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 [13], [8], [14], [11], [16], [6], [5], [7], [1], [4], [12], [15], and [10] provide the notation and terminology for this paper.

Let $x$ be a set. The functor $\text{CastNat}_x$ yields a natural number and is defined by:

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

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

For simplicity, we use the following convention: $k, n$ 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 $\text{atom}_n$ yields a finite sequence of elements of $\mathbb{N}$ and is defined as follows:

\[(\text{Def. 2}) \quad \text{atom}_n = \langle 6 + n \rangle.\]

Let us consider $p$. The functor $\neg p$ yields a finite sequence of elements of $\mathbb{N}$ and is defined as follows:

\[(\text{Def. 3}) \quad \neg p = \langle 0 \rangle \smallfrown p.\]

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

\[(\text{Def. 4}) \quad p \land q = \langle 1 \rangle \smallfrown p \smallfrown q.\]

The functor $p \lor q$ yielding a finite sequence of elements of $\mathbb{N}$ is defined as follows:
Let us consider $p$. The functor $\mathbf{X}p$ yields a finite sequence of elements of $\mathbb{N}$ and is defined by:

\[(\text{Def. 6}) \quad \mathbf{X}p = \langle 3 \rangle \lhd p.\]

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

\[(\text{Def. 7}) \quad p\mathcal{U}q = \langle 4 \rangle \lhd p \lhd q.\]

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

\[(\text{Def. 8}) \quad p\mathcal{R}q = \langle 5 \rangle \lhd p \lhd q.\]

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

\[(\text{Def. 9}) \quad \text{For every } a \text{ such that } a \in \text{WFF}_{\text{LTL}} \text{ holds } a \text{ is a finite sequence of elements of } \mathbb{N} \text{ and for every } n \text{ holds atom}. n \in \text{WFF}_{\text{LTL}} \text{ and for every } p \text{ such that } p \in \text{WFF}_{\text{LTL}} \text{ holds } \neg p \in \text{WFF}_{\text{LTL}} \text{ and for all } p, q \text{ such that } p, q \in \text{WFF}_{\text{LTL}} \text{ holds } p \land q \in \text{WFF}_{\text{LTL}} \text{ and for all } p, q \text{ such that } p, q \in \text{WFF}_{\text{LTL}} \text{ holds } p \lor q \in \text{WFF}_{\text{LTL}} \text{ and for every } D \text{ such that for every } a \text{ such that } a \in D \text{ holds } a \text{ is a finite sequence of elements of } \mathbb{N} \text{ and for every } n \text{ holds atom}. n \in D \text{ and for every } p \text{ such that } p \in D \text{ holds } \neg p \in D \text{ and for all } p, q \text{ such that } p, q \in D \text{ holds } p \land q \in D \text{ and for all } p, q \text{ such that } p, q \in D \text{ holds } p \lor q \in D \text{ and for every } D \text{ such that for every } D \text{ holds } p \mathcal{U} q \in D \text{ holds } \text{WFF}_{\text{LTL}} \subseteq D.\]

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:

\[(\text{Def. 10}) \quad I_1 \text{ is an element of } \text{WFF}_{\text{LTL}}.\]

Let us mention 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 $\mathbb{N}$.

The following proposition is true

\[(1) \quad a \text{ is an LTL-formula iff } a \in \text{WFF}_{\text{LTL}}.\]

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

Let us consider $n$. Note that atom. $n$ is LTL-formula-like.

Let us consider $H$. Observe that $\neg H$ is LTL-formula-like and $\mathbf{X}H$ is LTL-formula-like. Let us consider $G$. One can verify the following observations:

* $H \land G$ is LTL-formula-like,
* $H \lor G$ 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 $H = \text{atom}.n$.

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 $H = F \land G$.

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

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

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

(Def. 15) There exists $H_1$ such that $H = X H_1$.

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

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

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

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

One can prove the following propositions:

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

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

Let us consider $H$. Let us assume that $H$ is negative or next. The functor $\text{Arg}(H)$ yielding an LTL-formula is defined as follows:

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

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

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

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

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

(iii) there exists $H_1$ such that $\text{LeftArg}(H) \mathcal{U} H_1 = H$ if $H$ is until,

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

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

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

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

(iii) there exists $H_1$ such that $H_1 \mathcal{U} \text{RightArg}(H) = H$ if $H$ is until,

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

The following propositions are true:

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

(5) If $H$ is next, then $H = X \text{Arg}(H)$.

(6) If $H$ is conjunctive, then $H = \text{LeftArg}(H) \land \text{RightArg}(H)$. 
(7) If $H$ is disjunctive, then $H = \text{LeftArg}(H) \lor \text{RightArg}(H)$.

(8) If $H$ is until, then $H = \text{LeftArg}(H) \mathcal{U} \text{RightArg}(H)$.

(9) If $H$ is release, then $H = \text{LeftArg}(H) \mathcal{R} \text{RightArg}(H)$.

(10) If $H$ is negative or next, then $\text{len } H = 1 + \text{len } \text{Arg}(H)$ and $\text{len } \text{Arg}(H) < \text{len } H$.

(11) If $H$ is conjunctive, or disjunctive, or until, or release, then $\text{len } H = 1 + \text{len } \text{LeftArg}(H) + \text{len } \text{RightArg}(H)$ and $\text{len } \text{LeftArg}(H) < \text{len } H$ and $\text{len } \text{RightArg}(H) < \text{len } H$.

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 $F = \mathbf{X} H$ or there exists $H_1$ such that $F = H \land H_1$ or $F = H_1 \land H$ or $F = H \lor H_1$ or $F = H_1 \lor H$ 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 $(F \land G)(1) = 1$ and $(F \lor G)(1) = 2$ and $(\mathbf{X} F)(1) = 3$ 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 $\mathbf{X} F$ iff $H = F$.

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

(16) $H$ is an immediate constituent of $F \lor G$ 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 $H = \text{Arg}(F)$.

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

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

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

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

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

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

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) \( \text{len } L = n \),

(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

\[
L(k) = H_1 \quad \text{and} \quad L(k+1) = F_1 \quad \text{and} \quad H_1 \text{ is an immediate constituent of } F_1.
\]

Next we 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 \( H \neq F \).

We now state a number of propositions:

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

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

(30) If \( G \) is negative or next, then \( \text{Arg}(G) \) is a subformula of \( G \).

(31) Suppose \( G \) is conjunctive, or disjunctive, or until, or release. Then \( \text{LeftArg}(G) \) is a subformula of \( G \) and \( \text{RightArg}(G) \) is a subformula of \( G \).

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

(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 negative or next and \( F \) is a proper subformula of \( G \), then \( F \) is a subformula of \( \text{Arg}(G) \).

(38) Suppose \( G \) is conjunctive, or disjunctive, or until, or release and \( F \) is a proper subformula of \( G \). Then \( F \) is a subformula of \( \text{LeftArg}(G) \) or a subformula of \( \text{RightArg}(G) \).

(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 \( X H \), then \( F \) is a subformula of \( H \).

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

(42) If \( F \) is a proper subformula of \( G \lor H \), then \( F \) is a subformula of \( G \) or a subformula of \( H \).
(43) If \( F \) is a proper subformula of \( G \cup H \), then \( F \) is a subformula of \( G \) or a subformula of \( H \).

(44) If \( F \) is a proper subformula of \( G \cap H \), then \( F \) is a subformula of \( G \) or a subformula of \( H \).

Let us consider \( H \). The functor Subformulae \( H \) yields a set and is defined as follows:

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

We now state the proposition

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

Let us consider \( H \). One can verify that Subformulae \( H \) is non empty. Next we state two propositions:

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

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

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

For every \( H \) holds \( P[H] \)

provided the following requirements are met:

- For every \( H \) such that \( H \) is atomic holds \( P[H] \),
- For every \( H \) such that \( H \) is negative or next and \( P[\text{Arg}(H)] \) holds \( P[H] \), and
- For every \( H \) such that \( H \) is conjunctive, or disjunctive, or until, or release and \( P[\text{LeftArg}(H)] \) and \( P[\text{RightArg}(H)] \) holds \( P[H] \).

The scheme \( \text{LTLCompInd} \) concerns a unary predicate \( P \), and states that:

For every \( H \) holds \( P[H] \)

provided the following condition is met:

- For every \( H \) such that for every \( F \) such that \( F \) is a proper subformula of \( H \) holds \( P[F] \) holds \( P[H] \).

Let \( x \) be a set. The functor \( \text{CastLTL} \) \( x \) yielding an LTL-formula is defined as follows:

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

We introduce LTL-model structures which are systems

\( \langle \text{assignations, basic assignations, a conjunction, an or-operation, a negation, a next-operation, an until-operation, a release-operation } \rangle \),

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 or-operation 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 \( \text{atomic}_{\text{LTL}} \) of \( \text{WFF}_{\text{LTL}} \) is defined as follows:

(Def. 26) \( \text{atomic}_{\text{LTL}} = \{ x \mid x \text{ ranges over LTL-formulae: } x \text{ is atomic} \} \).

