FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

The Lawson Topology[1]

Grzegorz Bancerek
University of Białystok

Summary. The article includes definitions, lemmas and theorems 1.1–1.7, 1.9, 1.10 presented in Chapter III of [9, pp. 142–146].

MML Identifier: `WAYBEL19`.

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

1. Lower Topology

Let T be a non empty FR-structure. We say that T is lower if and only if:

(Def. 1) $\{-\uparrow x : x$ ranges over elements of $T\}$ is a prebasis of T.

Let us note that every non empty reflexive topological space-like FR-structure which is trivial is also lower.

One can verify that there exists a top-lattice which is lower, trivial, complete, and strict.

We now state the proposition

(1) For every non empty relational structure L_1 holds there exists a strict correct topological augmentation of L_1 which is lower.

We now state the proposition

(2) Let L_2, L_3 be topological space-like lower non empty FR-structures. Suppose the relational structure of L_2 = the relational structure of L_3. Then the topology of L_2 = the topology of L_3.

[1]This work has been partially supported by KBN grant 8 T11C 018 12 and NATO CRG 951368 grant.

ISSN 1426–2630

Let R be a non empty relational structure. The functor $\omega(R)$ yielding a family of subsets of R is defined by:

(Def. 2) For every lower correct topological augmentation T of R holds $\omega(R) =$ the topology of T.

Next we state a number of propositions:

(3) Let R_1, R_2 be non empty relational structures. Suppose the relational structure of $R_1 =$ the relational structure of R_2. Then $\omega(R_1) = \omega(R_2)$.

(4) For every lower non empty FR-structure T and for every point x of T holds $-\uparrow x$ is open and $\uparrow x$ is closed.

(5) For every transitive lower non empty FR-structure T and for every subset A of T such that A is open holds A is lower.

(6) For every transitive lower non empty FR-structure T and for every subset A of T such that A is closed holds A is upper.

(7) Let T be a non empty topological space-like FR-structure. Then T is lower if and only if $\{-\uparrow F; F$ ranges over subsets of T: F is finite$\}$ is a basis of T.

(8) Let S, T be lower complete top-lattices and f be a map from S into T. Suppose that for every non empty subset X of S holds f preserves inf of X. Then f is continuous.

(9) Let S, T be lower complete top-lattices and f be a map from S into T. If f is infs-preserving, then f is continuous.

(10) Let T be a lower complete top-lattice, B_1 be a prebasis of T, and F be a non empty filtered subset of T. Suppose that for every subset A of T such that $A \in B_1$ and $\inf F \in A$ holds F meets A. Then $\inf F \in \overline{F}$.

(11) Let S, T be lower complete top-lattices and f be a map from S into T. If f is continuous, then f is filtered-infs-preserving.

(12) Let S, T be lower complete top-lattices and f be a map from S into T. Suppose f is continuous and for every finite subset X of S holds f preserves inf of X. Then f is infs-preserving.

(13) Let T be a lower topological space-like reflexive transitive non empty FR-structure and x be a point of T. Then $\overline{\{x\}} = \uparrow x$.

A top-poset is a topological space-like reflexive transitive antisymmetric FR-structure.

One can check that every non empty top-poset which is lower is also T_0.

Let R be a lower-bounded non empty relational structure. One can verify that every topological augmentation of R is lower-bounded.

We now state four propositions:

(14) Let S, T be non empty relational structures, s be an element of S, and t be an element of T. Then $-\uparrow\langle s, t\rangle = [\!: -\uparrow s, \text{the carrier of } T :\!] \cup [\!: \text{the carrier of } S, -\uparrow t :\!]$.

(15) Let S, T be lower-bounded non empty posets, S' be a lower correct topological augmentation of S, and T' be a lower correct topological augmentation of T. Then $\omega([\!: S, T :\!]) =$ the topology of $[\!: S'$, (T' **qua** non empty topological space) $:\!]$.

(16) Let S, T be lower lower-bounded non empty top-posets. Then $\omega([\!: S$, (T **qua** poset) $:\!]) =$ the topology of $[\!: S$, (T **qua** non empty topological space) $:\!]$.

(17) Let T, T_2 be lower complete top-lattices. Suppose T_2 is a topological augmentation of $[\!: T$, (T **qua** lattice) $:\!]$. Let f be a map from T_2 into T. If $f = \sqcap_T$, then f is continuous.

2. Refinements Revisited

The scheme *TopInd* deals with a top-lattice $\mathcal{A}$ and and states that:

For every subset A of $\mathcal{A}$ such that A is open holds $\mathcal{P}[A]$

provided the following conditions are met:

- There exists a prebasis K of $\mathcal{A}$ such that for every subset A of $\mathcal{A}$ such that $A \in K$ holds $\mathcal{P}[A]$,
- For every family F of subsets of $\mathcal{A}$ such that for every subset A of $\mathcal{A}$ such that $A \in F$ holds $\mathcal{P}[A]$ holds $\mathcal{P}[\bigcup F]$,
- For all subsets A_1, A_2 of $\mathcal{A}$ such that $\mathcal{P}[A_1]$ and $\mathcal{P}[A_2]$ holds $\mathcal{P}[A_1 \cap A_2]$, and
- $\mathcal{P}[\Omega_{\mathcal{A}}]$.

One can prove the following proposition

(18) Let L_2, L_3 be up-complete antisymmetric non empty reflexive relational structures. Suppose that

(i) the relational structure of $L_2 =$ the relational structure of L_3, and

(ii) for every element x of L_2 holds $\Downarrow x$ is directed and non empty.

If L_2 satisfies axiom of approximation, then L_3 satisfies axiom of approximation.

Let T be a continuous non empty poset. One can verify that every topological augmentation of T is continuous.

The following propositions are true:

(19) Let T, S be topological spaces, R be a refinement of T and S, and W be a subset of R. If $W \in$ the topology of T or $W \in$ the topology of S, then W is open.

(20) Let T, S be topological spaces, R be a refinement of T and S, V be a subset of T, and W be a subset of R. If $W = V$, then if V is open, then W is open.

(21) Let T, S be topological spaces. Suppose the carrier of T = the carrier of S. Let R be a refinement of T and S, V be a subset of T, and W be a subset of R. If $W = V$, then if V is closed, then W is closed.

(22) Let T be a non empty topological space and K, O be sets such that $K \subseteq O$ and $O \subseteq$ the topology of T. Then

(i) if K is a basis of T, then O is a basis of T, and

(ii) if K is a prebasis of T, then O is a prebasis of T.

(23) Let T_1, T_2 be non empty topological spaces. Suppose the carrier of T_1 = the carrier of T_2. Let T be a refinement of T_1 and T_2, B_2 be a prebasis of T_1, and B_3 be a prebasis of T_2. Then $B_2 \cup B_3$ is a prebasis of T.

(24) Let T_1, S_1, T_2, S_2 be non empty topological spaces, R_1 be a refinement of T_1 and S_1, R_2 be a refinement of T_2 and S_2, f be a map from T_1 into T_2, g be a map from S_1 into S_2, and h be a map from R_1 into R_2. Suppose $h = f$ and $h = g$. If f is continuous and g is continuous, then h is continuous.

(25) Let T be a non empty topological space, K be a prebasis of T, N be a net in T, and p be a point of T. Suppose that for every subset A of T such that $p \in A$ and $A \in K$ holds N is eventually in A. Then $p \in \operatorname{Lim} N$.

(26) Let T be a non empty topological space, N be a net in T, and S be a subset of T. If N is eventually in S, then $\operatorname{Lim} N \subseteq \overline{S}$.

(27) Let R be a non empty relational structure and X be a non empty subset of R. Then the mapping of $\langle X; \mathrm{id} \rangle = \mathrm{id}_X$ and the mapping of $\langle X^{\mathrm{op}}; \mathrm{id} \rangle = \mathrm{id}_X$.

(28) For every reflexive antisymmetric non empty relational structure R and for every element x of R holds $\uparrow x \cap \downarrow x = \{x\}$.

3. Lawson Topology

Let T be a reflexive non empty FR-structure. We say that T is Lawson if and only if:

(Def. 3) $\omega(T) \cup \sigma(T)$ is a prebasis of T.

Next we state the proposition

(29) Let R be a complete lattice, L_1 be a lower correct topological augmentation of R, S be a Scott topological augmentation of R, and T be a correct topological augmentation of R. Then T is Lawson if and only if T is a refinement of S and L_1.

Let R be a complete lattice. One can check that there exists a topological augmentation of R which is Lawson, strict, and correct.

Let us observe that there exists a top-lattice which is Scott, complete, and strict and there exists a complete strict top-lattice which is Lawson and continuous.

We now state three propositions:

(30) For every Lawson complete top-lattice T holds $\sigma(T) \cup \{-\uparrow x : x$ ranges over elements of $T\}$ is a prebasis of T.

(31) Let T be a Lawson complete top-lattice. Then $\sigma(T) \cup \{W \setminus \uparrow x; W$ ranges over subsets of T, x ranges over elements of T: $W \in \sigma(T)\}$ is a prebasis of T.

(32) Let T be a Lawson complete top-lattice. Then $\{W \setminus \uparrow F; W$ ranges over subsets of T, F ranges over subsets of T: $W \in \sigma(T) \ \wedge \ F$ is finite$\}$ is a basis of T.

Let T be a complete lattice. The functor $\lambda(T)$ yields a family of subsets of T and is defined as follows:

(Def. 4) For every Lawson correct topological augmentation S of T holds $\lambda(T) =$ the topology of S.

We now state a number of propositions:

(33) For every complete lattice R holds $\lambda(R) = \mathrm{UniCl}(\mathrm{FinMeetCl}(\sigma(R) \cup \omega(R)))$.

(34) Let R be a complete lattice, T be a lower correct topological augmentation of R, S be a Scott correct topological augmentation of R, and M be a refinement of S and T. Then $\lambda(R) =$ the topology of M.

(35) For every lower up-complete top-lattice T and for every subset A of T such that A is open holds A has the property (S).

(36) For every Lawson complete top-lattice T and for every subset A of T such that A is open holds A has the property (S).

(37) Let S be a Scott complete top-lattice, T be a Lawson correct topological augmentation of S, and A be a subset of S. If A is open, then for every subset C of T such that $C = A$ holds C is open.

(38) Let T be a Lawson complete top-lattice and x be an element of T. Then $\uparrow x$ is closed and $\downarrow x$ is closed and $\{x\}$ is closed.

(39) For every Lawson complete top-lattice T and for every element x of T holds $-\uparrow x$ is open and $-\downarrow x$ is open and $-\{x\}$ is open.

(40) For every Lawson complete continuous top-lattice T and for every element x of T holds $\twoheaduparrow x$ is open and $-\twoheaduparrow x$ is closed.

(41) Let S be a Scott complete top-lattice, T be a Lawson correct topological augmentation of S, and A be an upper subset of T. If A is open, then for every subset C of S such that $C = A$ holds C is open.

(42) Let T be a Lawson complete top-lattice and A be a lower subset of T.

Then A is closed if and only if A is closed under directed sups.

(43) For every Lawson complete top-lattice T and for every non empty filtered subset F of T holds $\mathrm{Lim}\langle F^{\mathrm{op}}; \mathrm{id}\rangle = \{\inf F\}$.

Let us observe that every complete top-lattice which is Lawson is also T_1 and compact.

Let us observe that every complete continuous top-lattice which is Lawson is also Hausdorff.

References

[1] Grzegorz Bancerek. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.
[2] Grzegorz Bancerek. Bounds in posets and relational substructures. *Formalized Mathematics*, 6(**1**):81–91, 1997.
[3] Grzegorz Bancerek. Directed sets, nets, ideals, filters, and maps. *Formalized Mathematics*, 6(**1**):93–107, 1997.
[4] Grzegorz Bancerek. The "way-below" relation. *Formalized Mathematics*, 6(**1**):169–176, 1997.
[5] Grzegorz Bancerek. Bases and refinements of topologies. *Formalized Mathematics*, 7(**1**):35–43, 1998.
[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[8] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[9] G. Gierz, K.H. Hofmann, K. Keimel, J.D. Lawson, M. Mislove, and D.S. Scott. *A Compendium of Continuous Lattices*. Springer-Verlag, Berlin, Heidelberg, New York, 1980.
[10] Artur Korniłowicz. Cartesian products of relations and relational structures. *Formalized Mathematics*, 6(**1**):145–152, 1997.
[11] Artur Korniłowicz. Meet–continuous lattices. *Formalized Mathematics*, 6(**1**):159–167, 1997.
[12] Artur Korniłowicz. On the topological properties of meet-continuous lattices. *Formalized Mathematics*, 6(**2**):269–277, 1997.
[13] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[14] Alexander Yu. Shibakov and Andrzej Trybulec. The Cantor set. *Formalized Mathematics*, 5(**2**):233–236, 1996.
[15] Andrzej Trybulec. A Borsuk theorem on homotopy types. *Formalized Mathematics*, 2(**4**):535–545, 1991.
[16] Andrzej Trybulec. Moore-Smith convergence. *Formalized Mathematics*, 6(**2**):213–225, 1997.
[17] Andrzej Trybulec. Scott topology. *Formalized Mathematics*, 6(**2**):311–319, 1997.
[18] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[20] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

Received June 21, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Kernel Projections and Quotient Lattices

Piotr Rudnicki[1]
University of Alberta
Edmonton

Summary. This article completes the Mizar formalization of Chapter I, Section 2 from [12]. After presenting some preliminary material (not all of which is later used in this article) we give the proof of theorem 2.7 (i), p.60. We do not follow the hint from [12] suggesting using the equations 2.3, p. 58. The proof is taken directly from the definition of continuous lattice. The goal of the last section is to prove the correspondence between the set of all congruences of a continuous lattice and the set of all kernel operators of the lattice which preserve directed sups (Corollary 2.13).

MML Identifier: `WAYBEL20`.

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

1. Preliminaries

The following two propositions are true:

(1) For every set X and for every subset S of $\triangle_X$ holds $\pi_1(S) = \pi_2(S)$.

(2) For all non empty sets X, Y and for every function f from X into Y holds $[\![f, f]\!]^{-1}(\triangle_Y)$ is an equivalence relation of X.

Let L_1, L_2, T_1, T_2 be relational structures, let f be a map from L_1 into T_1, and let g be a map from L_2 into T_2. Then $[\![f, g]\!]$ is a map from $[\![L_1, L_2]\!]$ into $[\![T_1, T_2]\!]$.

One can prove the following propositions:

[1]This work was partially supported by NSERC Grant OGP9207 and NATO CRG 951368.

ISSN 1426–2630

(3) For all functions f, g and for every set X holds $\pi_1([: f, g :]^\circ X) \subseteq f^\circ \pi_1(X)$ and $\pi_2([: f, g :]^\circ X) \subseteq g^\circ \pi_2(X)$.

(4) For all functions f, g and for every set X such that $X \subseteq [: \operatorname{dom} f, \operatorname{dom} g :]$ holds $\pi_1([: f, g :]^\circ X) = f^\circ \pi_1(X)$ and $\pi_2([: f, g :]^\circ X) = g^\circ \pi_2(X)$.

(5) For every non empty antisymmetric relational structure S such that inf $\emptyset$ exists in S holds S is upper-bounded.

(6) For every non empty antisymmetric relational structure S such that sup $\emptyset$ exists in S holds S is lower-bounded.

(7) Let L_1, L_2 be antisymmetric non empty relational structures and D be a subset of $[: L_1, L_2 :]$. If inf D exists in $[: L_1, L_2 :]$, then $\inf D = \langle \inf \pi_1(D), \inf \pi_2(D) \rangle$.

(8) Let L_1, L_2 be antisymmetric non empty relational structures and D be a subset of $[: L_1, L_2 :]$. If sup D exists in $[: L_1, L_2 :]$, then $\sup D = \langle \sup \pi_1(D), \sup \pi_2(D) \rangle$.

(9) Let L_1, L_2, T_1, T_2 be antisymmetric non empty relational structures, f be a map from L_1 into T_1, and g be a map from L_2 into T_2. Suppose f is infs-preserving and g is infs-preserving. Then $[: f, g :]$ is infs-preserving.

(10) Let L_1, L_2, T_1, T_2 be antisymmetric reflexive non empty relational structures, f be a map from L_1 into T_1, and g be a map from L_2 into T_2. Suppose f is filtered-infs-preserving and g is filtered-infs-preserving. Then $[: f, g :]$ is filtered-infs-preserving.

