid}(f, k_1, k_2)$ is a finite 0-sequence of $D$.

Let $f$ be a finite 0-sequence of $\mathbb{R}$. The functor $\sum f$ yields an element of $\mathbb{R}$ and is defined by the condition (Def. 4).

(Def. 4) There exists a finite 0-sequence $g$ of $\mathbb{R}$ such that $\operatorname{len} f = \operatorname{len} g$ and $f(0) = g(0)$ and for every natural number $i$ such that $i+1 < \operatorname{len} f$ holds $g(i+1) = g(i) + f(i + 1)$ and $\sum f = g(\operatorname{len} f -' 1)$.

Let $f$ be an empty finite 0-sequence of $\mathbb{R}$. Observe that $\sum f$ is zero.

We now state two propositions:

(29) For every empty finite 0-sequence $f$ of $\mathbb{R}$ holds $\sum f = 0$.

(30) For all finite 0-sequences $h_1$, $h_2$ of $\mathbb{R}$ holds $\sum h_1 \frown h_2 = (\sum h_1) + \sum h_2$.

## 3. Selected Subsequences

Let $X$ be a finite natural-membered set. The functor $\operatorname{Sgm}_0 X$ yields a finite 0-sequence of $\mathbb{N}$ and is defined as follows:

(Def. 5) $\operatorname{rng} \operatorname{Sgm}_0 X = X$ and for all natural numbers $l$, $m$, $k_1$, $k_2$ such that $l < m < \operatorname{len} \operatorname{Sgm}_0 X$ and $k_1 = (\operatorname{Sgm}_0 X)(l)$ and $k_2 = (\operatorname{Sgm}_0 X)(m)$ holds $k_1 < k_2$.

Let $A$ be a finite natural-membered set. Note that $\operatorname{Sgm}_0 A$ is one-to-one.

Next we state three propositions:

(31) For every finite natural-membered set $A$ holds $\operatorname{len} \operatorname{Sgm}_0 A = \overline{\overline{A}}$.

(32) For all finite natural-membered sets $X$, $Y$ such that $X \subseteq Y$ and $X \neq \emptyset$ holds $(\operatorname{Sgm}_0 Y)(0) \leq (\operatorname{Sgm}_0 X)(0)$.

(33) For every natural number $n$ holds $(\operatorname{Sgm}_0 \{n\})(0) = n$.

Let $B_1$, $B_2$ be sets. The predicate $B_1 < B_2$ is defined by:

(Def. 6) For all natural numbers $n$, $m$ such that $n \in B_1$ and $m \in B_2$ holds $n < m$.

Let $B_1$, $B_2$ be sets. The predicate $B_1 \leq B_2$ is defined by:

(Def. 7) For all natural numbers $n$, $m$ such that $n \in B_1$ and $m \in B_2$ holds $n \leq m$.

The following propositions are true:

(34) For all sets $B_1$, $B_2$ such that $B_1 < B_2$ holds $B_1 \cap B_2 \cap \mathbb{N} = \emptyset$.

(35) For all finite natural-membered sets $B_1$, $B_2$ such that $B_1 < B_2$ holds $B_1$ misses $B_2$.

(36) For all sets $A$, $B_1$, $B_2$ such that $B_1 < B_2$ holds $A \cap B_1 < A \cap B_2$.

(37) For all finite natural-membered sets $X$, $Y$ such that $Y \neq \emptyset$ and there exists a set $x$ such that $x \in X$ and $\{x\} \leq Y$ holds $(\mathrm{Sgm}_0\, X)(0) \leq (\mathrm{Sgm}_0\, Y)(0)$.

(38) Let $X_0$, $Y_0$ be finite natural-membered sets and $i$ be a natural number. If $X_0 < Y_0$ and $i < \mathrm{card}\, X_0$, then $\mathrm{rng}(\mathrm{Sgm}_0(X_0 \cup Y_0) \restriction \mathrm{card}\, X_0) = X_0$ and $(\mathrm{Sgm}_0(X_0 \cup Y_0) \restriction \mathrm{card}\, X_0)(i) = (\mathrm{Sgm}_0(X_0 \cup Y_0))(i)$.

(39) For all finite natural-membered sets $X$, $Y$ and for every natural number $i$ such that $X < Y$ and $i \in \overline{\overline{X}}$ holds $(\mathrm{Sgm}_0(X \cup Y))(i) \in X$.

(40) Let $X$, $Y$ be finite natural-membered sets and $i$ be a natural number. If $X < Y$ and $i < \mathrm{len}\, \mathrm{Sgm}_0\, X$, then $(\mathrm{Sgm}_0\, X)(i) = (\mathrm{Sgm}_0(X \cup Y))(i)$.