Let \( V \) be an LTL-model structure, let \( K_1 \) be a function from \( \text{atomic}_{\text{LTL}} \)
into the basic assignations of \( V \), and let \( f \) be a function from \( \text{WFF}_{\text{LTL}} \)
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 \( f(H) = ( \text{the negation of } V)(f(\text{Arg}(H))) \),
(iii) if \( H \) is conjunctive, then \( f(H) = ( \text{the conjunction of } V)(f(\text{LeftArg}(H)),
                     f(\text{RightArg}(H))) \),
(iv) if \( H \) is disjunctive, then \( f(H) = ( \text{the or-operation of } V)(f(\text{LeftArg}(H)),
                     f(\text{RightArg}(H))) \),
(v) if \( H \) is next, then \( f(H) = ( \text{the next-operation of } V)(f(\text{Arg}(H))) \),
(vi) if \( H \) is until, then \( f(H) = ( \text{the until-operation of } V)(f(\text{LeftArg}(H)),
                     f(\text{RightArg}(H))) \), and
(vii) if \( H \) is release, then \( f(H) = ( \text{the release-operation of } V)(f(\text{LeftArg}(H)),
                     f(\text{RightArg}(H))) \).

Let \( V \) be an LTL-model structure, let \( K_1 \) be a function from \( \text{atomic}_{\text{LTL}} \)
into the basic assignations of \( V \), let \( f, h \) be functions from \( \text{WFF}_{\text{LTL}} \) 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 \( \text{len } H \leq n \). Then

(i) if \( H \) is atomic, then \( f(H) = K_1(H) \),
(ii) if \( H \) is negative, then \( f(H) = ( \text{the negation of } V)(f(\text{Arg}(H))) \),
(iii) if \( H \) is conjunctive, then \( f(H) = ( \text{the conjunction of } V)(f(\text{LeftArg}(H)),
                     f(\text{RightArg}(H))) \),
(iv) if \( H \) is disjunctive, then \( f(H) = ( \text{the or-operation of } V)(f(\text{LeftArg}(H)),
                     f(\text{RightArg}(H))) \),
(v) if \( H \) is next, then \( f(H) = ( \text{the next-operation of } V)(f(\text{Arg}(H))) \),
(vi) if \( H \) is until, then \( f(H) = ( \text{the until-operation of } V)(f(\text{LeftArg}(H)),
                     f(\text{RightArg}(H))) \), and
(vii) if \( H \) is release, then \( f(H) = ( \text{the release-operation of } V)(f(\text{LeftArg}(H)),
                     f(\text{RightArg}(H))) \).

Let \( V \) be an LTL-model structure, let \( K_1 \) be a function from \( \text{atomic}_{\text{LTL}} \)
into the basic assignations of \( V \), let \( f, h \) be functions from \( \text{WFF}_{\text{LTL}} \) into the
assignations of \( V \), let \( n \) be a natural number, and let \( H \) be an LTL-formula.

The functor \( \text{GraftEval}(V, K, f, h, n, H) \) yielding a set is defined by:

\[
\text{GraftEval}(V, K, f, h, n, H) = \begin{cases} 
  f(H), & \text{if } \text{len } H > n + 1, \\
  K_1(H), & \text{if } \text{len } H = n + 1 \text{ and } H \text{ is atomic,} \\
  (\text{the negation of } V)(h(\text{Arg}(H))), & \text{if } \text{len } H = n + 1 \text{ and} \\
  (\text{the conjunction of } V)(h(\text{LeftArg}(H))), & \text{if } \text{len } H = n + 1 \text{ and} \\
  (\text{the or-operation of } V)(h(\text{LeftArg}(H))), & \text{if } \text{len } H = n + 1 \text{ and} \\
  (\text{the next-operation of } V)(h(\text{Arg}(H))), & \text{if } \text{len } H = n + 1 \text{ and} \\
  (\text{the until-operation of } V)(h(\text{LeftArg}(H))), & \text{if } \text{len } H = n + 1 \text{ and} \\
  (\text{the release-operation of } V)(h(\text{LeftArg}(H))), & \text{if } \text{len } H = n + 1 \text{ and} \\
  h(H), & \text{if } \text{len } H < n + 1, \\
  \emptyset, & \text{otherwise.} 
\end{cases}
\]

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

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

\[
\text{EvalSet}(V, K_1, n) = \{ h; h \text{ ranges over functions from } \text{WFF}_{\text{LTL}} \text{ into the assignations of } V; \ h \text{ is a } n\text{-pre-evaluation for } K_1 \}.
\]

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 \( \text{CastEval}(V, x, v_0) \) yielding a function from \( \text{WFF}_{\text{LTL}} \) into the assignations of \( V \) is defined by:

\[
\text{CastEval}(V, x, v_0) = \begin{cases} 
  x, & \text{if } x \in (\text{the assignations of } V)^{\text{WFF}_{\text{LTL}}}, \\
  \text{WFF}_{\text{LTL}} \mapsto v_0, & \text{otherwise.} 
\end{cases}
\]

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

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

\begin{enumerate}
  \item \( p \in 2^{(\text{the assignations of } V)^{\text{WFF}_{\text{LTL}}}}, \text{ and} \)
  \item there exists a natural number \( n \) such that \( p = \text{EvalSet}(V, K_1, n) \).
\end{enumerate}

The following propositions are true:

\begin{enumerate}
  \item There exists \( f \) which is an evaluation for \( K_1 \).
  \item If \( f_1 \) is an evaluation for \( K_1 \) and \( f_2 \) is an evaluation for \( K_1 \), then \( f_1 = f_2 \).
\end{enumerate}

Let \( V \) be an LTL-model structure, let \( K_1 \) be a function from atomic_{\text{LTL}} into the basic assignations of \( V \), and let \( H \) be an LTL-formula. The functor \( \text{Evaluate}(H, K_1) \) yielding an assignation of \( V \) is defined as follows:

\[
\text{Evaluate}(H, K_1) = f(H).
\]

\( \text{Def. 29} \)
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 as follows:

(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 $f \land g$ yielding an assignation of $V$ is defined as follows:

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

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

(Def. 36) \( f \lor g = (\text{the or-operation of } V)(f, g) \).

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

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

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 as follows:

(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 by:

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

We now state several propositions:

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

(51) \( \text{Evaluate}(H_1 \land H_2, K_1) = \text{Evaluate}(H_1, K_1) \land \text{Evaluate}(H_2, K_1) \).

(52) \( \text{Evaluate}(H_1 \lor H_2, K_1) = \text{Evaluate}(H_1, K_1) \lor \text{Evaluate}(H_2, K_1) \).

(53) \( \text{Evaluate}(XH, K_1) = X \text{Evaluate}(H, K_1) \).

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

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

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

(Def. 40) \( \text{The infinite sequences of } S = S^\infty \).

Let $S$ be a non empty set and let $t$ be a sequence of $S$. The functor $\text{CastSeq}t$ yielding an element of the infinite sequences of $S$ is defined as follows:

(Def. 41) \( \text{CastSeq}t = t \).

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 $\text{CastSeq}(t, S)$ yields a sequence of $S$ and is defined by:

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

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

(Def. 43) \( \text{For every natural number } n \text{ holds } (\text{Shift}(t, k))(n) = t(n + k) \).
Let $S$ be a non empty set, let $t$ be a set, and let $k$ be a natural number. The functor $\text{Shift}(t, k, S)$ yields an element of the infinite sequences of $S$ and is defined by:

(Def. 44) \[ \text{Shift}(t, k, S) = \text{CastSeq} \text{Shift} (\text{CastSeq}(t, S), k) \]

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 $\text{Shift}(t, k)$ yielding an element of the infinite sequences of $S$ is defined as follows:

(Def. 45) \[ \text{Shift}(t, k) = \text{Shift}(t, k, S) \]

Let $S$ be a non empty set and let $f$ be a set. The functor $\text{Not}_0(f, S)$ yields an element of $\text{ModelSP}$ (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
\[ \neg \text{Castboolean} (\text{Fid}(f, \text{the infinite sequences of } S))(t) = \text{true} \] if and only if \[ (\text{Fid}(\text{Not}_0(f, S), \text{the infinite sequences of } S))(t) = \text{true} \]

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

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

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

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

Let $S$ be a non empty set and let $f$ be a set. The functor $\text{Next}_0(f, S)$ yields an element of $\text{ModelSP}$ (the infinite sequences of $S$) and is defined by the condition (Def. 49).