(11) Let L_1, L_2, T_1, T_2 be antisymmetric non empty relational structures, f be a map from L_1 into T_1, and g be a map from L_2 into T_2. Suppose f is sups-preserving and g is sups-preserving. Then $[: f, g :]$ is sups-preserving.

(12) Let L_1, L_2, T_1, T_2 be antisymmetric reflexive non empty relational structures, f be a map from L_1 into T_1, and g be a map from L_2 into T_2. Suppose f is directed-sups-preserving and g is directed-sups-preserving. Then $[: f, g :]$ is directed-sups-preserving.

(13) Let L be an antisymmetric non empty relational structure and X be a subset of $[: L, L :]$. Suppose $X \subseteq \triangle_{\text{the carrier of } L}$ and inf X exists in $[: L, L :]$. Then $\inf X \in \triangle_{\text{the carrier of } L}$.

(14) Let L be an antisymmetric non empty relational structure and X be a subset of $[: L, L :]$. Suppose $X \subseteq \triangle_{\text{the carrier of } L}$ and sup X exists in $[: L, L :]$. Then $\sup X \in \triangle_{\text{the carrier of } L}$.

(15) Let L, M be non empty relational structures. If L and M are isomorphic and L is reflexive, then M is reflexive.

(16) Let L, M be non empty relational structures. If L and M are isomorphic and L is transitive, then M is transitive.

(17) Let L, M be non empty relational structures. Suppose L and M are isomorphic and L is antisymmetric. Then M is antisymmetric.

(18) Let L, M be non empty relational structures. If L and M are isomorphic and L is complete, then M is complete.

(19) Let L be a non empty transitive relational structure and k be a map from L into L. If k is infs-preserving, then k° is infs-preserving.

(20) Let L be a non empty transitive relational structure and k be a map from L into L. If k is filtered-infs-preserving, then k° is filtered-infs-preserving.

(21) Let L be a non empty transitive relational structure and k be a map from L into L. If k is sups-preserving, then k° is sups-preserving.

(22) Let L be a non empty transitive relational structure and k be a map from L into L. If k is directed-sups-preserving, then k° is directed-sups-preserving.

(23) Let S, T be reflexive antisymmetric non empty relational structures and f be a map from S into T. If f is directed-sups-preserving, then f is monotone.

(24) Let S, T be reflexive antisymmetric non empty relational structures and f be a map from S into T. If f is filtered-infs-preserving, then f is monotone.

(25) Let S, T be non empty relational structures and f be a map from S into T. Suppose f is monotone. Let X be a subset of S. If X is filtered, then $f^\circ X$ is filtered.

(26) Let L_1, L_2, L_3 be non empty relational structures, f be a map from L_1 into L_2, and g be a map from L_2 into L_3. Suppose f is infs-preserving and g is infs-preserving. Then $g \cdot f$ is infs-preserving.

(27) Let L_1, L_2, L_3 be non empty reflexive antisymmetric relational structures, f be a map from L_1 into L_2, and g be a map from L_2 into L_3. Suppose f is filtered-infs-preserving and g is filtered-infs-preserving. Then $g \cdot f$ is filtered-infs-preserving.

(28) Let L_1, L_2, L_3 be non empty relational structures, f be a map from L_1 into L_2, and g be a map from L_2 into L_3. Suppose f is sups-preserving and g is sups-preserving. Then $g \cdot f$ is sups-preserving.

(29) Let L_1, L_2, L_3 be non empty reflexive antisymmetric relational structures, f be a map from L_1 into L_2, and g be a map from L_2 into L_3. Suppose f is directed-sups-preserving and g is directed-sups-preserving. Then $g \cdot f$ is directed-sups-preserving.

2. Some Remarks on Lattice Product

We now state several propositions:

(30) Let I be a non empty set and J be a relational structure yielding non-empty many sorted set indexed by I. Suppose that for every element i of I holds $J(i)$ is a lower-bounded antisymmetric relational structure. Then $\prod J$ is lower-bounded.

(31) Let I be a non empty set and J be a relational structure yielding non-empty many sorted set indexed by I. Suppose that for every element i of I holds $J(i)$ is an upper-bounded antisymmetric relational structure. Then $\prod J$ is upper-bounded.

(32) Let I be a non empty set and J be a relational structure yielding non-empty many sorted set indexed by I. Suppose that for every element i of I holds $J(i)$ is a lower-bounded antisymmetric relational structure. Let i be an element of I. Then $\perp_{\prod J}(i) = \perp_{J(i)}$.

(33) Let I be a non empty set and J be a relational structure yielding non-empty many sorted set indexed by I. Suppose that for every element i of I holds $J(i)$ is an upper-bounded antisymmetric relational structure. Let i be an element of I. Then $\top_{\prod J}(i) = \top_{J(i)}$.

(34) Let I be a non empty set and J be a relational structure yielding non-empty reflexive-yielding many sorted set indexed by I. Suppose that for every element i of I holds $J(i)$ is a continuous complete lattice. Then $\prod J$ is continuous.

3. Kernel Projections and Quotient Lattices

We now state the proposition

(35) Let L, T be continuous complete lattices, g be a CLHomomorphism of L, T, and S be a subset of the carrier of $[\!: L, L :\!]$. Suppose $S = [\!: g, g :\!]^{-1}(\triangle_{\text{the carrier of } T})$. Then $\operatorname{sub}(S)$ is a continuous subframe of $[\!: L, L :\!]$.

Let L be a relational structure and let R be a subset of the carrier of $[\!: L, L :\!]$. Let us assume that R is an equivalence relation of the carrier of L. The functor $\operatorname{EqRel}(R)$ yields an equivalence relation of the carrier of L and is defined by:

(Def. 1) $\operatorname{EqRel}(R) = R$.

Let L be a non empty relational structure and let R be a subset of $[\!: L, L :\!]$. We say that R is a continuous lattice congruence if and only if:

(Def. 2) R is an equivalence relation of the carrier of L and $\operatorname{sub}(R)$ is a continuous subframe of $[\!: L, L :\!]$.

We now state the proposition

(36) Let L be a complete lattice and R be a non empty subset of $[\!: L, L :\!]$. Suppose R is a continuous lattice congruence. Let x be an element of the carrier of L. Then $\langle \inf([x]_{\mathrm{EqRel}(R)}), x\rangle \in R$.

Let L be a complete lattice and let R be a non empty subset of $[\!: L, L :\!]$. Let us assume that R is a continuous lattice congruence. The kernel operation of R yields a kernel map from L into L and is defined by:

(Def. 3) For every element x of L holds (the kernel operation of R)$(x) = \inf([x]_{\mathrm{EqRel}(R)})$.

Next we state three propositions:

(37) Let L be a complete lattice and R be a non empty subset of $[\!: L, L :\!]$. Suppose R is a continuous lattice congruence. Then

(i) the kernel operation of R is directed-sups-preserving, and

(ii) $R = [\!:$ the kernel operation of R, the kernel operation of $R :\!]^{-1}(\triangle_{\text{the carrier of } L})$.

(38) Let L be a continuous complete lattice, R be a subset of $[\!: L, L :\!]$, and k be a kernel map from L into L. Suppose k is directed-sups-preserving and $R = [\!: k, k :\!]^{-1}(\triangle_{\text{the carrier of } L})$. Then there exists a continuous complete strict lattice L_4 such that

(i) the carrier of $L_4 = \mathrm{Classes}\,\mathrm{EqRel}(R)$,

(ii) the internal relation of $L_4 = \{\langle [x]_{\mathrm{EqRel}(R)}, [y]_{\mathrm{EqRel}(R)}\rangle; x$ ranges over elements of L, y ranges over elements of L: $k(x) \leqslant k(y)\}$, and

(iii) for every map g from L into L_4 such that for every element x of L holds $g(x) = [x]_{\mathrm{EqRel}(R)}$ holds g is a CLHomomorphism of L, L_4.

(39) Let L be a continuous complete lattice and R be a subset of $[\!: L, L :\!]$. Suppose that

(i) R is an equivalence relation of the carrier of L, and

(ii) there exists a continuous complete lattice L_4 such that the carrier of $L_4 = \mathrm{Classes}\,\mathrm{EqRel}(R)$ and for every map g from L into L_4 such that for every element x of L holds $g(x) = [x]_{\mathrm{EqRel}(R)}$ holds g is a CLHomomorphism of L, L_4.

Then $\mathrm{sub}(R)$ is a continuous subframe of $[\!: L, L :\!]$.

Let L be a non empty reflexive relational structure. Observe that there exists a map from L into L which is directed-sups-preserving and kernel.

Let L be a non empty reflexive relational structure and let k be a kernel map from L into L. The kernel congruence of k yields a non empty subset of $[\!: L, L :\!]$ and is defined by:

(Def. 4) The kernel congruence of $k = [\!: k, k :\!]^{-1}(\triangle_{\text{the carrier of } L})$.

We now state two propositions:

(40) Let L be a non empty reflexive relational structure and k be a kernel map from L into L. Then the kernel congruence of k is an equivalence relation of the carrier of L.

(41) Let L be a continuous complete lattice and k be a directed-sups-preserving kernel map from L into L. Then the kernel congruence of k is a continuous lattice congruence.

Let L be a continuous complete lattice and let R be a non empty subset of $[\!: L, L :\!]$. Let us assume that R is a continuous lattice congruence. The functor ${}^{L}/_{R}$ yielding a continuous complete strict lattice is defined by:

(Def. 5) The carrier of ${}^{L}/_{R} = \mathrm{Classes}\,\mathrm{EqRel}(R)$ and for all elements x, y of ${}^{L}/_{R}$ holds $x \leqslant y$ iff $\bigsqcap_{L} x \leqslant \bigsqcap_{L} y$.

The following propositions are true:

(42) Let L be a continuous complete lattice and R be a non empty subset of $[\!: L, L :\!]$. Suppose R is a continuous lattice congruence. Let x be a set. Then x is an element of ${}^{L}/_{R}$ if and only if there exists an element y of L such that $x = [y]_{\mathrm{EqRel}(R)}$.

(43) Let L be a continuous complete lattice and R be a non empty subset of $[\!: L, L :\!]$. Suppose R is a continuous lattice congruence. Then $R =$ the kernel congruence of the kernel operation of R.

(44) Let L be a continuous complete lattice and k be a directed-sups-preserving kernel map from L into L. Then $k =$ the kernel operation of the kernel congruence of k.

(45) Let L be a continuous complete lattice and p be a projection map from L into L. Suppose p is infs-preserving. Then $\mathrm{Im}\, p$ is a continuous lattice and $\mathrm{Im}\, p$ is infs-inheriting.

References

[1] Grzegorz Bancerek. Curried and uncurried functions. *Formalized Mathematics*, 1(**3**):537–541, 1990.
[2] Grzegorz Bancerek. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.
[3] Grzegorz Bancerek. Bounds in posets and relational substructures. *Formalized Mathematics*, 6(**1**):81–91, 1997.
[4] Grzegorz Bancerek. Directed sets, nets, ideals, filters, and maps. *Formalized Mathematics*, 6(**1**):93–107, 1997.
[5] Grzegorz Bancerek. The "way-below" relation. *Formalized Mathematics*, 6(**1**):169–176, 1997.
[6] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.
[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[10] Czesław Byliński. Galois connections. *Formalized Mathematics*, 6(**1**):131–143, 1997.
[11] Agata Darmochwał. Families of subsets, subspaces and mappings in topological spaces. *Formalized Mathematics*, 1(**2**):257–261, 1990.

[12] G. Gierz, K.H. Hofmann, K. Keimel, J.D. Lawson, M. Mislove, and D.S. Scott. *A Compendium of Continuous Lattices.* Springer-Verlag, Berlin, Heidelberg, New York, 1980.
[13] Adam Grabowski. On the category of posets. *Formalized Mathematics*, 5(**4**):501–505, 1996.
[14] Adam Grabowski and Robert Milewski. Boolean posets, posets under inclusion and products of relational structures. *Formalized Mathematics*, 6(**1**):117–121, 1997.
[15] Artur Korniłowicz. Cartesian products of relations and relational structures. *Formalized Mathematics*, 6(**1**):145–152, 1997.
[16] Robert Milewski. Completely-irreducible elements. *Formalized Mathematics*, 7(**1**):9–12, 1998.
[17] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[18] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.
[19] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[20] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[21] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[22] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[23] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[24] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[25] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[26] Mariusz Żynel and Czesław Byliński. Properties of relational structures, posets, lattices and maps. *Formalized Mathematics*, 6(**1**):123–130, 1997.

Received July 6, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Lawson Topology in Continuous Lattices[1]

Grzegorz Bancerek
University of Białystok

Summary. The article completes Mizar formalization of Section 1 of Chapter III of [9, pp. 145–147].

MML Identifier: `WAYBEL21`.

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

1. Semilattice Homomorphism and Inheritance

Let S, T be semilattices. Let us assume that if S is upper-bounded, then T is upper-bounded. A map from S into T is said to be a semilattice morphism from S into T if:

(Def. 1) For every finite subset X of S holds it preserves inf of X.

Let S, T be semilattices. One can check that every map from S into T which is meet-preserving is also monotone.

Let S be a semilattice and let T be an upper-bounded semilattice. One can check that every semilattice morphism from S into T is meet-preserving.

Next we state a number of propositions:

(1) For all upper-bounded semilattices S, T and for every semilattice morphism f from S into T holds $f(\top_S) = \top_T$.

(2) Let S, T be semilattices and f be a map from S into T. Suppose f is meet-preserving. Let X be a finite non empty subset of S. Then f preserves inf of X.

[1]Partially supported by NATO Grant CRG 951368, NSERC OGP 9207 grant and KBN grant 8 T11C 018 12.

ISSN 1426–2630

(3) Let S, T be upper-bounded semilattices and f be a meet-preserving map from S into T. If $f(\top_S) = \top_T$, then f is a semilattice morphism from S into T.

(4) Let S, T be semilattices and f be a map from S into T. Suppose f is meet-preserving and for every filtered non empty subset X of S holds f preserves inf of X. Let X be a non empty subset of S. Then f preserves inf of X.

(5) Let S, T be semilattices and f be a map from S into T. Suppose f is infs-preserving. Then f is a semilattice morphism from S into T.

(6) Let S_1, T_1, S_2, T_2 be non empty relational structures. Suppose that
(i) the relational structure of S_1 = the relational structure of S_2, and
(ii) the relational structure of T_1 = the relational structure of T_2.
Let f_1 be a map from S_1 into T_1 and f_2 be a map from S_2 into T_2 such that $f_1 = f_2$. Then
(iii) if f_1 is infs-preserving, then f_2 is infs-preserving, and
(iv) if f_1 is directed-sups-preserving, then f_2 is directed-sups-preserving.

(7) Let S_1, T_1, S_2, T_2 be non empty relational structures. Suppose that
(i) the relational structure of S_1 = the relational structure of S_2, and
(ii) the relational structure of T_1 = the relational structure of T_2.
Let f_1 be a map from S_1 into T_1 and f_2 be a map from S_2 into T_2 such that $f_1 = f_2$. Then
(iii) if f_1 is sups-preserving, then f_2 is sups-preserving, and
(iv) if f_1 is filtered-infs-preserving, then f_2 is filtered-infs-preserving.

(8) Let T be a complete lattice and S be an infs-inheriting full non empty relational substructure of T. Then $\mathrm{incl}(S,T)$ is infs-preserving.

(9) Let T be a complete lattice and S be a sups-inheriting full non empty relational substructure of T. Then $\mathrm{incl}(S,T)$ is sups-preserving.

(10) Let T be an up-complete non empty poset and S be a directed-sups-inheriting full non empty relational substructure of T. Then $\mathrm{incl}(S,T)$ is directed-sups-preserving.

(11) Let T be a complete lattice and S be a filtered-infs-inheriting full non empty relational substructure of T. Then $\mathrm{incl}(S,T)$ is filtered-infs-preserving.

(12) Let T_1, T_2, R be relational structures and S be a relational substructure of T_1. Suppose that
(i) the relational structure of T_1 = the relational structure of T_2, and
(ii) the relational structure of S = the relational structure of R.
Then R is a relational substructure of T_2 and if S is full, then R is a full relational substructure of T_2.

(13) Every non empty relational structure T is an infs-inheriting sups-inheriting full relational substructure of T.