(41) Let $X_0$, $Y_0$ be finite natural-membered sets and $i$ be a natural number. If $X_0 < Y_0$ and $i < \mathrm{card}\, Y_0$, then $\mathrm{rng}((\mathrm{Sgm}_0(X_0 \cup Y_0))_{\lfloor \mathrm{card}\, X_0}) = Y_0$ and $(\mathrm{Sgm}_0(X_0 \cup Y_0))_{\lfloor \mathrm{card}\, X_0}(i) = (\mathrm{Sgm}_0(X_0 \cup Y_0))(i + \mathrm{card}\, X_0)$.

(42) Let $X$, $Y$ be finite natural-membered sets and $i$ be a natural number. If $X < Y$ and $i < \mathrm{len}\, \mathrm{Sgm}_0\, Y$, then $(\mathrm{Sgm}_0\, Y)(i) = (\mathrm{Sgm}_0(X \cup Y))(i + \mathrm{len}\, \mathrm{Sgm}_0\, X)$.

(43) For all finite natural-membered sets $X$, $Y$ such that $Y \neq \emptyset$ and $X < Y$ holds $(\mathrm{Sgm}_0\, Y)(0) = (\mathrm{Sgm}_0(X \cup Y))(\mathrm{len}\, \mathrm{Sgm}_0\, X)$.

(44) Let $l$, $m$, $n$, $k$ be natural numbers and $X$ be a finite natural-membered set. If $k < l$ and $m < \mathrm{len}\, \mathrm{Sgm}_0\, X$ and $(\mathrm{Sgm}_0\, X)(m) = k$ and $(\mathrm{Sgm}_0\, X)(n) = l$, then $m < n$.

(45) For all finite natural-membered sets $X$, $Y$ such that $X \neq \emptyset$ and $X < Y$ holds $(\mathrm{Sgm}_0\, X)(0) = (\mathrm{Sgm}_0(X \cup Y))(0)$.

(46) For all finite natural-membered sets $X$, $Y$ holds $X < Y$ iff $\mathrm{Sgm}_0(X \cup Y) = (\mathrm{Sgm}_0\, X) \frown \mathrm{Sgm}_0\, Y$.

Let $f$ be a finite 0-sequence and let $B$ be a set. The $B$-subsequence of $f$ yields a finite 0-sequence and is defined as follows:

(Def. 8) The $B$-subsequence of $f = f \cdot \mathrm{Sgm}_0(B \cap \mathrm{len}\, f)$.

One can prove the following proposition

(47) Let $f$ be a finite 0-sequence and $B$ be a set. Then

(i) len (the $B$-subsequence of $f$) $= \overline{\overline{B \cap \mathrm{len}\, f}}$, and

(ii) for every natural number $i$ such that $i <$ len (the $B$-subsequence of $f$) holds (the $B$-subsequence of $f$)$(i) = f((\mathrm{Sgm}_0(B \cap \mathrm{len}\, f))(i))$.

Let $D$ be a set, let $f$ be a finite 0-sequence of $D$, and let $B$ be a set. Then the $B$-subsequence of $f$ is a finite 0-sequence of $D$.

Let $f$ be a finite 0-sequence. One can verify that the $\emptyset$-subsequence of $f$ is empty.

Let $B$ be a set. Observe that the $B$-subsequence of $\emptyset$ is empty.

We now state the proposition

(48) Let $B_1$, $B_2$ be finite natural-membered sets and $f$ be a finite 0-sequence of $\mathbb{R}$. Suppose $B_1 < B_2$. Then $\sum$ the $B_1 \cup B_2$-subsequence of $f = (\sum$ the $B_1$-subsequence of $f) + \sum$ the $B_2$-subsequence of $f$.

## 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. Increasing and continuous ordinal sequences. *Formalized Mathematics*, 1(**4**):711–714, 1990.
[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[6] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[7] Paul R. Halmos. *Lectures on Ergodic Theory.* The Mathematical Society of Japan, 1956. No.3.
[8] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[9] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[10] Karol Pąk. Cardinal numbers and finite sets. *Formalized Mathematics*, 13(**3**):399–406, 2005.
[11] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[12] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[13] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.
[14] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.


*Received June 27, 2008*

FORMALIZED MATHEMATICS
Volume 16, Number 3, 2008

# Addenda

## Authors



## MML Identifiers






ISSN 1426–2630(p), 1898-9934(e)