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

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

(Def. 50) For every set $f$ such that $f \in \text{ModelSP}$ (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 $\text{ModelSP}$ (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
\[ \text{Castboolean} (\text{Fid}(f, \text{the infinite sequences of } S))(t) \land \text{Castboolean} (\text{Fid}(g, \text{the infinite sequences of } S))(t) = \text{true} \] if and only if \[ (\text{Fid}(\text{And}_0(f, g, S), \text{the infinite sequences of } S))(t) = \text{true} \].
Let $S$ be a non empty set. The 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 \((\text{the and } S)(f, g) = \text{And}_0(f, g, S)\).

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 Until-univ$(t, f, g, S)$ yields an element of Boolean and is defined as follows:

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

Let $S$ be a non empty set and let $f, g$ be sets. The functor 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) Until-univ$(t, f, g, S) = \text{true if and only if } (\text{Fid}(\text{Until}_0(f, g, S)), \text{the infinite sequences of } S)(t) = \text{true}$.

Let $S$ be a non empty set. The functor 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 \((\text{Until}_S)(f, g) = \text{Until}_0(f, g, S)\).

Let $S$ be a non empty set. The functor $\lor_S$ 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 $\lor_S(f, g) = (\text{Not } S)((\text{the and } S)(f, (\text{Not } S)(g)))$.

The functor Release$_S$ yielding a binary operation on ModelSP (the infinite sequences of S) 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 $\text{Release}_S(f, g) = (\text{Not } S)((\text{Release}_S)(f, (\text{Not } S)(g)))$.

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 LTLModel$(S, B_1)$ yielding an LTL-model structure is defined as follows:

(Def. 58) LTLModel$(S, B_1) = (\text{ModelSP (the infinite sequences of S), } B_1, \text{the and } S, \lor_S, \text{Not } S, \text{Next } S, \text{Until } S, \text{Release } S)$.

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 LTLModel$(S, B_1)$. 
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 LTLModel($S, B_1$). The predicate $t \models f$ is defined as follows:

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

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 LTLModel($S, B_1$). We introduce $t \not\models f$ as an antonym of $t \models f$.

Next we state several propositions:

(56) \(f \lor g = \neg(\neg f \land \neg g)\) and \(f \mathcal{R} g = \neg(\neg f \mathcal{U} \neg g).\)

(57) \(t \models \neg f \text{ iff } t \not\models f.\)

(58) \(t \models f \land g \text{ iff } t \models f \text{ and } t \models g.\)

(59) \(t \models X f \text{ iff Shift}(t, 1) \models f.\)

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

(61) \(t \models f \lor g \text{ iff } t \models f \text{ or } t \models g.\)

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

The non empty set AtomicFamily is defined by:

(Def. 60) AtomicFamily = $2^{\text{atomicLTL}}$.

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

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

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

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

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

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

The function AtomicKai from atomicLTL into the basic assignations of LTLModel(AtomicFamily) is defined as follows:
(Def. 64) For every set $a$ such that $a \in \text{atomic}_{\text{LTL}}$ holds $(\text{AtomicKai})(a) = \text{AtomicAsgn} a$.

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) $r \models \text{Evaluate}(H, \text{AtomicKai})$.

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 $\text{WFF}_{\text{LTL}}$. The predicate $r \models W$ is defined as follows:

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

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

Let $W$ be a subset of $\text{WFF}_{\text{LTL}}$. The functor $\text{X} W$ yields a subset of $\text{WFF}_{\text{LTL}}$ and is defined as follows:

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

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

One can prove the following propositions:

(63) If $H$ is atomic, then $r \models H$ iff $H \in (\text{CastSeq}(r, \text{AtomicFamily}))(0)$.
(64) $r \models \neg H$ iff $r \not\models H$.
(65) $r \models H_1 \land H_2$ iff $r \models H_1$ and $r \models H_2$.
(66) $r \models H_1 \lor H_2$ iff $r \models H_1$ or $r \models H_2$.
(67) $r \models \text{X} H$ iff $\text{Shift}(r, 1) \models H$.
(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 $\text{Shift}(r, j) \models H_1$ and $\text{Shift}(r, m) \models H_2$.
(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 $\text{Shift}(r, j) \models \neg H_1$ holds $\text{Shift}(r, m) \models H_2$.
(70) $r \models \neg(H_1 \lor H_2)$ iff $r \models \neg H_1 \land \neg H_2$.
(71) $r \models \neg(H_1 \land H_2)$ iff $r \models \neg H_1 \lor \neg H_2$.
(72) $r \models H_1 \mathcal{R} H_2$ iff $r \models \neg(H_1 \mathcal{U} \neg H_2)$.
(73) $r \not\models \neg H$ iff $r \models H$.
(74) $r \models \text{X} \neg H$ iff $r \models \neg \text{X} H$.
(75) $r \models H_1 \mathcal{U} H_2$ iff $r \models H_2 \lor H_1 \land \text{X}(H_1 \mathcal{U} H_2)$.
(76) $r \models H_1 \mathcal{R} H_2$ iff $r \models H_1 \land H_2 \lor H_2 \land \text{X}(H_1 \mathcal{R} H_2)$.

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

We now state several propositions:
(77) \( r \models X W \) iff \( \text{Shift}(r, 1) \models W \).

(78)(i) If \( H \) is atomic, then \( H \) is not negative and \( H \) is not conjunctive and \( H \) is not disjunctive and \( H \) is not next and \( H \) is not until and \( H \) is not release,

(ii) if \( H \) is negative, then \( H \) is not atomic and \( H \) is not conjunctive and \( H \) is not disjunctive and \( H \) is not next and \( H \) is not until and \( H \) is not release,

(iii) if \( H \) is conjunctive, then \( H \) is not atomic and \( H \) is not negative and \( H \) is not disjunctive and \( H \) is not next and \( H \) is not until and \( H \) is not release,

(iv) if \( H \) is disjunctive, then \( H \) is not atomic and \( H \) is not negative and \( H \) is not conjunctive and \( H \) is not next and \( H \) is not until and \( H \) is not release,

(v) if \( H \) is next, then \( H \) is not atomic and \( H \) is not negative and \( H \) is not conjunctive and \( H \) is not disjunctive and \( H \) is not until and \( H \) is not release,

(vi) if \( H \) is until, then \( H \) is not atomic and \( H \) is not negative and \( H \) is not conjunctive and \( H \) is not disjunctive and \( H \) is not next and \( H \) is not release, and

(vii) if \( H \) is release, then \( H \) is not atomic and \( H \) is not negative and \( H \) is not conjunctive and \( H \) is not disjunctive and \( H \) is not next and \( H \) is not until.

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

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

(81) For every sequence \( s_1 \) of \( S \) holds \( \text{CastSeq}(\text{CastSeq}_1, S) = s_1 \).

(82) For every element \( s_1 \) of the infinite sequences of \( S \) holds \( \text{CastSeq}_1(\text{CastSeq}_1, S) = s_1 \).

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

References

Received April 21, 2008
Modular Integer Arithmetic

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.

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. Observe that $f|0$ is empty.

Let $f$ be a complex-valued finite sequence and let $n$ be a natural number. Observe that $f|n$ is complex-valued.

Let $f$ be an integer-valued finite sequence and let $n$ be a natural number. Observe that $f|n$ is integer-valued.

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

Let $i$ be an integer. One can check that $\langle i \rangle$ is integer-valued.

Let $f, g$ be integer-valued finite sequences. One can check that $f \sim g$ is integer-valued.

Next we state four propositions:

\footnote{This work has been partially supported by grant BW 5100-5-0293-7.}
(1) For all complex-valued finite sequences \( f_1, f_2 \) holds \( \text{len}(f_1 + f_2) = \min(\text{len} f_1, \text{len} f_2) \).

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

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

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

Let \( F \) be an integer-valued finite sequence. One can check 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 \( i + 1 \leq \text{len} f \), then \( (f \mid i) \cap (f(i + 1)) = f(i + 1) \).

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

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

(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 \( i \in \text{dom} m \) and \( m(i) \neq 0 \), then \( \prod_{m(i)}^m \) is an integer.

(10) Let \( m \) be an integer-valued finite sequence and \( i \) be a natural number. If \( i \in \text{dom} m \), 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 \( i, j \in \text{dom} m \) and \( j \neq i \) and \( m(j) \neq 0 \), then \( \prod_{m(i) \cdot m(j)}^m \) is an integer.

(12) Let \( m \) be an integer-valued finite sequence and \( i, j \) be natural numbers. Suppose \( i, j \in \text{dom} m \) and \( j \neq i \) and \( m(j) \neq 0 \). Then there exists an integer \( z \) such that \( z \cdot m(i) = \prod_{m(j)}^m \).

2. More on Greatest Common Divisors

The following propositions are true:

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

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

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

(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 \( i \cdot j \mid \text{lcm}(i, j) \).

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

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

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 \( i \in \text{dom } f \) 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 \( i, j \in \text{dom } f \) and \( i \neq j \) holds \( f(i) \) and \( f(j) \) are relative prime.