Let T be a complete lattice. Observe that there exists a continuous subframe of T which is complete.

We now state a number of propositions:

(14) Let T be a semilattice and S be a full non empty relational substructure of T. Then S is meet-inheriting if and only if for every finite non empty subset X of S holds $\bigsqcap_T X \in$ the carrier of S.

(15) Let T be a sup-semilattice and S be a full non empty relational substructure of T. Then S is join-inheriting if and only if for every finite non empty subset X of S holds $\bigsqcup_T X \in$ the carrier of S.

(16) Let T be an upper-bounded semilattice and S be a meet-inheriting full non empty relational substructure of T. Suppose $\top_T \in$ the carrier of S and S is filtered-infs-inheriting. Then S is infs-inheriting.

(17) Let T be a lower-bounded sup-semilattice and S be a join-inheriting full non empty relational substructure of T. Suppose $\perp_T \in$ the carrier of S and S is directed-sups-inheriting. Then S is sups-inheriting.

(18) Let T be a complete lattice and S be a full non empty relational substructure of T. If S is infs-inheriting, then S is complete.

(19) Let T be a complete lattice and S be a full non empty relational substructure of T. If S is sups-inheriting, then S is complete.

(20) Let T_1, T_2 be non empty relational structures, S_1 be a non empty full relational substructure of T_1, and S_2 be a non empty full relational substructure of T_2. Suppose that

(i) the relational structure of $T_1 =$ the relational structure of T_2, and

(ii) the carrier of $S_1 =$ the carrier of S_2.

If S_1 is infs-inheriting, then S_2 is infs-inheriting.

(21) Let T_1, T_2 be non empty relational structures, S_1 be a non empty full relational substructure of T_1, and S_2 be a non empty full relational substructure of T_2. Suppose that

(i) the relational structure of $T_1 =$ the relational structure of T_2, and

(ii) the carrier of $S_1 =$ the carrier of S_2.

If S_1 is sups-inheriting, then S_2 is sups-inheriting.

(22) Let T_1, T_2 be non empty relational structures, S_1 be a non empty full relational substructure of T_1, and S_2 be a non empty full relational substructure of T_2. Suppose that

(i) the relational structure of $T_1 =$ the relational structure of T_2, and

(ii) the carrier of $S_1 =$ the carrier of S_2.

If S_1 is directed-sups-inheriting, then S_2 is directed-sups-inheriting.

(23) Let T_1, T_2 be non empty relational structures, S_1 be a non empty full relational substructure of T_1, and S_2 be a non empty full relational substructure of T_2. Suppose that

(i) the relational structure of T_1 = the relational structure of T_2, and

(ii) the carrier of S_1 = the carrier of S_2.

If S_1 is filtered-infs-inheriting, then S_2 is filtered-infs-inheriting.

2. Nets and Limits

The following proposition is true

(24) Let S, T be non empty topological spaces, N be a net in S, and f be a map from S into T. If f is continuous, then $f^\circ \operatorname{Lim} N \subseteq \operatorname{Lim}(f \cdot N)$.

Let T be a non empty relational structure and let N be a non empty net structure over T. Let us observe that N is antitone if and only if:

(Def. 2) For all elements i, j of N such that $i \leqslant j$ holds $N(i) \geqslant N(j)$.

Let T be a non empty reflexive relational structure and let x be an element of T. Observe that $\langle \{x\}^{\mathrm{op}}; \mathrm{id} \rangle$ is transitive directed monotone and antitone.

Let T be a non empty reflexive relational structure. Note that there exists a net in T which is monotone, antitone, reflexive, and strict.

Let T be a non empty relational structure and let F be a non empty subset of T. Note that $\langle F^{\mathrm{op}}; \mathrm{id} \rangle$ is antitone.

Let S, T be non empty reflexive relational structures, let f be a monotone map from S into T, and let N be an antitone non empty net structure over S. Note that $f \cdot N$ is antitone.

We now state a number of propositions:

(25) Let S be a complete lattice and N be a net in S. Then $\{\bigsqcap_S\{N(i); i$ ranges over elements of the carrier of N: $i \geqslant j\} : j$ ranges over elements of the carrier of $N\}$ is a directed non empty subset of S.

(26) Let S be a non empty poset and N be a monotone reflexive net in S. Then $\{\bigsqcap_S\{N(i); i$ ranges over elements of the carrier of N: $i \geqslant j\} : j$ ranges over elements of the carrier of $N\}$ is a directed non empty subset of S.

(27) Let S be a non empty 1-sorted structure, N be a non empty net structure over S, and X be a set. If rng (the mapping of N) $\subseteq X$, then N is eventually in X.

(28) For every inf-complete non empty poset R and for every non empty filtered subset F of R holds $\liminf \langle F^{\mathrm{op}}; \mathrm{id} \rangle = \inf F$.

(29) Let S, T be inf-complete non empty posets, X be a non empty filtered subset of S, and f be a monotone map from S into T. Then $\liminf(f \cdot \langle X^{\mathrm{op}}; \mathrm{id}\rangle) = \inf(f^\circ X)$.

(30) Let S, T be non empty top-posets, X be a non empty filtered subset of S, f be a monotone map from S into T, and Y be a non empty filtered subset of T. If $Y = f^\circ X$, then $f \cdot \langle X^{\mathrm{op}}; \mathrm{id}\rangle$ is a subnet of $\langle Y^{\mathrm{op}}; \mathrm{id}\rangle$.

(31) Let S, T be non empty top-posets, X be a non empty filtered subset of S, f be a monotone map from S into T, and Y be a non empty filtered subset of T. If $Y = f^\circ X$, then $\mathrm{Lim}\langle Y^{\mathrm{op}}; \mathrm{id}\rangle \subseteq \mathrm{Lim}(f \cdot \langle X^{\mathrm{op}}; \mathrm{id}\rangle)$.

(32) Let S be a non empty reflexive relational structure and D be a non empty subset of S. Then the mapping of $\mathrm{NetStr}(D) = \mathrm{id}_D$ and the carrier of $\mathrm{NetStr}(D) = D$ and $\mathrm{NetStr}(D)$ is a full relational substructure of S.

(33) Let S, T be up-complete non empty posets, f be a monotone map from S into T, and D be a non empty directed subset of S. Then $\liminf(f \cdot \mathrm{NetStr}(D)) = \sup(f^\circ D)$.

(34) Let S be a non empty reflexive relational structure, D be a non empty directed subset of S, and i, j be elements of $\mathrm{NetStr}(D)$. Then $i \leqslant j$ if and only if $(\mathrm{NetStr}(D))(i) \leqslant (\mathrm{NetStr}(D))(j)$.

(35) For every Lawson complete top-lattice T and for every directed non empty subset D of T holds $\sup D \in \mathrm{Lim}\,\mathrm{NetStr}(D)$.

Let T be a non empty 1-sorted structure, let N be a net in T, and let M be a non empty net structure over T. Let us assume that M is a subnet of N. A map from M into N is said to be a embedding of M into N if it satisfies the conditions (Def. 3).

(Def. 3)(i) The mapping of $M =$ (the mapping of N) $\cdot$ it, and

(ii) for every element m of N there exists an element n of M such that for every element p of M such that $n \leqslant p$ holds $m \leqslant \mathrm{it}(p)$.

One can prove the following propositions:

(36) Let T be a non empty 1-sorted structure, N be a net in T, M be a non empty subnet of N, e be a embedding of M into N, and i be an element of M. Then $M(i) = N(e(i))$.

(37) For every complete lattice T and for every net N in T and for every subnet M of N holds $\liminf N \leqslant \liminf M$.

(38) Let T be a complete lattice, N be a net in T, M be a subnet of N, and e be a embedding of M into N. Suppose that for every element i of N and for every element j of M such that $e(j) \leqslant i$ there exists an element j' of M such that $j' \geqslant j$ and $N(i) \geqslant M(j')$. Then $\liminf N = \liminf M$.

(39) Let T be a non empty relational structure, N be a net in T, and M be a non empty full structure of a subnet of N. Suppose that for every element i of N there exists an element j of N such that $j \geqslant i$ and $j \in$ the carrier

of M. Then M is a subnet of N and $\mathrm{incl}(M, N)$ is a embedding of M into N.

(40) Let T be a non empty relational structure, N be a net in T, and i be an element of N. Then $N{\restriction}i$ is a subnet of N and $\mathrm{incl}(N{\restriction}i, N)$ is a embedding of $N{\restriction}i$ into N.

(41) For every complete lattice T and for every net N in T and for every element i of N holds $\liminf(N{\restriction}i) = \liminf N$.

(42) Let T be a non empty relational structure, N be a net in T, and X be a set. Suppose N is eventually in X. Then there exists an element i of N such that $N(i) \in X$ and $\mathrm{rng}\,(\text{the mapping of } N{\restriction}i) \subseteq X$.

(43) Let T be a Lawson complete top-lattice and N be an eventually-filtered net in T. Then $\mathrm{rng}\,(\text{the mapping of } N)$ is a filtered non empty subset of T.

(44) For every Lawson complete top-lattice T and for every eventually-filtered net N in T holds $\mathrm{Lim}\, N = \{\inf N\}$.

3. Lawson Topology Revisited

One can prove the following propositions:

(45) Let S, T be Lawson complete top-lattices and f be a meet-preserving map from S into T. Then f is continuous if and only if the following conditions are satisfied:

(i) f is directed-sups-preserving, and

(ii) for every non empty subset X of S holds f preserves inf of X.

(46) Let S, T be Lawson complete top-lattices and f be a semilattice morphism from S into T. Then f is continuous if and only if f is infs-preserving and directed-sups-preserving.

Let S, T be non empty relational structures and let f be a map from S into T. We say that f is liminfs-preserving if and only if:

(Def. 4) For every net N in S holds $f(\liminf N) = \liminf(f \cdot N)$.

One can prove the following propositions:

(47) Let S, T be Lawson complete top-lattices and f be a semilattice morphism from S into T. Then f is continuous if and only if f is liminfs-preserving.

(48) Let T be a Lawson complete continuous top-lattice and S be a meet-inheriting full non empty relational substructure of T. Suppose $\top_T \in$ the carrier of S and there exists a subset X of T such that $X =$ the carrier of S and X is closed. Then S is infs-inheriting.

(49) Let T be a Lawson complete continuous top-lattice and S be a full non empty relational substructure of T. Given a subset X of T such that $X =$ the carrier of S and X is closed. Then S is directed-sups-inheriting.

(50) Let T be a Lawson complete continuous top-lattice and S be an infs-inheriting directed-sups-inheriting full non empty relational substructure of T. Then there exists a subset X of T such that $X =$ the carrier of S and X is closed.

(51) Let T be a Lawson complete continuous top-lattice, S be an infs-inheriting directed-sups-inheriting full non empty relational substructure of T, and N be a net in T. If N is eventually in the carrier of S, then $\liminf N \in$ the carrier of S.

(52) Let T be a Lawson complete continuous top-lattice and S be a meet-inheriting full non empty relational substructure of T. Suppose that

(i) $\top_T \in$ the carrier of S, and

(ii) for every net N in T such that rng (the mapping of N) $\subseteq$ the carrier of S holds $\liminf N \in$ the carrier of S.

Then S is infs-inheriting.

(53) Let T be a Lawson complete continuous top-lattice and S be a full non empty relational substructure of T. Suppose that for every net N in T such that rng (the mapping of N) $\subseteq$ the carrier of S holds $\liminf N \in$ the carrier of S. Then S is directed-sups-inheriting.

(54) Let T be a Lawson complete continuous top-lattice, S be a meet-inheriting full non empty relational substructure of T, and X be a subset of T. Suppose $X =$ the carrier of S and $\top_T \in X$. Then X is closed if and only if for every net N in T such that N is eventually in X holds $\liminf N \in X$.

References

[1] Grzegorz Bancerek. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.
[2] Grzegorz Bancerek. Bounds in posets and relational substructures. *Formalized Mathematics*, 6(**1**):81–91, 1997.
[3] Grzegorz Bancerek. Directed sets, nets, ideals, filters, and maps. *Formalized Mathematics*, 6(**1**):93–107, 1997.
[4] Grzegorz Bancerek. The "way-below" relation. *Formalized Mathematics*, 6(**1**):169–176, 1997.
[5] Grzegorz Bancerek. Bases and refinements of topologies. *Formalized Mathematics*, 7(**1**):35–43, 1998.
[6] Grzegorz Bancerek. The Lawson topology. *Formalized Mathematics*, 7(**2**):163–168, 1998.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[9] G. Gierz, K.H. Hofmann, K. Keimel, J.D. Lawson, M. Mislove, and D.S. Scott. *A Compendium of Continuous Lattices.* Springer-Verlag, Berlin, Heidelberg, New York, 1980.
[10] Adam Grabowski. On the category of posets. *Formalized Mathematics*, 5(**4**):501–505, 1996.
[11] Adam Grabowski. Scott-continuous functions. *Formalized Mathematics*, 7(**1**):13–18, 1998.

[12] Artur Korniłowicz. On the topological properties of meet-continuous lattices. *Formalized Mathematics*, 6(**2**):269–277, 1997.
[13] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[14] Andrzej Trybulec. Moore-Smith convergence. *Formalized Mathematics*, 6(**2**):213–225, 1997.
[15] Andrzej Trybulec. Scott topology. *Formalized Mathematics*, 6(**2**):311–319, 1997.
[16] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[17] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[18] Mariusz Żynel and Czesław Byliński. Properties of relational structures, posets, lattices and maps. *Formalized Mathematics*, 6(**1**):123–130, 1997.

Received July 12, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Representation Theorem for Free Continuous Lattices

Piotr Rudnicki[1]
University of Alberta
Edmonton

Summary. We present the Mizar formalization of theorem 4.17, Chapter I from [11]: a free continuous lattice with m generators is isomorphic to the lattice of filters of 2^X ($\overline{\overline{X}} = m$) which is freely generated by $\{\uparrow x : x \in X\}$ (the set of ultrafilters).

MML Identifier: `WAYBEL22`.

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

1. Preliminaries

The following propositions are true:

(1) For every upper-bounded semilattice L and for every non empty directed subset F of $\langle \mathrm{Filt}(L), \subseteq \rangle$ holds $\sup F = \bigcup F$.

(2) Let L, S, T be complete non empty posets, f be a CLHomomorphism of L, S, and g be a CLHomomorphism of S, T. Then $g \cdot f$ is a CLHomomorphism of L, T.

(3) For every non empty relational structure L holds id_L is infs-preserving.

(4) For every non empty relational structure L holds id_L is directed-sups-preserving.

(5) For every complete non empty poset L holds id_L is a CLHomomorphism of L, L.

[1]This work was partially supported by NSERC Grant OGP9207 and NATO CRG 951368.

ISSN 1426–2630

(6) For every upper-bounded non empty poset L with g.l.b.'s holds $\langle \mathrm{Filt}(L), \subseteq \rangle$ is a continuous subframe of $2_{\subseteq}^{\text{the carrier of } L}$.

Let L be an upper-bounded non empty poset with g.l.b.'s. Observe that $\langle \mathrm{Filt}(L), \subseteq \rangle$ is continuous.

Let L be an upper-bounded non empty poset. One can check that every element of the carrier of $\langle \mathrm{Filt}(L), \subseteq \rangle$ is non empty.

2. Free Generators of Continuous Lattices

Let S be a continuous complete non empty poset and let A be a set. We say that A is a set of free generators of S if and only if the condition (Def. 1) is satisfied.

(Def. 1) Let T be a continuous complete non empty poset and f be a function from A into the carrier of T. Then there exists a CLHomomorphism h of S, T such that $h \restriction A = f$ and for every CLHomomorphism h' of S, T such that $h' \restriction A = f$ holds $h' = h$.

Next we state two propositions:

(7) Let S be a continuous complete non empty poset and A be a set. If A is a set of free generators of S, then A is a subset of S.

(8) Let S be a continuous complete non empty poset and A be a set. Suppose A is a set of free generators of S. Let h' be a CLHomomorphism of S, S. If $h' \restriction A = \mathrm{id}_A$, then $h' = \mathrm{id}_S$.

3. Representation Theorem for Free Continuous Lattices

In the sequel X is a set, F is a filter of $2_{\subseteq}^{X}$, x is an element of $2_{\subseteq}^{X}$, and z is an element of X.

Let us consider X. The fixed ultrafilters of X is a family of subsets of $2_{\subseteq}^{X}$ and is defined as follows:

(Def. 2) The fixed ultrafilters of $X = \{\uparrow x : \bigvee_z \; x = \{z\}\}$.

One can prove the following three propositions:

(9) The fixed ultrafilters of $X \subseteq \mathrm{Filt}(2_{\subseteq}^{X})$.

(10) $\overline{\overline{\text{the fixed ultrafilters of } X}} = \overline{\overline{X}}$.

(11) $F = \bigsqcup_{(\langle \mathrm{Filt}(2_{\subseteq}^{X}), \subseteq \rangle)} \{ \bigsqcap_{(\langle \mathrm{Filt}(2_{\subseteq}^{X}), \subseteq \rangle)} \{\uparrow x : \bigvee_z \; (x = \{z\} \land z \in Y)\}; Y$ ranges over subsets of X: $Y \in F\}$.

Let us consider X, let L be a continuous complete non empty poset, and let f be a function from the fixed ultrafilters of X into the carrier of L. The extension of f to homomorphism is a map from $\langle \mathrm{Filt}(2^X_\subseteq), \subseteq\rangle$ into L and is defined by the condition (Def. 3).

(Def. 3) Let F_1 be an element of the carrier of $(\langle \mathrm{Filt}(2^X_\subseteq), \subseteq\rangle)$. Then (the extension of f to homomorphism)$(F_1) = \bigsqcup_L \{\bigsqcap_L \{f(\uparrow x) : \bigvee_z\ (x = \{z\}\ \wedge\ z \in Y)\}; Y$ ranges over subsets of X: $Y \in F_1\}$.

One can prove the following propositions:

(12) Let L be a continuous complete non empty poset and f be a function from the fixed ultrafilters of X into the carrier of L. Then the extension of f to homomorphism is monotone.

(13) Let L be a continuous complete non empty poset and f be a function from the fixed ultrafilters of X into the carrier of L. Then (the extension of f to homomorphism)$(\top_{\langle \mathrm{Filt}(2^X_\subseteq), \subseteq\rangle}) = \top_L$.

Let us consider X, let L be a continuous complete non empty poset, and let f be a function from the fixed ultrafilters of X into the carrier of L. Observe that the extension of f to homomorphism is directed-sups-preserving.

Let us consider X, let L be a continuous complete non empty poset, and let f be a function from the fixed ultrafilters of X into the carrier of L. Note that the extension of f to homomorphism is infs-preserving.

The following propositions are true:

(14) Let L be a continuous complete non empty poset and f be a function from the fixed ultrafilters of X into the carrier of L. Then (the extension of f to homomorphism)$\restriction$(the fixed ultrafilters of X) $= f$.

(15) Let L be a continuous complete non empty poset, f be a function from the fixed ultrafilters of X into the carrier of L, and h be a CLHomomorphism of $\langle \mathrm{Filt}(2^X_\subseteq), \subseteq\rangle$, L. Suppose $h\restriction$the fixed ultrafilters of $X = f$. Then $h =$ the extension of f to homomorphism.

(16) The fixed ultrafilters of X is a set of free generators of $\langle \mathrm{Filt}(2^X_\subseteq), \subseteq\rangle$.

(17) Let L, M be continuous complete lattices and F, G be sets. Suppose F is a set of free generators of L and G is a set of free generators of M and $\overline{\overline{F}} = \overline{\overline{G}}$. Then L and M are isomorphic.

(18) Let L be a continuous complete lattice and G be a set. Suppose G is a set of free generators of L and $\overline{\overline{G}} = \overline{\overline{X}}$. Then L and $\langle \mathrm{Filt}(2^X_\subseteq), \subseteq\rangle$ are isomorphic.

References

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

[2] Grzegorz Bancerek. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.

[3] Grzegorz Bancerek. Bounds in posets and relational substructures. *Formalized Mathematics*, 6(**1**):81–91, 1997.

[4] Grzegorz Bancerek. Directed sets, nets, ideals, filters, and maps. *Formalized Mathematics*, 6(**1**):93–107, 1997.

[5] Grzegorz Bancerek. The "way-below" relation. *Formalized Mathematics*, 6(**1**):169–176, 1997.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Galois connections. *Formalized Mathematics*, 6(**1**):131–143, 1997.
[9] Agata Darmochwał. Families of subsets, subspaces and mappings in topological spaces. *Formalized Mathematics*, 1(**2**):257–261, 1990.
[10] Mariusz Giero. More on products of many sorted algebras. *Formalized Mathematics*, 5(**4**):621–626, 1996.
[11] G. Gierz, K.H. Hofmann, K. Keimel, J.D. Lawson, M. Mislove, and D.S. Scott. *A Compendium of Continuous Lattices*. Springer-Verlag, Berlin, Heidelberg, New York, 1980.
[12] Adam Grabowski. On the category of posets. *Formalized Mathematics*, 5(**4**):501–505, 1996.
[13] Adam Grabowski and Robert Milewski. Boolean posets, posets under inclusion and products of relational structures. *Formalized Mathematics*, 6(**1**):117–121, 1997.
[14] Robert Milewski. Completely-irreducible elements. *Formalized Mathematics*, 7(**1**):9–12, 1998.
[15] Michał Muzalewski. Categories of groups. *Formalized Mathematics*, 2(**4**):563–571, 1991.
[16] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[17] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[18] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[19] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[20] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received July 21, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Oriented Chains

Yatsuka Nakamura
Shinshu University
Nagano

Piotr Rudnicki
University of Alberta
Edmonton

Summary. In [5] we introduced a number of notions about vertex sequences associated with undirected chains of edges in graphs. In this article, we introduce analogous concepts for oriented chains and use them to prove properties of cutting and glueing of oriented chains, and the existence of a simple oriented chain in an oriented chain.

MML Identifier: `GRAPH_4`.

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

1. Oriented Vertex Sequences

For simplicity, we adopt the following rules: p, q denote finite sequences, m, n denote natural numbers, G denotes a graph, x, y, v, v_1, v_2, v_3, v_4 denote elements of the vertices of G, e denotes a set, and X denotes a set.

Let us consider G, let us consider x, y, and let us consider e. We say that e orientedly joins x, y if and only if:

(Def. 1) (The source of $G)(e) = x$ and (the target of $G)(e) = y$.

We now state the proposition

(1) If e orientedly joins v_1, v_2, then e joins v_1 with v_2.

Let us consider G and let x, y be elements of the vertices of G. We say that x, y are orientedly incident if and only if:

(Def. 2) There exists a set v such that $v \in$ the edges of G and v orientedly joins x, y.

ISSN 1426–2630

One can prove the following proposition

(2) If e orientedly joins v_1, v_2 and e orientedly joins v_3, v_4, then $v_1 = v_3$ and $v_2 = v_4$.

We follow the rules: v_5, v_6, v_7 are finite sequences of elements of the vertices of G and c, c_1, c_2 are oriented chains of G.

We now state the proposition

(3) ε is an oriented chain of G.

Let us consider G. Observe that there exists a chain of G which is empty and oriented.

Let us consider G, X. The functor G-SVSet X yields a set and is defined by:

(Def. 3) $G\text{-SVSet}\,X = \{v : \bigvee_{e:\text{element of the edges of } G} (e \in X \ \wedge\ v = (\text{the source of } G)(e))\}$.

Let us consider G, X. The functor G-TVSet X yielding a set is defined by:

(Def. 4) $G\text{-TVSet}\,X = \{v : \bigvee_{e:\text{element of the edges of } G} (e \in X \ \wedge\ v = (\text{the target of } G)(e))\}$.

Next we state the proposition

(4) If $X = \emptyset$, then $G\text{-SVSet}\,X = \emptyset$ and $G\text{-TVSet}\,X = \emptyset$.

Let us consider G, v_5 and let c be a finite sequence. We say that v_5 is oriented vertex seq of c if and only if:

(Def. 5) $\operatorname{len} v_5 = \operatorname{len} c + 1$ and for every n such that $1 \leqslant n$ and $n \leqslant \operatorname{len} c$ holds $c(n)$ orientedly joins $\pi_n v_5$, $\pi_{n+1} v_5$.

One can prove the following propositions:

(5) If v_5 is oriented vertex seq of c, then v_5 is vertex sequence of c.

(6) If v_5 is oriented vertex seq of c, then $G\text{-SVSet}\operatorname{rng} c \subseteq \operatorname{rng} v_5$.

(7) If v_5 is oriented vertex seq of c, then $G\text{-TVSet}\operatorname{rng} c \subseteq \operatorname{rng} v_5$.

(8) If $c \neq \varepsilon$ and v_5 is oriented vertex seq of c, then $\operatorname{rng} v_5 \subseteq (G\text{-SVSet}\operatorname{rng} c) \cup (G\text{-TVSet}\operatorname{rng} c)$.

2. Cutting and Glueing of Oriented Chains

One can prove the following propositions:

(9) $\langle v \rangle$ is oriented vertex seq of ε.

(10) There exists v_5 such that v_5 is oriented vertex seq of c.

(11) If $c \neq \varepsilon$ and v_6 is oriented vertex seq of c and v_7 is oriented vertex seq of c, then $v_6 = v_7$.

Let us consider G, c. Let us assume that $c \neq \varepsilon$. The functor oriented-vertex-seq c yielding a finite sequence of elements of the vertices of G is defined as follows:

(Def. 6) oriented-vertex-seq c is oriented vertex seq of c.

Next we state several propositions:

(12) If v_5 is oriented vertex seq of c and $c_1 = c \restriction \operatorname{Seg} n$ and $v_6 = v_5 \restriction \operatorname{Seg}(n+1)$, then v_6 is oriented vertex seq of c_1.

(13) If $1 \leqslant m$ and $m \leqslant n$ and $n \leqslant \operatorname{len} c$ and $q = \langle c(m), \ldots, c(n) \rangle$, then q is an oriented chain of G.

(14) Suppose $1 \leqslant m$ and $m \leqslant n$ and $n \leqslant \operatorname{len} c$ and $c_1 = \langle c(m), \ldots, c(n) \rangle$ and v_5 is oriented vertex seq of c and $v_6 = \langle v_5(m), \ldots, v_5(n+1) \rangle$. Then v_6 is oriented vertex seq of c_1.

(15) Suppose v_6 is oriented vertex seq of c_1 and v_7 is oriented vertex seq of c_2 and $v_6(\operatorname{len} v_6) = v_7(1)$. Then $c_1 \frown c_2$ is an oriented chain of G.

(16) Suppose v_6 is oriented vertex seq of c_1 and v_7 is oriented vertex seq of c_2 and $v_6(\operatorname{len} v_6) = v_7(1)$ and $c = c_1 \frown c_2$ and $v_5 = v_6 \frown\!\frown v_7$. Then v_5 is oriented vertex seq of c.

3. Oriented Simple Chains in Oriented Chains

Let us consider G and let I_1 be an oriented chain of G. We say that I_1 is Simple if and only if the condition (Def. 7) is satisfied.

(Def. 7) There exists v_5 such that v_5 is oriented vertex seq of I_1 and for all n, m such that $1 \leqslant n$ and $n < m$ and $m \leqslant \operatorname{len} v_5$ and $v_5(n) = v_5(m)$ holds $n = 1$ and $m = \operatorname{len} v_5$.

Let us consider G. Note that there exists an oriented chain of G which is Simple.

Let us consider G. One can verify that there exists a chain of G which is oriented and simple.

Next we state two propositions:

(17) Every oriented simple chain of G is an oriented chain of G.

(18) For every oriented chain q of G holds $q \restriction \operatorname{Seg} n$ is an oriented chain of G.

In the sequel s_1 is an oriented simple chain of G.

Next we state several propositions:

(19) $s_1 \restriction \operatorname{Seg} n$ is an oriented simple chain of G.

(20) For every oriented chain s'_1 of G such that $s'_1 = s_1$ holds s'_1 is Simple.

(21) Every Simple oriented chain of G is an oriented simple chain of G.

(22) Suppose c is not Simple and v_5 is oriented vertex seq of c. Then there exists a FinSubsequence f_1 of c and there exists a FinSubsequence f_2 of v_5 and there exist c_1, v_6 such that $\operatorname{len} c_1 < \operatorname{len} c$ and v_6 is oriented vertex seq of c_1 and $\operatorname{len} v_6 < \operatorname{len} v_5$ and $v_5(1) = v_6(1)$ and $v_5(\operatorname{len} v_5) = v_6(\operatorname{len} v_6)$ and $\operatorname{Seq} f_1 = c_1$ and $\operatorname{Seq} f_2 = v_6$.

(23) Suppose v_5 is oriented vertex seq of c. Then there exists a FinSubsequence f_1 of c and there exists a FinSubsequence f_2 of v_5 and there exist s_1, v_6 such that $\operatorname{Seq} f_1 = s_1$ and $\operatorname{Seq} f_2 = v_6$ and v_6 is oriented vertex seq of s_1 and $v_5(1) = v_6(1)$ and $v_5(\operatorname{len} v_5) = v_6(\operatorname{len} v_6)$.

Let us consider G. Observe that every oriented chain of G which is empty is also oriented.

Next we state three propositions:

(24) If p is an oriented path of G, then $p \restriction \operatorname{Seg} n$ is an oriented path of G.

(25) s_1 is an oriented path of G.

(26) Let c_1 be a finite sequence. Then
- (i) c_1 is a Simple oriented chain of G iff c_1 is an oriented simple chain of G, and
- (ii) if c_1 is an oriented simple chain of G, then c_1 is an oriented path of G.

References

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

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

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

[4] Krzysztof Hryniewiecki. Graphs. *Formalized Mathematics*, 2(**3**):365–370, 1991.

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

[6] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

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

[8] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

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

Received August 19, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Graph Theoretical Properties of Arcs in the Plane and Fashoda Meet Theorem

Yatsuka Nakamura
Shinshu University
Nagano

Summary. We define a graph on an abstract set, edges of which are pairs of any two elements. For any finite sequence of a plane, we give a definition of nodic, which means that edges by a finite sequence are crossed only at terminals. If the first point and the last point of a finite sequence differs, simpleness as a chain and nodic condition imply unfoldedness and s.n.c. condition. We generalize Goboard Theorem, proved by us before, to a continuous case. We call this Fashoda Meet Theorem, which was taken from Fashoda incident of 100 years ago.

MML Identifier: JGRAPH_1.

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

1. A Graph by Cartesian Product

For simplicity, we adopt the following convention: G denotes a graph, v_1 denotes a finite sequence of elements of the vertices of G, I_1 denotes an oriented chain of G, n, m, k, i, j denote natural numbers, and r, r_1, r_2 denote real numbers.

Next we state four propositions:

(1) $\frac{0}{r} = 0$.

(2) $\sqrt{{r_1}^{\mathbf{2}} + {r_2}^{\mathbf{2}}} \leqslant |r_1| + |r_2|$.

(3) $|r_1| \leqslant \sqrt{{r_1}^{\mathbf{2}} + {r_2}^{\mathbf{2}}}$ and $|r_2| \leqslant \sqrt{{r_1}^{\mathbf{2}} + {r_2}^{\mathbf{2}}}$.

ISSN 1426–2630

(4) Let given v_1. Suppose I_1 is Simple and v_1 is oriented vertex seq of I_1. Let given n, m. If $1 \leqslant n$ and $n < m$ and $m \leqslant \operatorname{len} v_1$ and $v_1(n) = v_1(m)$, then $n = 1$ and $m = \operatorname{len} v_1$.

Let X be a set. The functor PGraph X yields a multi graph structure and is defined by:

(Def. 1) $\mathrm{PGraph}\, X = \langle X, [\!:X, X:\!], \pi_1(X \times X), \pi_2(X \times X)\rangle$.

We now state two propositions:

(5) For every non empty set X holds PGraph X is a graph.

(6) For every non empty set X holds the vertices of $\mathrm{PGraph}\, X = X$.

Let f be a finite sequence. The functor PairF f yielding a finite sequence is defined by:

(Def. 2) $\operatorname{len} \mathrm{PairF}\, f = \operatorname{len} f -' 1$ and for every natural number i such that $1 \leqslant i$ and $i < \operatorname{len} f$ holds $(\mathrm{PairF}\, f)(i) = \langle f(i),\ f(i+1)\rangle$.

In the sequel X is a non empty set.

Let X be a non empty set. Then PGraph X is a graph.

The following propositions are true:

(7) Every finite sequence of elements of X is a finite sequence of elements of the vertices of PGraph X.