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

Let us observe that every integer-valued finite sequence which is multiplicative-trivial is also non empty.

One can prove the following proposition
(24) For every CR-sequence $f$ and for every natural number $m$ such that $0 < m \leq \text{len } f$ holds $f|m$ is a CR-sequence.

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

One can prove the following proposition

(25) Let $m$ be a CR-sequence and $i$ be a natural number. Suppose $i \in \text{dom } m$.

Let $m_3$ be an integer. If $m_3 = \prod_{m(i)} m | m$, then $m_3$ and $m(i)$ are relative prime.

4. Integer Arithmetic based on CRT

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

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

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

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

(Def. 4)(i) $\text{len } \text{it} = \text{len } m$,

(ii) for every natural number $i$ such that $i \in \text{dom } \text{it}$ there exists an integer $s$ and there exists an integer $m_3$ such that $m_3 = \prod_{m(i)} m$, and $s \cdot m_3 \equiv 1(\mod m(i))$ and $\text{it}(i) = s \cdot \prod_{m(i)} m$.

Let $m$ be a CR-sequence. Observe that every CR-coefficients of $m$ is integer-valued.

The following propositions are true:

(26) Let $m$ be a CR-sequence, $c$ be a CR-coefficients of $m$, and $i$ be a natural number. If $i \in \text{dom } c$, then $c(i) \equiv 1(\mod m(i))$.

(27) Let $m$ be a CR-sequence, $c$ be a CR-coefficients of $m$, and $i, j$ be natural numbers. If $i, j \in \text{dom } c$ and $i \neq j$, then $c(i) \equiv 0(\mod m(j))$.

(28) Let $m$ be a CR-sequence, $c_1, c_2$ be CR-coefficients(s) of $m$, and $i$ be a natural number. If $i \in \text{dom } c_1$, then $c_1(i) \equiv c_2(i)(\mod m(i))$.

(29) Let $u$ be an integer-valued finite sequence and $m$ be a CR-sequence. Suppose $\text{len } m = \text{len } u$. Let $c$ be a CR-coefficients of $m$ and $i$ be a natural number. If $i \in \text{dom } m$, then $\sum u \cdot c \equiv u(i)(\mod m(i))$.

(30) Let $u$ be an integer-valued finite sequence and $m$ be a CR-sequence. If $\text{len } m = \text{len } u$, then for all CR-coefficients(s) $c_1, c_2$ of $m$ holds $\sum u \cdot c_1 \equiv \sum u \cdot c_2(\mod \prod m)$.

Let $u$ be an integer-valued finite sequence and let $m$ be a CR-sequence. Let us assume that $\text{len } m = \text{len } u$. The functor $\mathbb{Z}(u, m)$ yielding an integer is defined by:
(Def. 5) For every CR-coefficients $c$ of $m$ holds $Z(u, m) = (\sum u_c) \mod \prod m$.

One can prove the following propositions:

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

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

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

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

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

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

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

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

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

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

5. Chinese Remainder Theorem Revisited

The following two propositions are true:

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

(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 $i \in \text{dom } m$ holds $z_1 \equiv u(i)(\mod m(i))$,
(iv) $0 \leq z_2$,
(v) $z_2 < \prod m$, and
(vi) for every natural number $i$ such that $i \in \text{dom } m$ holds $z_2 \equiv u(i)(\mod m(i))$. 
Then \( z_1 = z_2 \).

**References**


Received May 13, 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 [8]. 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: BCIALG5, version: 7.9.01 4.103.1019

The articles [12], [5], [14], [6], [15], [11], [2], [3], [7], [9], [1], [4], [10], [13], and [16] 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 $\text{Polynom}(m, n, x, y)$ yields an element of $X$ and is defined by:

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

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

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

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

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

(7) $\text{Polynom}(0, 0, x, y) = x \backslash (x \backslash y)$.

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

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

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

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

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

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 $N$ such that for all elements $x, y$ of $X$ holds $\text{Polynom}(i, j, x, y) = \text{Polynom}(m, n, y, x)$.

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

Let us observe that there exists a BCI-algebra which is quasi-commutative.

Let $i, j, m, n$ be elements of $N$. A BCI-algebra is called a BCI-algebra commutative with $i, j, m, n$ if:

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

One can prove the following three propositions:

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

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

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

Let us observe that there exists a BCK-algebra which is quasi-commutative.

Let $i, j, m, n$ be elements of $N$. A BCI-algebra commutative with $i, j, m, n$ which is BCK-5.

Let $i, j, m, n$ be elements of $N$. A BCK-algebra commutative with $i, j, m, n$ is BCK-5 BCI-algebra commutative with $i, j, m, n$.

Next we state several propositions:
(16) $X$ is a BCK-algebra commutative with $i, j, m, n$ and $i$ if and only if $X$ is a BCK-algebra commutative with $m, n, i, j$. 

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

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

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

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

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

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

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 commutative with $i, j, m, n$. Suppose $i = \min(i, j, m, n)$. If $i = j$, then $X$ is a BCK-algebra commutative with $i, i, i, i$. 

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

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

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

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

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

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

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

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

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

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

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

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 $X$.

The following propositions are true:

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

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

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

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

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

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

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

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

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

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

Let us observe that every BCK-algebra which is BCK-implicative is also commutative and every BCK-algebra which is BCK-implicative is also BCK-positive-implicative.

One can prove the following propositions:

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

(52) Let $X$ be a quasi-commutative BCK-algebra. Then $X$ is a BCK-algebra commutative with 0, 1, 0, and 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 commutative with $n, n+1, n$, and $n+1$ 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 commutative with 0, 1, 0, and 0, then $X$ is a BCI-commutative BCI-algebra.

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

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

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

(58) Let $X$ be a BCK-algebra commutative with $i, j, m, and n$. Suppose $n = 0$ and $i \neq 0$. Then $X$ is a BCK-algebra commutative with 0, 0, 0, and 0.
Let $X$ be a BCK-algebra commutative with $i$, $j$, $m$, and $n$. Suppose $i = 0$ and $n \neq 0$. Then $X$ is a BCK-algebra commutative with $0, 1, 0, \text{ and } 1$.

**References**


*Received May 13, 2008*
Block Diagonal Matrices

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

1. Preliminaries

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

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 $\text{len } f_1 = \text{len } f_2$, then $(f_1 + f_2) \bowtie (g_1 + g_2) = f_1 \bowtie g_1 + f_2 \bowtie g_2$.

2. For all finite sequences $f, g$ of elements of $D$ such that $i \in \text{dom } f$ holds $(f \bowtie g)_i = (f_i) \bowtie g$.

3. For all finite sequences $f, g$ of elements of $D$ such that $i \in \text{dom } g$ holds $(f \bowtie g)_{i + \text{len } f} = f \bowtie (g_i)$.
(4) If \( i \in \text{Seg}(n + 1) \), then \(((n + 1) \mapsto d)|_i = n \mapsto d\).

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

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

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

The following propositions are true:

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

(7) If \( i \in \text{Seg}(\sum f) \), then \( \min(f, i) - 1 = \min(f, i) - 1 \) and \( \sum f| (\min(f, i) - 1) < i \).

(8) If \( i \in \text{Seg}(\sum f) \), then \( \min(f \cap g, i) = \min(f, i) \).

(9) If \( i \in \text{Seg}((\sum f + \sum g) \setminus \text{Seg}(\sum f)) \), then \( \min(f \cap g, i) = \min(g, i - \sum f) \).

(10) If \( i \in \text{dom } f \) and \( j \in \text{Seg}(f_i) \), then \( j + \sum f|(i - 1) \) holds \( \in \text{Seg}(\sum f|i) \) and \( \min(f, j + \sum f|(i - 1)) = i \).

(11) For all \( i, j \) such that \( i \leq \text{len } f \) and \( j \leq \text{len } f \) and \( \sum f|i = \sum f|j \) and if \( i \in \text{dom } f \), then \( f(i) \neq 0 \) and if \( j \in \text{dom } f \), 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 \( i \in \text{dom } F \) holds \( F(i) \) is a matrix over \( D \).

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

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

Let us consider \( K \). A finite sequence of matrix of \( K \) is a matrix-yielding finite sequence of elements of \(((\text{the carrier of } K)^*)^*\).

Next we state the proposition

(12) \( \emptyset \) is a finite sequence of matrix of \( D \).

We adopt the following convention: \( F, F_1, F_2 \) denote finite sequence of matrices of \( D \) and \( G, G', G_1, G_2 \) denote finite sequence of matrices of \( K \).

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

Let us consider \( D, F_1, F_2 \). Then \( F_1 \cap F_2 \) is a finite sequence of matrix of \( D \).

Let us consider \( D, M_1 \). Then \( \langle M_1 \rangle \) is a finite sequence of matrix of \( D \).

Let us consider \( M_2 \). Then \( \langle M_1, M_2 \rangle \) is a finite sequence of matrix of \( D \).

Let us consider \( D, F, n \). Then \( F|n \) is a finite sequence of matrix of \( D \). Then \( F|n \) is a finite sequence of matrix of \( D \).
3. Sequences of Sizes of Matrices in a Finite Sequence

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

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

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

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

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

One can prove the following propositions:

(13) If $\sum \text{Len} F = 0$, then $\sum \text{Width} F = 0$.
(14) $\text{Len}(F_1 \triangleleft F_2) = (\text{Len} F_1) \triangleleft \text{Len} F_2$.
(15) $\text{Len}(M) = \langle \text{len} M \rangle$.
(16) $\sum \text{Len}(M_1, M_2) = \text{len} M_1 + \text{len} M_2$.
(17) $\text{Len}(F_1|n) = \text{Len} F_1|n$.
(18) $\text{Width}(F_1 \triangleleft F_2) = (\text{Width} F_1) \triangleleft \text{Width} F_2$.
(19) $\text{Width}(M) = \langle \text{width} M \rangle$.
(20) $\sum \text{Width}(M_1, M_2) = \text{width} M_1 + \text{width} M_2$.
(21) $\text{Width}(F_1|n) = \text{Width} F_1|n$.

4. Block Diagonal Matrices

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

(Def. 5)(i) \( \text{len} (\text{the block diagonal of } F \text{ and } d) = \sum \text{Len} F \),
(ii) \( \text{width} (\text{the block diagonal of } F \text{ and } d) = \sum \text{Width} F \), and
(iii) for all $i, j$ such that $\langle i, j \rangle \in \text{the indices of the block diagonal of } F$ and $d$ holds if $j \leq \sum \text{Width} F|\text{min}(\text{Len} F, i) - 1)$ or $j > \sum \text{Width} F|\min(\text{Len} F, i)$, then (the block diagonal of $F$ and $d$), $j = d$ and if $\sum \text{Width} F|\text{min}(\text{Len} F, i) - 1) < j \leq \sum \text{Width} F|\min(\text{Len} F, i)$, then (the block diagonal of $F$ and $d$), $j = F(\text{min}(\text{Len} F, i))_{i,j} \sum \text{Len} F(\text{min}(\text{Len} F, i) - 1), j - \sum \text{Width} F|\text{min}(\text{Len} F, i) - 1)$.

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

One can prove the following propositions:

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

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

(24) Let $M$ be a matrix over $D$ of dimension $\sum \text{Len}(M_1, M_2) \times \sum \text{Width}(M_1, M_2)$. Then $M$ = the block diagonal of $(M_1, M_2)$ and $d$ if and only if for every $i$ holds if $i \in \text{Seg width} M_1$, then $M_1 \cap i = (\text{len} M_2 \rightarrow d)$ and if $i \in \text{Seg width} M_2$, then $M_2 \cap i + \text{width} M_1 = (\text{len} M_1 \rightarrow d) \cap ((M_2)\cap i)$.

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

(26) Suppose $\langle i, j \rangle \in$ the indices of the block diagonal of $F_1$ and $d$. Then (the block diagonal of $F_1$ and $d$)\text{,}_i,j = (the block diagonal of $F_1 \cap F_2$ and $d$)\text{,}_i,j.

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

(28) Suppose $\langle i, j \rangle \in$ the indices of the block diagonal of $F_2$ and $d$. Then (the block diagonal of $F_2$ and $d$)\text{,}_i,j = (the block diagonal of $F_1 \cap F_2$ and $d_1 + \sum \text{Len} F_1, j + \sum \text{Width} F_1$).

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

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

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

(ii) $F(i)\text{,}_j,k = (the block diagonal of $F$ and $d$)\text{,}_j + \sum \text{Len} F\text{'}[i \rightarrow 1'), k + \sum \text{Width} F\text{'}[i \rightarrow 1')$.

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

(32) $M = \text{Segm}(\text{the block diagonal of } (M) \cap F$ and $d$, $\text{Seg len} M, \text{Seg width} M)$.

(33) $M = \text{Segm}(\text{the block diagonal of } F \cap (M) \cap F$ and $d$, $\text{Seg len} M + \sum \text{Len} F \setminus \text{Seg}(\sum \text{Len} F), \text{Seg}(\text{width} M + \sum \text{Width} F) \setminus \text{Seg}(\sum \text{Width} F))$.

(34) The block diagonal of $(M)$ and $d = M$.

(35) The block diagonal of $F_1 \cap F_2$ and $d$ = the block diagonal of $(the block diagonal of $F_1$ and $d$) \cap F_2$ and $d$. 
(36) The block diagonal of $F_1 \cap F_2$ and $d = \text{the block diagonal of } F_1 \cap \langle \text{the block diagonal of } F_2 \text{ and } d \rangle$ and $d$.

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

(38) If $i \in \text{Seg}(\sum \text{Width } F)$ and $m = \min(\text{Width } F, i)$, then $\text{Line}(\text{the block diagonal of } F \text{ and } d, i) = ((\sum \text{Len } F[(m -' 1)]) \mapsto d) \cap (F(m) \mapsto (\sum \text{Width } F[(m -' 1)]) \cap (((\sum \text{Len } F) -' \sum \text{Len } F[m]) \mapsto d)$.

(39) Let $M_1, M_2, N_1, N_2$ be matrices over $D$. Suppose that

(i) $\text{len } M_1 = \text{len } N_1$,
(ii) $\text{width } M_1 = \text{width } N_1$,
(iii) $\text{len } M_2 = \text{len } N_2$,
(iv) $\text{width } M_2 = \text{width } N_2$, and
(v) the block diagonal of $\langle M_1, M_2 \rangle$ and $d_1 = \text{the block diagonal of } \langle N_1, N_2 \rangle$ and $d_2$.

Then $M_1 = N_1$ and $M_2 = N_2$.

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

(i) the block diagonal of $F \cap \langle M \rangle$ and $d = \text{the block diagonal of } F \text{ and } d$, and

(ii) the block diagonal of $\langle M \rangle \cap F$ and $d = \text{the block diagonal of } F \text{ and } d$.

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

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

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

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

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 $i \in \text{dom } F$ there exists $n$ such that $F(i)$ is a matrix over $D$ of dimension $n$.

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

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

Let us consider $K$. A finite sequence of square-matrix of $K$ is a square-matrix-yielding finite sequence of elements of $((\text{the carrier of } K)^*)^*$. 

We follow the rules: $S, S_1, S_2$ denote finite sequence of square-matrices of $D$ and $R, R_1, R_2$ denote finite sequence of square-matrices of $K$.

The following proposition is true 
(45) $\emptyset$ is a finite sequence of square-matrix of $D$.

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

Let us consider $D, S_1, S_2$. Then $S_1 \sqcup S_2$ is a finite sequence of square-matrix of $D$.

Let us consider $D, n$ and let $M_1$ be a matrix over $D$ of dimension $n$. Then $(M_1)$ is a finite sequence of square-matrix of $D$.

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

Let us consider $D, S, n$. Then $S|n$ is a finite sequence of square-matrix of $D$. Then $S|n$ is a finite sequence of square-matrix of $D$.

We now state the proposition 
(46) $\text{Len} S = \text{Width} S$.

Let us consider $D, n$ and let $M_1$ be a matrix over $D$ of dimension $n$. Then the block diagonal of $S$ and $d$ is a matrix over $D$ of dimension $\sum \text{Len} S$.

One can prove the following propositions:

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

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

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

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

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

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

We now state several propositions:
(49) $\det(N) = \langle \det N \rangle$.
(50) $\det(R_1 \cap R_2) = \det R_1 \cap \det R_2$.
(51) $\det(R[n]) = \det R[n]$.
(52) $\det$ (the block diagonal of $\langle N, N_1 \rangle$ and $0_K$) = $\det N \cdot \det N_1$.
(53) $\det$ (the block diagonal of $R$ and $0_K$) = $\prod \det R$.
(54) If $\text{len } A_1 \neq \text{width } A_1$ and $N = \det$ (the block diagonal of $\langle A_1, A_2 \rangle$ and $0_K$), then $\det N = 0_K$.
(55) Suppose $\text{Len } G \neq \text{Width } G$. Let $M$ be a matrix over $K$ of dimension $n$. If $M = \det$ (the block diagonal of $G$ and $0_K$), then $\det M = 0_K$.

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 $\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}$ yields a finite sequence of square-matrix of $K$ and is defined as follows:

(Def. 8) $\text{dom}(\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^f) = \text{dom } f$ and for every $i$ such that $i \in \text{dom}(\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^f)$, holds $\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^f(i) = \begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^f(i \times f(i))$.

We now state several propositions:

(56) $\text{Len}(\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^f) = f$ and $\text{Width}(\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^f) = f$.