(8) For every finite sequence f of elements of X holds PairF f is a finite sequence of elements of the edges of PGraph X.

Let X be a non empty set and let f be a finite sequence of elements of X. Then PairF f is a finite sequence of elements of the edges of PGraph X.

We now state two propositions:

(9) Let n be a natural number and f be a finite sequence of elements of X. If $1 \leqslant n$ and $n \leqslant \operatorname{len} \mathrm{PairF}\, f$, then $(\mathrm{PairF}\, f)(n) \in$ the edges of PGraph X.

(10) For every finite sequence f of elements of X holds PairF f is an oriented chain of PGraph X.

Let X be a non empty set and let f be a finite sequence of elements of X. Then PairF f is an oriented chain of PGraph X.

The following proposition is true

(11) Let f be a finite sequence of elements of X and f_1 be a finite sequence of elements of the vertices of PGraph X. If $\operatorname{len} f \geqslant 1$ and $f = f_1$, then f_1 is oriented vertex seq of PairF f.

2. Shortcuts of Finite Sequences in Plane

Let X be a non empty set and let f, g be finite sequences of elements of X. We say that g is Shortcut of f if and only if the conditions (Def. 3) are satisfied.

(Def. 3)(i) $f(1) = g(1)$,

(ii) $f(\operatorname{len} f) = g(\operatorname{len} g)$, and

(iii) there exists a FinSubsequence f_2 of PairF f and there exists a FinSubsequence f_3 of f and there exists an oriented simple chain s_1 of PGraph X and there exists a finite sequence g_1 of elements of the vertices of PGraph X such that Seq $f_2 = s_1$ and Seq $f_3 = g$ and $g_1 = g$ and g_1 is oriented vertex seq of s_1.

We now state four propositions:

(12) For all finite sequences f, g of elements of X such that g is Shortcut of f holds $1 \leqslant \operatorname{len} g$ and $\operatorname{len} g \leqslant \operatorname{len} f$.

(13) Let f be a finite sequence of elements of X. Suppose $\operatorname{len} f \geqslant 1$. Then there exists a finite sequence g of elements of X such that g is Shortcut of f.

(14) For all finite sequences f, g of elements of X such that g is Shortcut of f holds rng PairF $g \subseteq$ rng PairF f.

(15) Let f, g be finite sequences of elements of X. Suppose $f(1) \neq f(\operatorname{len} f)$ and g is Shortcut of f. Then g is one-to-one and rng PairF $g \subseteq$ rng PairF f and $g(1) = f(1)$ and $g(\operatorname{len} g) = f(\operatorname{len} f)$.

Let us consider n and let I_1 be a finite sequence of elements of $\mathcal{E}^n_{\mathrm{T}}$. We say that I_1 is nodic if and only if the condition (Def. 4) is satisfied.

(Def. 4) Let given i, j. Suppose $\mathcal{L}(I_1, i) \cap \mathcal{L}(I_1, j) \neq \emptyset$. Then $\mathcal{L}(I_1, i) \cap \mathcal{L}(I_1, j) = \{I_1(i)\}$ but $I_1(i) = I_1(j)$ or $I_1(i) = I_1(j + 1)$ or $\mathcal{L}(I_1, i) \cap \mathcal{L}(I_1, j) = \{I_1(i+1)\}$ but $I_1(i+1) = I_1(j)$ or $I_1(i+1) = I_1(j+1)$ or $\mathcal{L}(I_1, i) = \mathcal{L}(I_1, j)$.

One can prove the following propositions:

(16) For every finite sequence f of elements of $\mathcal{E}^2_{\mathrm{T}}$ such that f is s.n.c. holds f is s.c.c..

(17) For every finite sequence f of elements of $\mathcal{E}^2_{\mathrm{T}}$ such that f is s.c.c. and $\mathcal{L}(f, 1) \cap \mathcal{L}(f, \operatorname{len} f -' 1) = \emptyset$ holds f is s.n.c..

(18) For every finite sequence f of elements of $\mathcal{E}^2_{\mathrm{T}}$ such that f is nodic and PairF f is Simple holds f is s.c.c..

(19) For every finite sequence f of elements of $\mathcal{E}^2_{\mathrm{T}}$ such that f is nodic and PairF f is Simple and $f(1) \neq f(\operatorname{len} f)$ holds f is s.n.c..

(20) For all points p_1, p_2, p_3 of $\mathcal{E}^n_{\mathrm{T}}$ such that there exists a set x such that $x \neq p_2$ and $x \in \mathcal{L}(p_1, p_2) \cap \mathcal{L}(p_2, p_3)$ holds $p_1 \in \mathcal{L}(p_2, p_3)$ or $p_3 \in \mathcal{L}(p_1, p_2)$.

(21) Let f be a finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$. Suppose f is s.n.c. and $\mathcal{L}(f, 1) \cap \mathcal{L}(f, 1 + 1) \subseteq \{\pi_{1+1} f\}$ and $\mathcal{L}(f, \operatorname{len} f -' 2) \cap \mathcal{L}(f, \operatorname{len} f -' 1) \subseteq \{\pi_{\operatorname{len} f -' 1} f\}$. Then f is unfolded.

(22) For every finite sequence f of elements of X such that PairF f is Simple and $f(1) \neq f(\operatorname{len} f)$ holds f is one-to-one and $\operatorname{len} f \neq 1$.

(23) For every finite sequence f of elements of X such that f is one-to-one and $\operatorname{len} f > 1$ holds PairF f is Simple and $f(1) \neq f(\operatorname{len} f)$.

(24) Let f be a finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$. If f is nodic and PairF f is Simple and $f(1) \neq f(\operatorname{len} f)$, then f is unfolded.

(25) Let f, g be finite sequences of elements of $\mathcal{E}^2_{\mathrm{T}}$ and given i. Suppose g is Shortcut of f and $1 \leqslant i$ and $i + 1 \leqslant \operatorname{len} g$. Then there exists a natural number k_1 such that $1 \leqslant k_1$ and $k_1 + 1 \leqslant \operatorname{len} f$ and $\pi_{k_1} f = \pi_i g$ and $\pi_{k_1+1} f = \pi_{i+1} g$ and $f(k_1) = g(i)$ and $f(k_1 + 1) = g(i + 1)$.

(26) For all finite sequences f, g of elements of $\mathcal{E}^2_{\mathrm{T}}$ such that g is Shortcut of f holds $\operatorname{rng} g \subseteq \operatorname{rng} f$.

(27) For all finite sequences f, g of elements of $\mathcal{E}^2_{\mathrm{T}}$ such that g is Shortcut of f holds $\widetilde{\mathcal{L}}(g) \subseteq \widetilde{\mathcal{L}}(f)$.

(28) Let f, g be finite sequences of elements of $\mathcal{E}^2_{\mathrm{T}}$. If f is special and g is Shortcut of f, then g is special.

(29) Let f be a finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$. Suppose f is special and $2 \leqslant \operatorname{len} f$ and $f(1) \neq f(\operatorname{len} f)$. Then there exists a finite sequence g of elements of $\mathcal{E}^2_{\mathrm{T}}$ such that $2 \leqslant \operatorname{len} g$ and g is special and one-to-one and $\widetilde{\mathcal{L}}(g) \subseteq \widetilde{\mathcal{L}}(f)$ and $f(1) = g(1)$ and $f(\operatorname{len} f) = g(\operatorname{len} g)$ and $\operatorname{rng} g \subseteq \operatorname{rng} f$.

(30) Let f_1, f_4 be finite sequences of elements of $\mathcal{E}^2_{\mathrm{T}}$. Suppose that

(i) f_1 is special,

(ii) f_4 is special,

(iii) $2 \leqslant \operatorname{len} f_1$,

(iv) $2 \leqslant \operatorname{len} f_4$,

(v) $f_1(1) \neq f_1(\operatorname{len} f_1)$,

(vi) $f_4(1) \neq f_4(\operatorname{len} f_4)$,

(vii) **X**-coordinate(f_1) lies between $(\mathbf{X}\text{-coordinate}(f_1))(1)$ and $(\mathbf{X}\text{-coordinate}(f_1))(\operatorname{len} f_1)$,

(viii) **X**-coordinate(f_4) lies between $(\mathbf{X}\text{-coordinate}(f_1))(1)$ and $(\mathbf{X}\text{-coordinate}(f_1))(\operatorname{len} f_1)$,

(ix) **Y**-coordinate(f_1) lies between $(\mathbf{Y}\text{-coordinate}(f_4))(1)$ and $(\mathbf{Y}\text{-coordinate}(f_4))(\operatorname{len} f_4)$, and

(x) **Y**-coordinate(f_4) lies between $(\mathbf{Y}\text{-coordinate}(f_4))(1)$ and $(\mathbf{Y}\text{-coordinate}(f_4))(\operatorname{len} f_4)$.

Then $\widetilde{\mathcal{L}}(f_1) \cap \widetilde{\mathcal{L}}(f_4) \neq \emptyset$.

3. Norm of Points in $\mathcal{E}^n_{\mathrm{T}}$

The following proposition is true

(31) For all real numbers a, b, r_1, r_2 such that $a \leqslant r_1$ and $r_1 \leqslant b$ and $a \leqslant r_2$ and $r_2 \leqslant b$ holds $|r_1 - r_2| \leqslant b - a$.

Let us consider n and let p be a point of $\mathcal{E}^n_{\mathrm{T}}$. The functor $|p|$ yields a real number and is defined by:

(Def. 5) For every element w of $\mathcal{R}^n$ such that $p = w$ holds $|p| = |w|$.

In the sequel p, p_1, p_2 are points of $\mathcal{E}^n_{\mathrm{T}}$.

We now state a number of propositions:

(32) $|0_{\mathcal{E}^n_{\mathrm{T}}}| = 0$.

(33) If $|p| = 0$, then $p = 0_{\mathcal{E}^n_{\mathrm{T}}}$.

(34) $|p| \geqslant 0$.

(35) $|-p| = |p|$.

(36) $|r \cdot p| = |r| \cdot |p|$.

(37) $|p_1 + p_2| \leqslant |p_1| + |p_2|$.

(38) $|p_1 - p_2| \leqslant |p_1| + |p_2|$.

(39) $|p_1| - |p_2| \leqslant |p_1 + p_2|$.

(40) $|p_1| - |p_2| \leqslant |p_1 - p_2|$.

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

(42) If $p_1 \neq p_2$, then $|p_1 - p_2| > 0$.

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

(44) $|p_1 - p_2| \leqslant |p_1 - p| + |p - p_2|$.

(45) For all points x_1, x_2 of $\mathcal{E}^n$ such that $x_1 = p_1$ and $x_2 = p_2$ holds $|p_1 - p_2| = \rho(x_1, x_2)$.

(46) For every point p of $\mathcal{E}^2_{\mathrm{T}}$ holds $|p|^{\mathbf{2}} = |p_{\mathbf{1}}|^{\mathbf{2}} + |p_{\mathbf{2}}|^{\mathbf{2}}$.

(47) For every point p of $\mathcal{E}^2_{\mathrm{T}}$ holds $|p| = \sqrt{|p_{\mathbf{1}}|^{\mathbf{2}} + |p_{\mathbf{2}}|^{\mathbf{2}}}$.

(48) For every point p of $\mathcal{E}^2_{\mathrm{T}}$ holds $|p| \leqslant |p_{\mathbf{1}}| + |p_{\mathbf{2}}|$.

(49) For all points p_1, p_2 of $\mathcal{E}^2_{\mathrm{T}}$ holds $|p_1 - p_2| \leqslant |(p_1)_{\mathbf{1}} - (p_2)_{\mathbf{1}}| + |(p_1)_{\mathbf{2}} - (p_2)_{\mathbf{2}}|$.

(50) For every point p of $\mathcal{E}^2_{\mathrm{T}}$ holds $|p_{\mathbf{1}}| \leqslant |p|$ and $|p_{\mathbf{2}}| \leqslant |p|$.

(51) For all points p_1, p_2 of $\mathcal{E}^2_{\mathrm{T}}$ holds $|(p_1)_{\mathbf{1}} - (p_2)_{\mathbf{1}}| \leqslant |p_1 - p_2|$ and $|(p_1)_{\mathbf{2}} - (p_2)_{\mathbf{2}}| \leqslant |p_1 - p_2|$.

(52) If $p \in \mathcal{L}(p_1, p_2)$, then there exists r such that $0 \leqslant r$ and $r \leqslant 1$ and $p = (1 - r) \cdot p_1 + r \cdot p_2$.

(53) If $p \in \mathcal{L}(p_1, p_2)$, then $|p - p_1| \leqslant |p_1 - p_2|$ and $|p - p_2| \leqslant |p_1 - p_2|$.

4. Extended Goboard Theorem and Fashoda Meet Theorem

In the sequel M denotes a metric space.

Next we state several propositions:

(54) For all subsets P, Q of $M_{\rm top}$ such that $P \neq \emptyset$ and P is compact and $Q \neq \emptyset$ and Q is compact holds $\mathrm{dist}_{\min}^{\min}(P, Q) \geqslant 0$.

(55) Let P, Q be subsets of $M_{\rm top}$. Suppose $P \neq \emptyset$ and P is compact and $Q \neq \emptyset$ and Q is compact. Then $P \cap Q = \emptyset$ if and only if $\mathrm{dist}_{\min}^{\min}(P, Q) > 0$.

(56) Let f be a finite sequence of elements of $\mathcal{E}^2_{\rm T}$ and a, c, d be real numbers. Suppose that

(i) $1 \leqslant \mathrm{len}\, f$,

(ii) **X**-coordinate(f) lies between $(\mathbf{X}\text{-coordinate}(f))(1)$ and $(\mathbf{X}\text{-coordinate}(f))(\mathrm{len}\, f)$,

(iii) **Y**-coordinate(f) lies between c and d,

(iv) $a > 0$, and

(v) for every i such that $1 \leqslant i$ and $i + 1 \leqslant \mathrm{len}\, f$ holds $|\pi_i f - \pi_{i+1} f| < a$.

Then there exists a finite sequence g of elements of $\mathcal{E}^2_{\rm T}$ such that

(vi) g is special,

(vii) $g(1) = f(1)$,

(viii) $g(\mathrm{len}\, g) = f(\mathrm{len}\, f)$,

(ix) $\mathrm{len}\, g \geqslant \mathrm{len}\, f$,

(x) **X**-coordinate(g) lies between $(\mathbf{X}\text{-coordinate}(f))(1)$ and $(\mathbf{X}\text{-coordinate}(f))(\mathrm{len}\, f)$,

(xi) **Y**-coordinate(g) lies between c and d,

(xii) for every j such that $j \in \mathrm{dom}\, g$ there exists k such that $k \in \mathrm{dom}\, f$ and $|\pi_j g - \pi_k f| < a$, and

(xiii) for every j such that $1 \leqslant j$ and $j + 1 \leqslant \mathrm{len}\, g$ holds $|\pi_j g - \pi_{j+1} g| < a$.

(57) Let f be a finite sequence of elements of $\mathcal{E}^2_{\rm T}$ and a, c, d be real numbers. Suppose that

(i) $1 \leqslant \mathrm{len}\, f$,

(ii) **Y**-coordinate(f) lies between $(\mathbf{Y}\text{-coordinate}(f))(1)$ and $(\mathbf{Y}\text{-coordinate}(f))(\mathrm{len}\, f)$,

(iii) **X**-coordinate(f) lies between c and d,

(iv) $a > 0$, and

(v) for every i such that $1 \leqslant i$ and $i + 1 \leqslant \mathrm{len}\, f$ holds $|\pi_i f - \pi_{i+1} f| < a$.

Then there exists a finite sequence g of elements of $\mathcal{E}^2_{\rm T}$ such that

(vi) g is special,

(vii) $g(1) = f(1)$,

(viii) $g(\mathrm{len}\, g) = f(\mathrm{len}\, f)$,

(ix) $\mathrm{len}\, g \geqslant \mathrm{len}\, f$,

(x) **Y**-coordinate(g) lies between (**Y**-coordinate(f))(1) and (**Y**-coordinate(f))(len f),

(xi) **X**-coordinate(g) lies between c and d,

(xii) for every j such that $j \in \operatorname{dom} g$ there exists k such that $k \in \operatorname{dom} f$ and $|\pi_j g - \pi_k f| < a$, and

(xiii) for every j such that $1 \leqslant j$ and $j + 1 \leqslant \operatorname{len} g$ holds $|\pi_j g - \pi_{j+1} g| < a$.

(58) For every subset P of the carrier of $\mathcal{E}^2_{\mathrm{T}}$ and for all points p_1, p_2 of $\mathcal{E}^2_{\mathrm{T}}$ such that P is an arc from p_1 to p_2 holds $p_1 \neq p_2$.

(59) For every finite sequence f of elements of $\mathcal{E}^2_{\mathrm{T}}$ such that $1 \leqslant \operatorname{len} f$ holds len **X**-coordinate(f) = len f and (**X**-coordinate(f))(1) = $(\pi_1 f)_{\mathbf{1}}$ and (**X**-coordinate(f))(len f) = $(\pi_{\operatorname{len} f} f)_{\mathbf{1}}$.

(60) For every finite sequence f of elements of $\mathcal{E}^2_{\mathrm{T}}$ such that $1 \leqslant \operatorname{len} f$ holds len **Y**-coordinate(f) = len f and (**Y**-coordinate(f))(1) = $(\pi_1 f)_{\mathbf{2}}$ and (**Y**-coordinate(f))(len f) = $(\pi_{\operatorname{len} f} f)_{\mathbf{2}}$.

(61) For every finite sequence f of elements of $\mathcal{E}^2_{\mathrm{T}}$ and for every i such that $i \in \operatorname{dom} f$ holds (**X**-coordinate(f))(i) = $(\pi_i f)_{\mathbf{1}}$ and (**Y**-coordinate(f))(i) = $(\pi_i f)_{\mathbf{2}}$.

(62) Let P, Q be non empty subsets of the carrier of $\mathcal{E}^2_{\mathrm{T}}$ and p_1, p_2, q_1, q_2 be points of $\mathcal{E}^2_{\mathrm{T}}$. Suppose that

(i) P is an arc from p_1 to p_2,

(ii) Q is an arc from q_1 to q_2,

(iii) for every point p of $\mathcal{E}^2_{\mathrm{T}}$ such that $p \in P$ holds $(p_1)_{\mathbf{1}} \leqslant p_{\mathbf{1}}$ and $p_{\mathbf{1}} \leqslant (p_2)_{\mathbf{1}}$,

(iv) for every point p of $\mathcal{E}^2_{\mathrm{T}}$ such that $p \in Q$ holds $(p_1)_{\mathbf{1}} \leqslant p_{\mathbf{1}}$ and $p_{\mathbf{1}} \leqslant (p_2)_{\mathbf{1}}$,

(v) for every point p of $\mathcal{E}^2_{\mathrm{T}}$ such that $p \in P$ holds $(q_1)_{\mathbf{2}} \leqslant p_{\mathbf{2}}$ and $p_{\mathbf{2}} \leqslant (q_2)_{\mathbf{2}}$, and

(vi) for every point p of $\mathcal{E}^2_{\mathrm{T}}$ such that $p \in Q$ holds $(q_1)_{\mathbf{2}} \leqslant p_{\mathbf{2}}$ and $p_{\mathbf{2}} \leqslant (q_2)_{\mathbf{2}}$.

Then $P \cap Q \neq \emptyset$.

In the sequel X, Y are non empty topological spaces.

We now state three propositions:

(63) Let f be a map from X into Y, P be a non empty subset of the carrier of Y, and f_1 be a map from X into $Y \restriction P$. If $f = f_1$ and f is continuous, then f_1 is continuous.

(64) Let f be a map from X into Y and P be a non empty subset of the carrier of Y. Suppose X is compact and Y is a T_2 space and f is continuous and one-to-one and $P = \operatorname{rng} f$. Then there exists a map f_1 from X into $Y \restriction P$ such that $f = f_1$ and f_1 is a homeomorphism.

(65) Let f, g be maps from $\mathbb{I}$ into $\mathcal{E}^2_{\mathrm{T}}$, a, b, c, d be real numbers, and O, I be points of $\mathbb{I}$. Suppose that

(i) $O = 0$,

(ii) $I = 1$,

(iii) f is continuous and one-to-one,
(iv) g is continuous and one-to-one,
(v) $f(O)_{\mathbf{1}} = a$,
(vi) $f(I)_{\mathbf{1}} = b$,
(vii) $g(O)_{\mathbf{2}} = c$,
(viii) $g(I)_{\mathbf{2}} = d$, and
(ix) for every point r of $\mathbb{I}$ holds $a \leqslant f(r)_{\mathbf{1}}$ and $f(r)_{\mathbf{1}} \leqslant b$ and $a \leqslant g(r)_{\mathbf{1}}$ and $g(r)_{\mathbf{1}} \leqslant b$ and $c \leqslant f(r)_{\mathbf{2}}$ and $f(r)_{\mathbf{2}} \leqslant d$ and $c \leqslant g(r)_{\mathbf{2}}$ and $g(r)_{\mathbf{2}} \leqslant d$.

Then $\operatorname{rng} f \cap \operatorname{rng} g \neq \emptyset$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[3] Józef Białas and Yatsuka Nakamura. The theorem of Weierstrass. *Formalized Mathematics*, 5(**3**):353–359, 1996.
[4] Leszek Borys. Paracompact and metrizable spaces. *Formalized Mathematics*, 2(**4**):481–485, 1991.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[7] Czesław Byliński and Piotr Rudnicki. Bounding boxes for compact sets in $\mathcal{E}^2$. *Formalized Mathematics*, 6(**3**):427–440, 1997.
[8] Agata Darmochwał. Compact spaces. *Formalized Mathematics*, 1(**2**):383–386, 1990.
[9] Agata Darmochwał. Families of subsets, subspaces and mappings in topological spaces. *Formalized Mathematics*, 1(**2**):257–261, 1990.
[10] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[11] Agata Darmochwał and Yatsuka Nakamura. Metric spaces as topological spaces - fundamental concepts. *Formalized Mathematics*, 2(**4**):605–608, 1991.
[12] Agata Darmochwał and Yatsuka Nakamura. The topological space $\mathcal{E}^2_{\mathrm{T}}$. Arcs, line segments and special polygonal arcs. *Formalized Mathematics*, 2(**5**):617–621, 1991.
[13] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[14] Krzysztof Hryniewiecki. Graphs. *Formalized Mathematics*, 2(**3**):365–370, 1991.
[15] Stanisława Kanas, Adam Lecko, and Mariusz Startek. Metric spaces. *Formalized Mathematics*, 1(**3**):607–610, 1990.
[16] Jarosław Kotowicz and Yatsuka Nakamura. Go-board theorem. *Formalized Mathematics*, 3(**1**):125–129, 1992.
[17] Jarosław Kotowicz and Yatsuka Nakamura. Introduction to Go-board - part I. *Formalized Mathematics*, 3(**1**):107–115, 1992.
[18] Yatsuka Nakamura and Piotr Rudnicki. Vertex sequences induced by chains. *Formalized Mathematics*, 5(**3**):297–304, 1996.
[19] Yatsuka Nakamura and Piotr Rudnicki. Oriented chains. *Formalized Mathematics*, 7(**2**):189–192, 1998.
[20] Yatsuka Nakamura and Andrzej Trybulec. Decomposing a Go-board into cells. *Formalized Mathematics*, 5(**3**):323–328, 1996.
[21] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[22] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[23] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

[24] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[25] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[26] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[27] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[28] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received August 21, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Algebraic Group on Fixed-length Bit Integer and its Adaptation to IDEA Cryptography

Yasushi Fuwa
Shinshu University
Nagano

Yoshinori Fujisawa
Shinshu University
Nagano

Summary. In this article, an algebraic group on fixed-length bit integer is constructed and its adaptation to IDEA cryptography is discussed. In the first section, we present some selected theorems on integers. In the continuous section, we construct an algebraic group on fixed-length integer. In the third section, operations of IDEA Cryptograms are defined and some theorems on these operations are proved. In the fourth section, we define sequences of IDEA Cryptogram's operations and discuss their nature. Finally, we make a model of IDEA Cryptogram and prove that the ciphertext that is encrypted by IDEA encryption algorithm can be decrypted by the IDEA decryption algorithm.

MML Identifier: `IDEA_1`.

The articles [11], [2], [4], [5], [6], [3], [10], [14], [8], [1], [7], [15], [12], [13], and [9] provide the notation and terminology for this paper.

1. Some Selected Theorems on Integers

We adopt the following rules: i, j, k, n are natural numbers and x, y, z are tuples of n and *Boolean*.

Next we state several propositions:

(1) For all i, j, k such that j is prime and $i < j$ and $k < j$ and $i \neq 0$ there exists a natural number a such that $a \cdot i \bmod j = k$ and $a < j$.

(2) For all natural numbers n, k_1, k_2 such that $n \neq 0$ and $k_1 \bmod n = k_2 \bmod n$ and $k_1 \leqslant k_2$ there exists a natural number t such that $k_2 - k_1 = n \cdot t$.

ISSN 1426–2630

(3) For all natural numbers a, b holds $a - b \leqslant a$.

(4) For all natural numbers b_1, b_2, c such that $b_2 \leqslant c$ holds $b_2 - b_1 \leqslant c$.

(5) For all natural numbers a, b, c such that $0 < a$ and $0 < b$ and $a < c$ and $b < c$ and c is prime holds $a \cdot b \bmod c \neq 0$.

(6) For every non empty natural number n holds the n-th power of $2 \neq 1$.

2. Basic Operators of IDEA Cryptograms

Let us consider n. The functor $\mathrm{ZERO}\, n$ yielding a tuple of n and *Boolean* is defined by:

(Def. 1) $\mathrm{ZERO}\, n = n \mapsto \mathit{false}$.

Let us consider n and let x, y be tuples of n and *Boolean*. The functor $x \oplus y$ yields a tuple of n and *Boolean* and is defined by:

(Def. 2) For every i such that $i \in \mathrm{Seg}\, n$ holds $\pi_i(x \oplus y) = \pi_i x \oplus \pi_i y$.

The following propositions are true:

(7) For all n, x holds $x \oplus x = \mathrm{ZERO}\, n$.

(8) For all n, x, y holds $x \oplus y = y \oplus x$.

Let us consider n and let x, y be tuples of n and *Boolean*. Let us observe that the functor $x \oplus y$ is commutative.

One can prove the following propositions:

(9) For all n, x holds $\mathrm{ZERO}\, n \oplus x = x$.

(10) For all n, x, y, z holds $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.

Let us consider n and let i be a natural number. We say that i is expressible by n if and only if:

(Def. 3) $i <$ the n-th power of 2.

The following proposition is true

(11) For every n holds n-BinarySequence$(0) = \mathrm{ZERO}\, n$.

Let us consider n and let i, j be natural numbers. The functor $\mathrm{ADD\_MOD}(i, j, n)$ yields a natural number and is defined by:

(Def. 4) $\mathrm{ADD\_MOD}(i, j, n) = (i + j) \bmod (\text{the } n\text{-th power of } 2)$.

Let us consider n and let i be a natural number. Let us assume that i is expressible by n. The functor $\mathrm{NEG\_N}(i, n)$ yielding a natural number is defined by:

(Def. 5) $\mathrm{NEG\_N}(i, n) = (\text{the } n\text{-th power of } 2) - i$.

Let us consider n and let i be a natural number. Let us assume that i is expressible by n. The functor $\mathrm{NEG\_MOD}(i, n)$ yielding a natural number is defined as follows:

(Def. 6) NEG_MOD(i, n) = NEG_N(i, n) mod (the n-th power of 2).

We now state several propositions:

(12) For all n, i such that i is expressible by n holds ADD_MOD$(i,$ NEG_MOD$(i, n), n) = 0$.

(13) For all n, i, j holds ADD_MOD(i, j, n) = ADD_MOD(j, i, n).

(14) For all n, i such that i is expressible by n holds ADD_MOD$(0, i, n) = i$.

(15) For all n, i, j, k holds ADD_MOD(ADD_MOD$(i, j, n), k, n)$ = ADD_MOD$(i,$ ADD_MOD$(j, k, n), n)$.

(16) For all n, i, j holds ADD_MOD(i, j, n) is expressible by n.

(17) For all n, i such that i is expressible by n holds NEG_MOD(i, n) is expressible by n.

Let us consider n and let i be a natural number. The functor ChangeVal_1(i, n) yields a natural number and is defined by:

(Def. 7) $\text{ChangeVal\_1}(i, n) = \begin{cases} \text{the } n\text{-th power of 2}, & \text{if } i = 0, \\ i, & \text{otherwise.} \end{cases}$

We now state two propositions:

(18) For all n, i such that i is expressible by n holds ChangeVal_1$(i, n) \leqslant$ the n-th power of 2 and ChangeVal_1$(i, n) > 0$.

(19) Let n, a_1, a_2 be natural numbers. Suppose a_1 is expressible by n and a_2 is expressible by n and ChangeVal_1(a_1, n) = ChangeVal_1(a_2, n). Then $a_1 = a_2$.

Let us consider n and let i be a natural number. The functor ChangeVal_2(i, n) yields a natural number and is defined as follows:

(Def. 8) $\text{ChangeVal\_2}(i, n) = \begin{cases} 0, & \text{if } i = \text{the } n\text{-th power of 2}, \\ i, & \text{otherwise.} \end{cases}$

We now state two propositions:

(20) For all n, i such that i is expressible by n holds ChangeVal_2(i, n) is expressible by n.

(21) For all natural numbers n, a_1, a_2 such that $a_1 \neq 0$ and $a_2 \neq 0$ and ChangeVal_2(a_1, n) = ChangeVal_2(a_2, n) holds $a_1 = a_2$.

Let us consider n and let i, j be natural numbers. The functor MUL_MOD(i, j, n) yields a natural number and is defined as follows:

(Def. 9) MUL_MOD(i, j, n) = ChangeVal_2(ChangeVal_1$(i, n)\cdot$ ChangeVal_1(j, n) mod ((the n-th power of 2)+1)$, n)$.

Let n be a non empty natural number and let i be a natural number. Let us assume that i is expressible by n and (the n-th power of 2)+1 is prime. The functor INV_MOD(i, n) yielding a natural number is defined as follows:

(Def. 10) MUL_MOD$(i,$ INV_MOD$(i, n), n) = 1$ and INV_MOD(i, n) is expressible by n.

The following propositions are true:

(22) For all n, i, j holds $\mathrm{MUL\_MOD}(i, j, n) = \mathrm{MUL\_MOD}(j, i, n)$.

(23) For all n, i such that i is expressible by n holds $\mathrm{MUL\_MOD}(1, i, n) = i$.

(24) Let given n, i, j, k. Suppose that

(i) (the n-th power of 2)+1 is prime,

(ii) i is expressible by n,

(iii) j is expressible by n, and

(iv) k is expressible by n.

Then $\mathrm{MUL\_MOD}(\mathrm{MUL\_MOD}(i, j, n), k, n) =$
$\mathrm{MUL\_MOD}(i, \mathrm{MUL\_MOD}(j, k, n), n)$.

(25) For all n, i, j holds $\mathrm{MUL\_MOD}(i, j, n)$ is expressible by n.

(26) If $\mathrm{ChangeVal\_2}(i, n) = 1$, then $i = 1$.

3. Operations of IDEA Cryptograms

Let us consider n and let m, k be finite sequences of elements of $\mathbb{N}$. The functor $\mathrm{IDEAoperationA}(m, k, n)$ yielding a finite sequence of elements of $\mathbb{N}$ is defined by the conditions (Def. 11).

(Def. 11)(i) $\mathrm{len}\,\mathrm{IDEAoperationA}(m, k, n) = \mathrm{len}\, m$, and

(ii) for every natural number i such that $i \in \mathrm{dom}\, m$ holds if $i = 1$, then $(\mathrm{IDEAoperationA}(m, k, n))(i) = \mathrm{MUL\_MOD}(m(1), k(1), n)$ and if $i = 2$, then $(\mathrm{IDEAoperationA}(m, k, n))(i) = \mathrm{ADD\_MOD}(m(2), k(2), n)$ and if $i = 3$, then $(\mathrm{IDEAoperationA}(m, k, n))(i) = \mathrm{ADD\_MOD}(m(3), k(3), n)$ and if $i = 4$, then $(\mathrm{IDEAoperationA}(m, k, n))(i) = \mathrm{MUL\_MOD}(m(4), k(4), n)$ and if $i \neq 1$ and $i \neq 2$ and $i \neq 3$ and $i \neq 4$, then $(\mathrm{IDEAoperationA}(m, k, n))(i) = m(i)$.