(57) For every element $i$ of $\mathbb{N}$ holds $\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^{\langle i \rangle \times \langle i \rangle} = \begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^{\langle i \rangle \times \langle i \rangle}$.

(58) $\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^{(f^g) \times (f^g)} = (\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^{f^g}) \times (\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^{f^g})$.

(59) $\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^{(f^{|n|}) \times (f^{|n|})} = (\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}_{K}^{f^{|n|}})^{|n|}$. 

The block diagonal of \( \begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}^i \otimes K \) and \( 0_K = \begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}^{(i+j) \times (i+j)} \).

The block diagonal of \( \begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}^j \otimes K \) and \( 0_K = \begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix}^{(\Sigma_j f) \times (\Sigma_j f)} \).

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 \( p \cdot G \) yields a finite sequence of matrix of \( K \) and is defined by:

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

Let us consider \( K \) and let us consider \( R, p \). Then \( p \cdot R \) is a finite sequence of square-matrix of \( K \).

The following propositions are true:

(62) \( \text{Len}(p \cdot G) = \text{Len} G \) and \( \text{Width}(p \cdot G) = \text{Width} G \).

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

(64) If \( \text{len} G = \text{len} p \) and \( \text{len} G_1 \leq \text{len} p_1 \), then \( p^{-1} p_1 \cdot G \cap G_1 = (p \cdot G) \cap (p_1 \cdot G_1) \).

(65) \( a \cdot \) the block diagonal of \( G \) and \( a_1 \) = the block diagonal of \( \text{len} G \mapsto a \cdot G \) and \( a \cdot a_1 \).

Let us consider \( K \) and let \( G_1, G_2 \) be finite sequence of matrices of \( K \). The functor \( G_1 \oplus G_2 \) yielding a finite sequence of matrix of \( K \) is defined by:

(Def. 10) \( \text{dom}(G_1 \oplus G_2) = \text{dom} G_1 \) and for every \( i \) such that \( i \in \text{dom}(G_1 \oplus G_2) \) 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-matrix of \( K \).

Next we state several propositions:

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

(67) If \( \text{len} G = \text{len} G' \), then \( G \cap G_1 \oplus G' \cap G_2 = (G \oplus G') \cap (G_1 \oplus G_2) \).

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

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

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

\[
\text{dom}(G_1 G_2) = \text{dom} G_1 \text{ and for every } i \text{ such that } i \in \text{dom}(G_1 G_2) \text{ holds (} G_1 G_2)(i) = G_1(i) \cdot G_2(i) \).
\]

We now state several propositions:

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

(74) If \( \text{len} G = \text{len} G' \), then \( (G \circ G_1) (G' \circ G_2) = (G G') \circ (G_1 G_2) \).

(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 width \( A_1 = \text{len} B_1 \) and width \( A_2 = \text{len} B_2 \). Then (the block diagonal of \( \langle A_1, A_2 \rangle \) and \( 0_K \) \) \( + \) (the block diagonal of \( \langle B_1, B_2 \rangle \) and \( 0_K \) \) = the block diagonal of \( \langle A_1, A_2 \rangle \langle B_1, B_2 \rangle \) and \( 0_K \).

(79) Suppose \( \text{Width} R_1 = \text{Len} R_2 \). Then (the block diagonal of \( R_1 \) and \( 0_K \) \) \( + \) (the block diagonal of \( R_2 \) and \( 0_K \) \) = the block diagonal of \( R_1 \oplus R_2 \) and \( 0_K \).

REFERENCES

Received May 13, 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 [17], 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: [11], [28], [2], [3], [12], [29], [8], [10], [9], [4], [5], [27], [23], [16], [7], [13], [31], [32], [30], [26], [24], [22], [33], [6], [19], [17], [21], [15], [14], [18], [25], [1], and [20].

1. Preliminaries

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

Next we state several 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 $W_1 \cap W_2 = 0_V$. 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 $W_1 + W_2$. 
(3) Let $V$ be a vector space over $K$ and $W_1, W_2$ be subspaces of $V$. Suppose $W_1 \cap W_2 = 0_V$. 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 $V$ 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 $\dim(\text{Lin}(A)) = \text{card } A$, then $A$ is linearly independent.

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

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 $V_3$, $v_1$ 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 $K$.

Next we state a number of propositions:

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

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

(9) If $\text{len } p_1 = \text{len } R_1$ and $\text{len } p_2 = \text{len } R_2$, then $\text{lmlt}(p_1 \cap p_2, R_1 \cap R_2) = (\text{lmlt}(p_1, R_1)) \cap \text{lmlt}(p_2, R_2)$.

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

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

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

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

(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 $\text{lmlt}(p, B_1) = \text{lmlt}(p, B_2)$.

(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 $i \in \text{dom } R$, then $\sum \text{lmlt}(\text{Line}(\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 \\ \vdots & \cdots & \cdots & \vdots \\ 0 & \cdots & \cdots & 1 \end{bmatrix}_{\text{len } R \times \text{len } R}, i), R) = R_i$. 


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) \( a \cdot v_1 \rightarrow b_1 = a \cdot (v_1 \rightarrow b_1) \).

(19) If \( i \in \text{dom} \, b_1 \), then \( (b_1)_i \rightarrow b_1 = \text{Line}(\begin{pmatrix} 1 & 0 \\ \vdots & \iddots \\ 0 & 1 \end{pmatrix}^K, i) \).

(20) \( 0_{(V_1)} \rightarrow b_1 = \text{len} \, b_1 \mapsto 0_K \).

(21) \( \text{len} \, b_1 = \text{dim}(V_1) \).

(22)(i) \( \text{rng}(b_1|m) \) is a linearly independent subset of \( V_1 \), and

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

(23)(i) \( \text{rng}((b_1)|m) \) is a linearly independent subset of \( V_1 \), and

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

(24) Let \( W_1, W_2 \) be subspaces of \( V_1 \). Suppose \( W_1 \cap W_2 = 0_{(V_1)} \). 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 \( b = b_1 \cap b_2 \). 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 \( v \rightarrow b = (w_1 \rightarrow b_1) \cap (w_2 \rightarrow b_2) \).

(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 \( v \rightarrow b_1 = w \rightarrow w_1 \).

(26) Let \( W_1, W_2 \) be subspaces of \( V_1 \). Suppose \( W_1 \cap W_2 = 0_{(V_1)} \). Let \( w_1 \) be an ordered basis of \( W_1 \) and \( w_2 \) be an ordered basis of \( W_2 \). Then \( w_1 \cap w_2 \) 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 \( \text{AutMt}(f, B_1, b_2) \) is a matrix over \( K \) of dimension \( \text{len} \, b_1 \times \text{len} \, b_2 \).

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

(Def. 1) \( R|S = R|\text{the carrier of } S \).

Next we state the proposition

(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 \( \text{dim}(W_1) = 0 \), then \( \text{dim}(U_1) = 0 \) and if \( \text{dim}(W_2) = 0 \), then \( \text{dim}(U_2) = 0 \) 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 $f_1 = f|_{W_1}$ and
$f_2 = f|_{W_2}$. 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 $w_1 ^\sim w_2 = b_1$ and $u_1 ^\sim u_2 = b_2$. Then $\text{AutMt}(f, b_1, b_2) =$ the block
of dimension $\text{len} B_1 \times \text{len} B_1$ is defined by:

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

The following propositions are true:

(28) $\text{AutMt}(\text{id}_{V_1}, b_1, b_1) = \begin{pmatrix} 1 & 0 \\ & \ddots \\ 0 & 1 \end{pmatrix}_{\text{len} b_1 \times \text{len} b_1}$

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

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

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

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
$\text{len} b_1 \times \text{len} B_2$. The functor $\text{Mx2Tran}(M, b_1, B_2)$ yields a function from $V_1$ into
$V_2$ and is defined as follows:

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

The following propositions are true:

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

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

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

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

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

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

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 $n \times m$.

Next we state several propositions:

(37) For all matrices $A, B$ over $K$ of dimension $\text{len} b_1 \times \text{len} b_2$ holds $\text{Mx2Tran}(A + B, b_1, b_2) = \text{Mx2Tran}(A, b_1, B_2) + \text{Mx2Tran}(B, b_1, B_2)$.

(38) For every matrix $A$ over $K$ of dimension $\text{len} b_1 \times \text{len} b_2$ holds $a \cdot \text{Mx2Tran}(A, b_1, B_2) = \text{Mx2Tran}(a \cdot A, b_1, B_2)$.