In the sequel m, k, k_1, k_2 denote finite sequences of elements of $\mathbb{N}$.

Let n be a non empty natural number and let m, k be finite sequences of elements of $\mathbb{N}$. The functor $\mathrm{IDEAoperationB}(m, k, n)$ yielding a finite sequence of elements of $\mathbb{N}$ is defined by the conditions (Def. 12).

(Def. 12)(i) $\mathrm{len}\,\mathrm{IDEAoperationB}(m, k, n) = \mathrm{len}\, m$, and

(ii) for every natural number i such that $i \in \mathrm{dom}\, m$ holds if $i = 1$, then $(\mathrm{IDEAoperationB}(m, k, n))(i) = \mathrm{Absval}((n\text{-BinarySequence}(m(1))) \oplus (n\text{-BinarySequence}(\mathrm{MUL\_MOD}(\mathrm{ADD\_MOD}(\mathrm{MUL\_MOD}(\mathrm{Absval}((n\text{-BinarySequence}(m(1))) \oplus (n\text{-BinarySequence}(m(3)))), k(5), n), \mathrm{Absval}((n\text{-BinarySequence}(m(2))) \oplus (n\text{-BinarySequence}(m(4)))), n), k(6), n))))$ and if $i = 2$, then $(\mathrm{IDEAoperationB}(m, k, n))(i) = \mathrm{Absval}((n\text{-BinarySequence}(m(2))) \oplus (n\text{-BinarySequence}(\mathrm{ADD\_MOD}(\mathrm{MUL\_MOD}(\mathrm{Absval}((n\text{-BinarySequence}$

$(m(1))) \oplus (n\text{-BinarySequence}(m(3)))), k(5), n), \text{MUL\_MOD}(\text{ADD\_MOD}$ $(\text{MUL\_MOD}(\text{Absval}((n\text{-BinarySequence}$ $(m(1)))\oplus(n\text{-BinarySequence}(m(3)))), k(5), n), \text{Absval}((n\text{-BinarySequence}(m$ $(2))) \oplus (n\text{-BinarySequence}(m(4)))), n), k(6), n), n))))$ and if $i = 3$, then $(\text{IDEAoperationB}(m, k, n))(i) = \text{Absval}((n\text{-BinarySequence}(m(3))) \oplus$ $(n\text{-BinarySequence}(\text{MUL\_MOD}(\text{ADD\_MOD}(\text{MUL\_MOD}(\text{Absval}$ $((n\text{-BinarySequence}(m(1)))\oplus(n\text{-BinarySequence}(m(3)))), k(5), n), \text{Absval}$ $((n\text{-BinarySequence}(m(2))) \oplus (n\text{-BinarySequence}(m(4)))), n), k(6), n))))$ and if $i = 4$, then $(\text{IDEAoperationB}(m, k, n))(i) =$ $\text{Absval}((n\text{-BinarySequence}(m(4))) \oplus (n\text{-BinarySequence}$ $(\text{ADD\_MOD}(\text{MUL\_MOD}(\text{Absval}((n\text{-BinarySequence}(m(1)))\oplus$ $(n\text{-BinarySequence}(m(3)))), k(5), n), \text{MUL\_MOD}(\text{ADD\_MOD}(\text{MUL\_MOD}$ $(\text{Absval}((n\text{-BinarySequence}(m(1)))\oplus(n\text{-BinarySequence}(m(3)))), k(5), n),$ $\text{Absval}((n\text{-BinarySequence}(m(2)))\oplus(n\text{-BinarySequence}(m(4)))), n), k(6),$ $n), n))))$ and if $i \neq 1$ and $i \neq 2$ and $i \neq 3$ and $i \neq 4$, then $(\text{IDEAoperationB}(m, k, n))(i) = m(i)$.

Let m be a finite sequence of elements of $\mathbb{N}$. The functor IDEAoperationC m yields a finite sequence of elements of $\mathbb{N}$ and is defined as follows:

(Def. 13) $\operatorname{len} \text{IDEAoperationC}\, m = \operatorname{len} m$ and for every natural number i such that $i \in \operatorname{dom} m$ holds $(\text{IDEAoperationC}\, m)(i) = (i = 2 \rightarrow m(3), (i = 3 \rightarrow m(2), m(i)))$.

The following propositions are true:

(27) Let given n, m, k. Suppose $\operatorname{len} m \geqslant 4$. Then
- (i) $(\text{IDEAoperationA}(m, k, n))(1)$ is expressible by n,
- (ii) $(\text{IDEAoperationA}(m, k, n))(2)$ is expressible by n,
- (iii) $(\text{IDEAoperationA}(m, k, n))(3)$ is expressible by n, and
- (iv) $(\text{IDEAoperationA}(m, k, n))(4)$ is expressible by n.

(28) Let n be a non empty natural number and given m, k. Suppose $\operatorname{len} m \geqslant 4$. Then
- (i) $(\text{IDEAoperationB}(m, k, n))(1)$ is expressible by n,
- (ii) $(\text{IDEAoperationB}(m, k, n))(2)$ is expressible by n,
- (iii) $(\text{IDEAoperationB}(m, k, n))(3)$ is expressible by n, and
- (iv) $(\text{IDEAoperationB}(m, k, n))(4)$ is expressible by n.

(29) Let given m. Suppose that
- (i) $\operatorname{len} m \geqslant 4$,
- (ii) $m(1)$ is expressible by n,
- (iii) $m(2)$ is expressible by n,
- (iv) $m(3)$ is expressible by n, and
- (v) $m(4)$ is expressible by n.

Then
- (vi) $(\text{IDEAoperationC}\, m)(1)$ is expressible by n,

(vii) (IDEAoperationC m)(2) is expressible by n,
(viii) (IDEAoperationC m)(3) is expressible by n, and
(ix) (IDEAoperationC m)(4) is expressible by n.

(30) Let n be a non empty natural number and given m, k_1, k_2. Suppose that
(i) (the n-th power of 2)+1 is prime,
(ii) $\operatorname{len} m \geqslant 4$,
(iii) $m(1)$ is expressible by n,
(iv) $m(2)$ is expressible by n,
(v) $m(3)$ is expressible by n,
(vi) $m(4)$ is expressible by n,
(vii) $k_1(1)$ is expressible by n,
(viii) $k_1(2)$ is expressible by n,
(ix) $k_1(3)$ is expressible by n,
(x) $k_1(4)$ is expressible by n,
(xi) $k_2(1) = \text{INV\_MOD}(k_1(1), n)$,
(xii) $k_2(2) = \text{NEG\_MOD}(k_1(2), n)$,
(xiii) $k_2(3) = \text{NEG\_MOD}(k_1(3), n)$, and
(xiv) $k_2(4) = \text{INV\_MOD}(k_1(4), n)$.

Then $\text{IDEAoperationA}(\text{IDEAoperationA}(m, k_1, n), k_2, n) = m$.

(31) Let n be a non empty natural number and given m, k_1, k_2. Suppose that
(i) (the n-th power of 2)+1 is prime,
(ii) $\operatorname{len} m \geqslant 4$,
(iii) $m(1)$ is expressible by n,
(iv) $m(2)$ is expressible by n,
(v) $m(3)$ is expressible by n,
(vi) $m(4)$ is expressible by n,
(vii) $k_1(1)$ is expressible by n,
(viii) $k_1(2)$ is expressible by n,
(ix) $k_1(3)$ is expressible by n,
(x) $k_1(4)$ is expressible by n,
(xi) $k_2(1) = \text{INV\_MOD}(k_1(1), n)$,
(xii) $k_2(2) = \text{NEG\_MOD}(k_1(3), n)$,
(xiii) $k_2(3) = \text{NEG\_MOD}(k_1(2), n)$, and
(xiv) $k_2(4) = \text{INV\_MOD}(k_1(4), n)$.

Then $\text{IDEAoperationA}(\text{IDEAoperationC}\,\text{IDEAoperationA}(\text{IDEAoperationC}\,m, k_1, n), k_2, n) = m$.

(32) Let n be a non empty natural number and given m, k_1, k_2. Suppose that
(i) (the n-th power of 2)+1 is prime,
(ii) $\operatorname{len} m \geqslant 4$,
(iii) $m(1)$ is expressible by n,
(iv) $m(2)$ is expressible by n,

(v) $m(3)$ is expressible by n,
(vi) $m(4)$ is expressible by n,
(vii) $k_1(5)$ is expressible by n,
(viii) $k_1(6)$ is expressible by n,
(ix) $k_2(5) = k_1(5)$, and
(x) $k_2(6) = k_1(6)$.

Then IDEAoperationB(IDEAoperationB$(m, k_1, n), k_2, n) = m$.

(33) For every m such that $\operatorname{len} m \geqslant 4$ holds IDEAoperationC IDEAoperationC $m = m$.

4. Sequences of IDEA Cryptogram's Operations

The set MESSAGES is defined by:

(Def. 14) MESSAGES $= \mathbb{N}^*$.

Let us mention that MESSAGES is non empty.

Let us mention that every element of MESSAGES is function-like and relation-like.

Let us note that every element of MESSAGES is finite sequence-like.

Let n be a non empty natural number and let us consider k. The functor IDEA_P(k, n) yielding a function from MESSAGES into MESSAGES is defined as follows:

(Def. 15) For every m holds (IDEA_P$(k, n))(m)$ = IDEAoperationA (IDEAoperationC IDEAoperationB$(m, k, n), k, n)$.

Let n be a non empty natural number and let us consider k. The functor IDEA_Q(k, n) yields a function from MESSAGES into MESSAGES and is defined as follows:

(Def. 16) For every m holds (IDEA_Q$(k, n))(m)$ = IDEAoperationB (IDEAoperationA(IDEAoperationC $m, k, n), k, n)$.

Let r, l_1 be natural numbers, let n be a non empty natural number, and let K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$. The functor IDEA_P_F(K_1, n, r) yielding a finite sequence is defined as follows:

(Def. 17) len IDEA_P_F$(K_1, n, r) = r$ and for every i such that $i \in$ dom IDEA_P_F(K_1, n, r) holds (IDEA_P_F$(K_1, n, r))(i)$ = IDEA_P(Line$(K_1, i), n)$.

Let r, l_1 be natural numbers, let n be a non empty natural number, and let K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$. One can verify that IDEA_P_F(K_1, n, r) is function yielding.

Let r, l_1 be natural numbers, let n be a non empty natural number, and let K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$. The functor IDEA_Q_F(K_1, n, r) yielding a finite sequence is defined as follows:

(Def. 18) len IDEA_Q_F$(K_1, n, r) = r$ and for every i such that $i \in$ dom IDEA_Q_F(K_1, n, r) holds (IDEA_Q_F$(K_1, n, r))(i) =$ IDEA_Q(Line$(K_1, (r -' i) + 1), n)$.

Let r, l_1 be natural numbers, let n be a non empty natural number, and let K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$. Observe that IDEA_Q_F(K_1, n, r) is function yielding.

Let us consider k, n. The functor IDEA_PS(k, n) yields a function from MESSAGES into MESSAGES and is defined as follows:

(Def. 19) For every m holds (IDEA_PS$(k, n))(m) =$ IDEAoperationA(m, k, n).

Let us consider k, n. The functor IDEA_QS(k, n) yields a function from MESSAGES into MESSAGES and is defined as follows:

(Def. 20) For every m holds (IDEA_QS$(k, n))(m) =$ IDEAoperationA(m, k, n).

Let n be a non empty natural number and let us consider k. The functor IDEA_PE(k, n) yielding a function from MESSAGES into MESSAGES is defined by:

(Def. 21) For every m holds (IDEA_PE$(k, n))(m) =$ IDEAoperationA (IDEAoperationB$(m, k, n), k, n)$.

Let n be a non empty natural number and let us consider k. The functor IDEA_QE(k, n) yielding a function from MESSAGES into MESSAGES is defined by:

(Def. 22) For every m holds (IDEA_QE$(k, n))(m) =$ IDEAoperationB (IDEAoperationA$(m, k, n), k, n)$.

We now state a number of propositions:

(34) Let n be a non empty natural number and given m, k_1, k_2. Suppose that
- (i) (the n-th power of 2)+1 is prime,
- (ii) len $m \geqslant 4$,
- (iii) $m(1)$ is expressible by n,
- (iv) $m(2)$ is expressible by n,
- (v) $m(3)$ is expressible by n,
- (vi) $m(4)$ is expressible by n,
- (vii) $k_1(1)$ is expressible by n,
- (viii) $k_1(2)$ is expressible by n,
- (ix) $k_1(3)$ is expressible by n,
- (x) $k_1(4)$ is expressible by n,
- (xi) $k_1(5)$ is expressible by n,
- (xii) $k_1(6)$ is expressible by n,
- (xiii) $k_2(1) =$ INV_MOD$(k_1(1), n)$,

(xiv) $k_2(2) = \mathrm{NEG\_MOD}(k_1(3), n)$,
(xv) $k_2(3) = \mathrm{NEG\_MOD}(k_1(2), n)$,
(xvi) $k_2(4) = \mathrm{INV\_MOD}(k_1(4), n)$,
(xvii) $k_2(5) = k_1(5)$, and
(xviii) $k_2(6) = k_1(6)$.

Then $(\mathrm{IDEA\_Q}(k_2, n) \cdot \mathrm{IDEA\_P}(k_1, n))(m) = m$.

(35) Let n be a non empty natural number and given m, k_1, k_2. Suppose that
(i) (the n-th power of 2)+1 is prime,
(ii) $\mathrm{len}\, m \geqslant 4$,
(iii) $m(1)$ is expressible by n,
(iv) $m(2)$ is expressible by n,
(v) $m(3)$ is expressible by n,
(vi) $m(4)$ is expressible by n,
(vii) $k_1(1)$ is expressible by n,
(viii) $k_1(2)$ is expressible by n,
(ix) $k_1(3)$ is expressible by n,
(x) $k_1(4)$ is expressible by n,
(xi) $k_2(1) = \mathrm{INV\_MOD}(k_1(1), n)$,
(xii) $k_2(2) = \mathrm{NEG\_MOD}(k_1(2), n)$,
(xiii) $k_2(3) = \mathrm{NEG\_MOD}(k_1(3), n)$, and
(xiv) $k_2(4) = \mathrm{INV\_MOD}(k_1(4), n)$.

Then $(\mathrm{IDEA\_QS}(k_2, n) \cdot \mathrm{IDEA\_PS}(k_1, n))(m) = m$.

(36) Let n be a non empty natural number and given m, k_1, k_2. Suppose that
(i) (the n-th power of 2)+1 is prime,
(ii) $\mathrm{len}\, m \geqslant 4$,
(iii) $m(1)$ is expressible by n,
(iv) $m(2)$ is expressible by n,
(v) $m(3)$ is expressible by n,
(vi) $m(4)$ is expressible by n,
(vii) $k_1(1)$ is expressible by n,
(viii) $k_1(2)$ is expressible by n,
(ix) $k_1(3)$ is expressible by n,
(x) $k_1(4)$ is expressible by n,
(xi) $k_1(5)$ is expressible by n,
(xii) $k_1(6)$ is expressible by n,
(xiii) $k_2(1) = \mathrm{INV\_MOD}(k_1(1), n)$,
(xiv) $k_2(2) = \mathrm{NEG\_MOD}(k_1(2), n)$,
(xv) $k_2(3) = \mathrm{NEG\_MOD}(k_1(3), n)$,
(xvi) $k_2(4) = \mathrm{INV\_MOD}(k_1(4), n)$,
(xvii) $k_2(5) = k_1(5)$, and
(xviii) $k_2(6) = k_1(6)$.

Then $(\mathrm{IDEA\_QE}(k_2, n) \cdot \mathrm{IDEA\_PE}(k_1, n))(m) = m$.

(37) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. Then $\mathrm{IDEA\_P\_F}(K_1, n, k+1) = (\mathrm{IDEA\_P\_F}(K_1, n, k)) \frown \langle \mathrm{IDEA\_P}(\mathrm{Line}(K_1, k+1), n) \rangle$.

(38) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. Then $\mathrm{IDEA\_Q\_F}(K_1, n, k+1) = \langle \mathrm{IDEA\_Q}(\mathrm{Line}(K_1, k+1), n) \rangle \frown \mathrm{IDEA\_Q\_F}(K_1, n, k)$.