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

(40) Let $A$ be a matrix over $K$ of dimension $\text{len} b_1 \times \text{len} b_2$ and $B$ be a matrix over $K$ of dimension $\text{len} b_2 \times \text{len} b_3$. Suppose width $A = \text{len} B$. Let $A_1$ be a matrix over $K$ of dimension $\text{len} b_1 \times \text{len} b_3$. If $A_1 = A \cdot B$, then $\text{Mx2Tran}(A_1, b_1, B_3) = \text{Mx2Tran}(B, b_2, B_3) \cdot \text{Mx2Tran}(A, b_1, b_2)$.

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

(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 $\ker f = \{0_{V_1}\}$.

Let us consider $K$ and let $V_1$ be a vector space over $K$. Then $\text{id}_{V_1}$ 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 $K$, 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 $\text{len} b_1 \times \text{len} b_2$ such that $\text{rk}(A) = \text{len} b_1$ holds $\text{Mx2Tran}(A, b_1, b_2)$ is one-to-one.
Let $M$ be an ordered basis of the $n$-dimension vector space over $K$.

Suppose $M = \text{MX2FinS}(\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix})^K_{n \times n}$.

Then $v_1 \rightarrow M = v_1$.

Let $M$ be an ordered basis of the $\text{len} b_2$-dimension vector space over $K$.

Suppose $M = \text{MX2FinS}(\begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix})^K_{\text{len} b_2 \times \text{len} b_2}$.

Let $A$ be a matrix over $K$ of dimension $\text{len} b_1 \times \text{len} M$.

If $A = \text{AutMt}(f, b_1, b_2)$ and $f$ is linear, then $(\text{Mx2Tran}(A, b_1, M))(v_1) = f(v_1) \rightarrow b_2$.

6. The Main Theorems

We now state four propositions:

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

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

(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 Det $\text{AutEqMt}(f, b_1, b_2) = 0_K$.

(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 $g \mid \text{im} f$ is one-to-one, then rank$(g \cdot f) = \text{rank} f$ and nullity$(g \cdot f) = \text{nullity} f$.

References


Received May 13, 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 [13], 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 [5].

MML identifier: ROBBINS4, version: 7.9.03 4.104.1021

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

1. Preliminaries

Let \( L \) be a lattice. Note that the lattice structure of \( L \) is lattice-like.

The following proposition is true

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

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

One can verify that every ortholattice is lower-bounded and every ortholattice is upper-bounded.
In the sequel \( L \) denotes an ortholattice and \( a, b, c \) denote elements of \( L \).
The following propositions are true:

(2) \( a \sqcup a^c = \top_L \) and \( a \cap a^c = \bot_L \).

(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 \( a \sqcup b \sqcup c = (c \cap b^c)^c \sqcup a \),
    (ii) for all elements \( a, b \) of \( L \) holds \( a = a \cap (a \sqcup b) \), and
    (iii) for all elements \( a, b \) of \( L \) holds \( a = a \sqcup (b \cap b^c) \).

(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 \( b^c \sqsubseteq a^c \).

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 \( y = x \sqcup (x^c \cap y) \).

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

The following proposition is true

(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 \( x \sqcup (x^c \cap (x \sqcup y)) = x \sqcup y \).

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

(Def. 2) For all elements \( x, y \) of \( L \) holds \( x \sqcup (x^c \cap (x \sqcup y)) = x \sqcup y \).

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

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

Let us observe 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 anti-symmetric.

Let us observe that $B_6$ has l.u.b.’s and g.l.b.’s.

Next we state two propositions:

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

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

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

(Def. 4)(i) The lattice structure of Benzene $= L_{B_6}$, 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)$\overline{(x)} = y^c$.

Next we state three propositions:

(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 mention that Benzene is non empty and Benzene is lattice-like.

One can prove the following propositions:

(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 $x \subseteq y$.

(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 $a \lor b = x \sqcup y$ and $a \land b = x \sqcap y$.

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

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

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

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

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

(20) For all elements $a, b$ of Benzene such that $a = 3 \setminus 2$ and $b = 1$ holds $a \lor b = 3$. 
(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 $a^\mathcal{c} = 3$,
   (ii) if $a = 3$, then $a^\mathcal{c} = 0$,
   (iii) if $a = 1$, then $a^\mathcal{c} = 3 \setminus 1$,
   (iv) if $a = 3 \setminus 1$, then $a^\mathcal{c} = 1$,
   (v) if $a = 2$, then $a^\mathcal{c} = 3 \setminus 2$, and
   (vi) if $a = 3 \setminus 2$, then $a^\mathcal{c} = 2$.

(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 $a \sqcup x = a$.

Let us observe that Benzene is lower-bounded and Benzene is upper-bounded.

We now state two propositions:

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

(29) $\bot_{\text{Benzene}} = 0$.

One can verify 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) $a \sqsubseteq b^\mathcal{c}$.

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.

We now state the proposition

(30) $a \perp a$ if $a = \bot_L$.

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.

One can prove the following proposition

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

The following propositions are true:

(32) \( L \) is orthomodular iff for all elements \( a, b \) of \( L \) such that \( b^c \subseteq a \) and \( a \cap b = \bot_L \) holds \( a = b^c \).

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

(34) \( L \) is orthomodular iff for all elements \( a, b \) of \( L \) such that \( b \subseteq a \) holds \( a \cap (a^c \cup b) = b \).

(35) \( L \) is orthomodular iff for all \( a, b \) of \( L \) holds \( a \cap (a^c \cup (a \cap b)) = a \cap b \).

(36) \( L \) is orthomodular iff for all elements \( a, b \) of \( L \) holds \( a \cup b = ((a \cup b) \cap a) \cup ((a \cup b) \cap a^c) \).

(37) \( L \) is orthomodular iff for all \( a, b \) such that \( a \subseteq b \) holds \( (a \cup b) \cap (b \cup a^c) = (a \cap b) \cup (b \cap a^c) \).

(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 \( a \cup b \cup c = (c^c \cap b^c)^c \cup a \),

(ii) for all elements \( a, b, c \) of \( L \) holds \( a \cup b = ((a \cup b) \cap (a \cup c)) \cup ((a \cup b) \cap a^c) \), and

(iii) for all elements \( a, b \) of \( L \) holds \( a = a \cup (b \cap b^c) \).

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, de Morgan, and orthomodular.

References

Received June 27, 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 [10]) and it is the preparation for its proof.

MML identifier: AFINSQ_2, version: 7.9.03 4.104.1021

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

1. Preliminaries

In this paper $D$ denotes a set.

Next we state the proposition

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

One can verify that every natural number is natural-membered.
2. Additional Properties of Zero Based Finite Sequence

Next we state three 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 $b \in \text{rng } p$, then there exists an element $i$ of $\mathbb{N}$ such that $i \in \text{dom } p$ 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 $i \in \text{dom } p$ holds $p(i) \in D$. Then $p$ is a finite 0-sequence of $D$.

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

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

for all values of the parameters.

Next we state the proposition

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

One can prove the following two propositions:

(6) Let $f$ be a finite 0-sequence of $\mathbb{R}$ and $a$ be an element of $\mathbb{R}$. Then $\text{len } (f + a) = \text{len } f$ and for every natural number $i$ such that $i < \text{len } f$ 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 $i < \text{len } f_1$ holds $(f_1 \upharpoonright f_2)(i) = f_1(i)$.

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

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

Next we state the proposition

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

Let $D$ be a set and let $f$ be a finite 0-sequence of $D$. Then $\text{Rev}(f)$ 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 $p = q \upharpoonright \{x\}$.

(10) For every natural number $n$ and for every finite 0-sequence $f$ such that $\text{len } f \leq n$ holds $f|n = f$. 
For every finite 0-sequence $f$ and for all natural numbers $n, m$ such that $n \leq \text{len } f$ and $m \in n$ holds $(f\lceil n)(m) = f(m)$ and $m \in \text{dom } f$.

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

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

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

Let $f$ be a finite 0-sequence and let $n$ be a natural number. The functor $f\lceil n$ yielding a finite 0-sequence is defined as follows:

\begin{equation}
\text{len}(f\lceil n) = \text{len } f - n \quad \text{and for every natural number } m \text{ such that } m \in \text{dom}(f\lceil n) \text{ holds } f\lceil n(m) = f(m + n).
\end{equation}

Next we state three propositions:

For every finite 0-sequence $f$ and for every natural number $n$ such that $n \geq \text{len } f$ holds $f\lceil n = \emptyset$.

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

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

Let $f$ be an one-to-one finite 0-sequence and let $n$ be a natural number. One can check that $f\lceil n$ is one-to-one.

One can prove the following propositions:

For every finite 0-sequence $f$ and for every natural number $n$ holds $\text{rng}(f\lceil n) \subseteq \text{rng } f$.

For every finite 0-sequence $f$ holds $f\lceil 0 = f$.

For every natural number $i$ and for all finite 0-sequences $f, g$ holds $(f \circ g)\lceil \text{len } f + i = g\lceil i$.

For all finite 0-sequences $f, g$ holds $(f \circ g)\lceil \text{len } f = g$.

For every finite 0-sequence $f$ and for every element $n$ of $\mathbb{N}$ holds $(f\lceil n) \ominus (f\lceil n) = f$.

Let $D$ be a set, let $f$ be a finite 0-sequence of $D$, and let $n$ be a natural number. Then $f\lceil n$ 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 $\text{mid}(f, k_1, k_2)$ yields a finite 0-sequence and is defined as follows:

\begin{equation}
\text{mid}(f, k_1, k_2) = (f\lceil k_2)(k_1 - 1).
\end{equation}

We now state several propositions:

For all elements $k_{11}, k_{21}$ of $\mathbb{N}$ such that $k_{11} = k_1$ and $k_{21} = k_2$ holds $\text{mid}(f, k_1, k_2) = (f\lceil k_{21})(k_{11} - 1)$.

For every finite 0-sequence $f$ and for all natural numbers $k_1, k_2$ such that $k_1 > k_2$ holds $\text{mid}(f, k_1, k_2) = \emptyset$.\)
(24) For every finite 0-sequence $f$ and for all natural numbers $k_1$, $k_2$ such that $1 \leq k_1$ and $k_2 \leq \text{len } f$ holds $\text{mid}(f, k_1, k_2) = f|_{[k_1-1]'}((k_2 + 1)' - k_1)$.

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

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

(27) For every finite 0-sequence $f$ and for every element $k_2$ of $\mathbb{N}$ holds $	ext{mid}(f, 0, k_2) = \text{mid}(f, 1, k_2)$.

(28) For all finite 0-sequences $f$, $g$ holds $\text{mid}(f \succ g, \text{len } f + 1, \text{len } f + \text{len } g) = g$.

Let $D$ be a set, let $f$ be a finite 0-sequence of $D$, and let $k_1$, $k_2$ be natural numbers. Then $\text{mid}(f, k_1, k_2)$ 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 $\text{len } f = \text{len } g$ and $f(0) = g(0)$ and for every natural number $i$ such that $i + 1 < \text{len } f$ holds $g(i + 1) = g(i) + f(i + 1)$ and $\sum f = g(\text{len } f - 1)$.

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 $\sum h_1 \succ h_2 = (\sum h_1) + (\sum h_2)$.

3. Selected Subsequences

Let $X$ be a finite natural-membered set. The functor $\text{Sgm}_0 X$ yielding a finite 0-sequence of $\mathbb{N}$ is defined by:

(Def. 5) $\text{rng } \text{Sgm}_0 X = X$ and for all natural numbers $l$, $m$, $k_1$, $k_2$ such that $l < m < \text{len } \text{Sgm}_0 X$ and $k_1 = (\text{Sgm}_0 X)(l)$ and $k_2 = (\text{Sgm}_0 X)(m)$ holds $k_1 < k_2$.

Let $A$ be a finite natural-membered set. One can verify that $\text{Sgm}_0 A$ is one-to-one.

One can prove the following propositions:

(31) For every finite natural-membered set $A$ holds $\text{len } \text{Sgm}_0 A = \overline{\text{len } A}$.

(32) For all finite natural-membered sets $X$, $Y$ such that $X \subseteq Y$ and $X \neq \emptyset$ holds $(\text{Sgm}_0 Y)(0) \leq (\text{Sgm}_0 X)(0)$.

(33) For every natural number $n$ holds $(\text{Sgm}_0 \{n\})(0) = n$.

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 as follows:

(Def. 7) For all natural numbers $n$, $m$ such that $n \in B_1$ and $m \in B_2$ holds $n \leq m$. 
One can prove the following propositions:

(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 \( \text{rng}(\text{Sgm}_0 X)(0) \leq \text{rng}(\text{Sgm}_0 Y)(0) \).

(38) Let \( X_0, Y_0 \) be finite natural-membered sets and \( i \) be a natural number.
If \( X_0 < Y_0 \) and \( i < \text{card} X_0 \), then \( \text{rng}(\text{Sgm}_0 (X_0 \cup Y_0) | \text{card} X_0) = X_0 \) and \( \text{rng}(\text{Sgm}_0 (X_0 \cup Y_0) | \text{card} X_0)(i) = (\text{Sgm}_0 (X_0 \cup Y_0))(i) \).

(39) For all finite natural-membered sets \( X, Y \) and for every natural number \( i \) such that \( X < Y \) and \( i \in X \) holds \( (\text{Sgm}_0 (X \cup Y))(i) \in X \).

(40) Let \( X, Y \) be finite natural-membered sets and \( i \) be a natural number. If \( X < Y \) and \( i < \text{len} \text{Sgm}_0 X \), then \( (\text{Sgm}_0 X)(i) = (\text{Sgm}_0 (X \cup Y))(i) \).

(41) Let \( X_0, Y_0 \) be finite natural-membered sets and \( i \) be a natural number.
If \( X_0 < Y_0 \) and \( i < \text{card} Y_0 \), then \( \text{rng}(\text{Sgm}_0 (X_0 \cup Y_0) | \text{card} X_0) = Y_0 \) and \( \text{rng}(\text{Sgm}_0 (X_0 \cup Y_0) | \text{card} X_0)(i) = (\text{Sgm}_0 (X_0 \cup Y_0))(i + \text{card} X_0) \).

(42) Let \( X, Y \) be finite natural-membered sets and \( i \) be a natural number.
If \( X < Y \) and \( i < \text{len} \text{Sgm}_0 Y \), then \( (\text{Sgm}_0 Y)(i) = (\text{Sgm}_0 (X \cup Y))(i + \text{len} \text{Sgm}_0 X) \).

(43) For all finite natural-membered sets \( X, Y \) such that \( Y \neq \emptyset \) and \( X < Y \) holds \( (\text{Sgm}_0 Y)(0) = (\text{Sgm}_0 (X \cup Y))(\text{len} \text{Sgm}_0 X) \).

(44) Let \( l, m, n, k \) be natural numbers and \( X \) be a finite natural-membered set.
If \( k < l \) and \( m < \text{len} \text{Sgm}_0 X \) and \( (\text{Sgm}_0 X)(m) = k \) and \( (\text{Sgm}_0 X)(n) = l \), then \( m < n \).

(45) For all finite natural-membered sets \( X, Y \) such that \( X \neq \emptyset \) and \( X < Y \) holds \( (\text{Sgm}_0 X)(0) = (\text{Sgm}_0 (X \cup Y))(0) \).

(46) For all finite natural-membered sets \( X, Y \) holds \( X < Y \) iff \( \text{Sgm}_0 (X \cup Y) = (\text{Sgm}_0 X) \cap \text{Sgm}_0 Y \).

Let \( f \) be a finite 0-sequence and let \( B \) be a set. The functor \( \text{SubXFinS}(f, B) \) yields a finite 0-sequence and is defined by:

(Def. 8) \[ \text{SubXFinS}(f, B) = f \cdot \text{Sgm}_0 (B \cap \text{len} f). \]

The following proposition is true

(47) Let \( f \) be a finite 0-sequence and \( B \) be a set. Then \( \text{len} \text{SubXFinS}(f, B) = \overline{B \cap \text{len} f} \) and for every natural number \( i \) such that \( i < \text{len} \text{SubXFinS}(f, B) \) holds \( (\text{SubXFinS}(f, B))(i) = f((\text{Sgm}_0 (B \cap \text{len} f))(i)). \)

Let \( D \) be a set, let \( f \) be a finite 0-sequence of \( D \), and let \( B \) be a set. Then \( \text{SubXFinS}(f, B) \) is a finite 0-sequence of \( D \).
Let $f$ be a finite 0-sequence. One can verify that $\text{SubXFinS}(f, \emptyset)$ is empty.

Let $B$ be a set. One can verify that $\text{SubXFinS}(\emptyset, B)$ is empty.

Next we state the proposition

(48) Let $B_1, B_2$ be finite natural-membered sets and $f$ be a finite 0-sequence of $\mathbb{R}$. If $B_1 < B_2$, then $\sum \text{SubXFinS}(f, B_1 \cup B_2) = (\sum \text{SubXFinS}(f, B_1)) + \sum \text{SubXFinS}(f, B_2)$.

**References**


Received June 27, 2008
Contents

Model Checking. Part II
By Kazuhisa Ishida .............................................. 239

Modular Integer Arithmetic
By Christoph Schwarzweller ................................. 255

General Theory of Quasi-Commutative BCI-algebras
By Tao Sun et al. .................................................. 261

Block Diagonal Matrices
By Karol Pałk ..................................................... 267

Linear Map of Matrices
By Karol Pałk ..................................................... 277

Orthomodular Lattices
By Elżbieta Madra and Adam Grabowski ................. 285

Basic Properties and Concept of Selected Subsequence of Zero Based Finite Sequences
By Yatsuka Nakamura and Hisashi Ito .................... 291

Continued on inside back cover