(39) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. Then $\mathrm{IDEA\_P\_F}(K_1, n, k)$ is a composable finite sequence.

(40) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. Then $\mathrm{IDEA\_Q\_F}(K_1, n, k)$ is a composable finite sequence.

(41) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. If $k \neq 0$, then $\mathrm{IDEA\_P\_F}(K_1, n, k)$ is a composable sequence from MESSAGES into MESSAGES.

(42) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. If $k \neq 0$, then $\mathrm{IDEA\_Q\_F}(K_1, n, k)$ is a composable sequence from MESSAGES into MESSAGES.

(43) Let n be a non empty natural number, M be a finite sequence of elements of $\mathbb{N}$, and given m, k. Suppose $M = (\mathrm{IDEA\_P}(k, n))(m)$ and $\mathrm{len}\, m \geqslant 4$. Then

(i) $\mathrm{len}\, M \geqslant 4$,
(ii) $M(1)$ is expressible by n,
(iii) $M(2)$ is expressible by n,
(iv) $M(3)$ is expressible by n, and
(v) $M(4)$ is expressible by n.

(44) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and r be a natural number. Then $\mathrm{rng}\, \mathrm{compose}_{\mathrm{MESSAGES}}\, \mathrm{IDEA\_P\_F}(K_1, n, r) \subseteq \mathrm{MESSAGES}$ and $\mathrm{dom}\, \mathrm{compose}_{\mathrm{MESSAGES}}\, \mathrm{IDEA\_P\_F}(K_1, n, r) = \mathrm{MESSAGES}$.

(45) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and r be a natural number. Then $\mathrm{rng}\, \mathrm{compose}_{\mathrm{MESSAGES}}\, \mathrm{IDEA\_Q\_F}(K_1, n, r) \subseteq \mathrm{MESSAGES}$ and $\mathrm{dom}\, \mathrm{compose}_{\mathrm{MESSAGES}}\, \mathrm{IDEA\_Q\_F}(K_1, n, r) = \mathrm{MESSAGES}$.

(46) Let n be a non empty natural number, m be a finite sequence of elements

of $\mathbb{N}$, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, r be a natural number, and M be a finite sequence of elements of $\mathbb{N}$. If $M = (\text{compose}_{\text{MESSAGES}}\, \text{IDEA\_P\_F}(K_1, n, r))(m)$ and $\operatorname{len} m \geqslant 4$, then $\operatorname{len} M \geqslant 4$.

(47) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, r be a natural number, M be a finite sequence of elements of $\mathbb{N}$, and given m. Suppose that

(i) $M = (\text{compose}_{\text{MESSAGES}}\, \text{IDEA\_P\_F}(K_1, n, r))(m)$,
(ii) $\operatorname{len} m \geqslant 4$,
(iii) $m(1)$ is expressible by n,
(iv) $m(2)$ is expressible by n,
(v) $m(3)$ is expressible by n, and
(vi) $m(4)$ is expressible by n.

Then

(vii) $\operatorname{len} M \geqslant 4$,
(viii) $M(1)$ is expressible by n,
(ix) $M(2)$ is expressible by n,
(x) $M(3)$ is expressible by n, and
(xi) $M(4)$ is expressible by n.

5. Modeling of IDEA Cryptogram

One can prove the following propositions:

(48) Let n be a non empty natural number, l_1 be a natural number, K_2, K_3 be matrices over $\mathbb{N}$ of dimension $l_1 \times 6$, r be a natural number, and given m. Suppose that

(i) $l_1 \geqslant r$,
(ii) (the n-th power of 2)+1 is prime,
(iii) $\operatorname{len} m \geqslant 4$,
(iv) $m(1)$ is expressible by n,
(v) $m(2)$ is expressible by n,
(vi) $m(3)$ is expressible by n,
(vii) $m(4)$ is expressible by n, and
(viii) for every natural number i such that $i \leqslant r$ holds $(K_2)_{i,1}$ is expressible by n and $(K_2)_{i,2}$ is expressible by n and $(K_2)_{i,3}$ is expressible by n and $(K_2)_{i,4}$ is expressible by n and $(K_2)_{i,5}$ is expressible by n and $(K_2)_{i,6}$ is expressible by n and $(K_3)_{i,1}$ is expressible by n and $(K_3)_{i,2}$ is expressible by n and $(K_3)_{i,3}$ is expressible by n and $(K_3)_{i,4}$ is expressible by n and $(K_3)_{i,5}$ is expressible by n and $(K_3)_{i,6}$ is expressible by n and $(K_3)_{i,1} = \text{INV\_MOD}((K_2)_{i,1}, n)$ and $(K_3)_{i,2} = \text{NEG\_MOD}((K_2)_{i,3}, n)$ and $(K_3)_{i,3} =$

NEG_MOD($(K_2)_{i,2}, n$) and $(K_3)_{i,4}$ = INV_MOD($(K_2)_{i,4}, n$) and $(K_2)_{i,5} = (K_3)_{i,5}$ and $(K_2)_{i,6} = (K_3)_{i,6}$.
Then (compose$_{\mathrm{MESSAGES}}$((IDEA_P_F(K_2, n, r))$^\frown$IDEA_Q_F(K_3, n, r)))$(m) = m$.

(49) Let n be a non empty natural number, l_1 be a natural number, K_2, K_3 be matrices over $\mathbb{N}$ of dimension $l_1 \times 6$, r be a natural number, k_3, k_4, k_5, k_6 be finite sequences of elements of $\mathbb{N}$, and given m. Suppose that

(i) $l_1 \geqslant r$,
(ii) (the n-th power of 2)+1 is prime,
(iii) $\mathrm{len}\, m \geqslant 4$,
(iv) $m(1)$ is expressible by n,
(v) $m(2)$ is expressible by n,
(vi) $m(3)$ is expressible by n,
(vii) $m(4)$ is expressible by n,
(viii) for every natural number i such that $i \leqslant r$ holds $(K_2)_{i,1}$ is expressible by n and $(K_2)_{i,2}$ is expressible by n and $(K_2)_{i,3}$ is expressible by n and $(K_2)_{i,4}$ is expressible by n and $(K_2)_{i,5}$ is expressible by n and $(K_2)_{i,6}$ is expressible by n and $(K_3)_{i,1}$ is expressible by n and $(K_3)_{i,2}$ is expressible by n and $(K_3)_{i,3}$ is expressible by n and $(K_3)_{i,4}$ is expressible by n and $(K_3)_{i,5}$ is expressible by n and $(K_3)_{i,6}$ is expressible by n and $(K_3)_{i,1}$ = INV_MOD($(K_2)_{i,1}, n$) and $(K_3)_{i,2}$ = NEG_MOD($(K_2)_{i,3}, n$) and $(K_3)_{i,3}$ = NEG_MOD($(K_2)_{i,2}, n$) and $(K_3)_{i,4}$ = INV_MOD($(K_2)_{i,4}, n$) and $(K_2)_{i,5} = (K_3)_{i,5}$ and $(K_2)_{i,6} = (K_3)_{i,6}$,
(ix) $k_3(1)$ is expressible by n,
(x) $k_3(2)$ is expressible by n,
(xi) $k_3(3)$ is expressible by n,
(xii) $k_3(4)$ is expressible by n,
(xiii) $k_4(1)$ = INV_MOD($k_3(1), n$),
(xiv) $k_4(2)$ = NEG_MOD($k_3(2), n$),
(xv) $k_4(3)$ = NEG_MOD($k_3(3), n$),
(xvi) $k_4(4)$ = INV_MOD($k_3(4), n$),
(xvii) $k_5(1)$ is expressible by n,
(xviii) $k_5(2)$ is expressible by n,
(xix) $k_5(3)$ is expressible by n,
(xx) $k_5(4)$ is expressible by n,
(xxi) $k_5(5)$ is expressible by n,
(xxii) $k_5(6)$ is expressible by n,
(xxiii) $k_6(1)$ = INV_MOD($k_5(1), n$),
(xxiv) $k_6(2)$ = NEG_MOD($k_5(2), n$),
(xxv) $k_6(3)$ = NEG_MOD($k_5(3), n$),
(xxvi) $k_6(4)$ = INV_MOD($k_5(4), n$),
(xxvii) $k_6(5) = k_5(5)$, and

(xxviii) $k_6(6) = k_5(6)$.
Then $(\mathrm{IDEA\_QS}(k_4, n) \cdot (\mathrm{compose}_{\mathrm{MESSAGES}}\, \mathrm{IDEA\_Q\_F}(K_3, n, r) \cdot (\mathrm{IDEA\_QE}(k_6, n) \cdot (\mathrm{IDEA\_PE}(k_5, n) \cdot (\mathrm{compose}_{\mathrm{MESSAGES}}\, \mathrm{IDEA\_P\_F}(K_2, n, r) \cdot \mathrm{IDEA\_PS}(k_3, n))))))(m) = m$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[3] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.
[4] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[7] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[8] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.
[9] Andrzej Kondracki. The chinese remainder theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.
[10] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[11] Robert Milewski. Binary arithmetics. Binary sequences. *Formalized Mathematics*, 7(**1**):23–26, 1998.
[12] Konrad Raczkowski and Andrzej Nędzusiak. Serieses. *Formalized Mathematics*, 2(**4**):449–452, 1991.
[13] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[14] Edmund Woronowicz. Many–argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.
[15] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received September 7, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

The Definition and Basic Properties of Topological Groups

Artur Korniłowicz
University of Białystok

MML Identifier: TOPGRP_1.

The notation and terminology used in this paper are introduced in the following articles: [11], [5], [9], [2], [3], [8], [13], [14], [10], [16], [15], [17], [6], [18], [1], [7], [12], and [4].

1. Preliminaries

For simplicity, we follow the rules: S denotes a 1-sorted structure, R denotes a non empty 1-sorted structure, X denotes a subset of the carrier of R, T denotes a non empty topological structure, and x denotes a set.

Let X, Y be sets. One can verify that every function from X into Y which is bijective is also one-to-one and onto and every function from X into Y which is one-to-one and onto is also bijective.

Let X be a set. Observe that there exists a function from X into X which is one-to-one and onto.

Next we state the proposition

(1) $\mathrm{rng}(\mathrm{id}_S) = \Omega_S$.

Let R be a non empty 1-sorted structure. Note that $(\mathrm{id}_R)^{-1}$ is one-to-one.

We now state two propositions:

(2) $(\mathrm{id}_R)^{-1} = \mathrm{id}_R$.

(3) $(\mathrm{id}_R)^{-1}(X) = X$.

Let S be a 1-sorted structure. One can check that there exists a map from S into S which is one-to-one and onto.

ISSN 1426–2630

2. On the Groups

We use the following convention: H denotes a non empty groupoid, P, Q, P_1, Q_1 denote subsets of the carrier of H, and h denotes an element of the carrier of H.

The following propositions are true:

(4) If $P \subseteq P_1$ and $Q \subseteq Q_1$, then $P \cdot Q \subseteq P_1 \cdot Q_1$.

(5) If $P \subseteq Q$, then $P \cdot h \subseteq Q \cdot h$.

(6) If $P \subseteq Q$, then $h \cdot P \subseteq h \cdot Q$.

In the sequel G denotes a group, A, B denote subsets of the carrier of G, and a denotes an element of the carrier of G.

One can prove the following propositions:

(7) $a \in A^{-1}$ iff $a^{-1} \in A$.

(8) $(A^{-1})^{-1} = A$.

(9) $A \subseteq B$ iff $A^{-1} \subseteq B^{-1}$.

(10) $\cdot_G^{-1\circ} A = A^{-1}$.

(11) $\cdot_G^{-1-1}(A) = A^{-1}$.

(12) $\cdot_G^{-1}$ is one-to-one.

(13) $\operatorname{rng} \cdot_G^{-1} =$ the carrier of G.

Let G be a group. Observe that $\cdot_G^{-1}$ is one-to-one and onto.

Next we state two propositions:

(14) $\cdot_G^{-1-1} = \cdot_G^{-1}$.

(15) (The multiplication of $H)^\circ [\!: P, Q :\!] = P \cdot Q$.

Let G be a non empty groupoid and let a be an element of the carrier of G. The functor $a \cdot \square$ yielding a map from G into G is defined by:

(Def. 1) For every element x of the carrier of G holds $(a \cdot \square)(x) = a \cdot x$.

The functor $\square \cdot a$ yields a map from G into G and is defined as follows:

(Def. 2) For every element x of the carrier of G holds $(\square \cdot a)(x) = x \cdot a$.

Let G be a group and let a be an element of the carrier of G. One can verify that $a \cdot \square$ is one-to-one and onto and $\square \cdot a$ is one-to-one and onto.

Next we state four propositions:

(16) $(h \cdot \square)^\circ P = h \cdot P$.

(17) $(\square \cdot h)^\circ P = P \cdot h$.

(18) $(a \cdot \square)^{-1} = a^{-1} \cdot \square$.

(19) $(\square \cdot a)^{-1} = \square \cdot a^{-1}$.

3. On the Topological Spaces

Let T be a non empty topological structure. Observe that $(\mathrm{id}_T)^{-1}$ is continuous.

Next we state the proposition

(20) id_T is a homeomorphism.

Let T be a non empty topological space and let p be a point of T. Observe that every neighbourhood of p is non empty.

Next we state the proposition

(21) For every non empty topological space T and for every point p of T holds Ω_T is a neighbourhood of p.

Let T be a non empty topological space and let p be a point of T. One can check that there exists a neighbourhood of p which is non empty and open.

One can prove the following propositions:

(22) Let S, T be non empty topological spaces and f be a map from S into T. Suppose f is open. Let p be a point of S and P be a neighbourhood of p. Then there exists an open neighbourhood R of $f(p)$ such that $R \subseteq f^\circ P$.

(23) Let S, T be non empty topological spaces and f be a map from S into T. Suppose that for every point p of S and for every open neighbourhood P of p there exists a neighbourhood R of $f(p)$ such that $R \subseteq f^\circ P$. Then f is open.

(24) Let S, T be non empty topological structures and f be a map from S into T. Then f is a homeomorphism if and only if the following conditions are satisfied:

(i) $\mathrm{dom}\, f = \Omega_S$,
(ii) $\mathrm{rng}\, f = \Omega_T$,
(iii) f is one-to-one, and
(iv) for every subset P of T holds P is closed iff $f^{-1}(P)$ is closed.

(25) Let S, T be non empty topological structures and f be a map from S into T. Then f is a homeomorphism if and only if the following conditions are satisfied:

(i) $\mathrm{dom}\, f = \Omega_S$,
(ii) $\mathrm{rng}\, f = \Omega_T$,
(iii) f is one-to-one, and
(iv) for every subset P of S holds P is open iff $f^\circ P$ is open.

(26) Let S, T be non empty topological structures and f be a map from S into T. Then f is a homeomorphism if and only if the following conditions are satisfied:

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

(ii) $\operatorname{rng} f = \Omega_T$,
(iii) f is one-to-one, and
(iv) for every subset P of T holds P is open iff $f^{-1}(P)$ is open.

(27) Let S be a topological space, T be a non empty topological space, and f be a map from S into T. Then f is continuous if and only if for every subset P of the carrier of T holds $f^{-1}(\operatorname{Int} P) \subseteq \operatorname{Int}(f^{-1}(P))$.

Let T be a non empty topological space. One can verify that there exists a subset of T which is non empty and dense.

The following two propositions are true:

(28) Let S, T be non empty topological spaces, f be a map from S into T, and A be a dense subset of S. If f is a homeomorphism, then $f^{\circ}A$ is dense.

(29) Let S, T be non empty topological spaces, f be a map from S into T, and A be a dense subset of T. If f is a homeomorphism, then $f^{-1}(A)$ is dense.

Let S, T be non empty topological structures. Observe that every map from S into T which is homeomorphism is also onto, one-to-one, continuous, and open.

Let T be a non empty topological structure. Observe that there exists a map from T into T which is homeomorphism.

Let T be a non empty topological structure and let f be homeomorphism map from T into T. Note that f^{-1} is homeomorphism.

4. The Group of Homoemorphisms

Let T be a non empty topological structure. A map from T into T is said to be a homeomorphism of T if:

(Def. 3) It is a homeomorphism.

Let T be a non empty topological structure. Then id_T is a homeomorphism of T.

Let T be a non empty topological structure. One can check that every homeomorphism of T is homeomorphism.

We now state two propositions:

(30) For every homeomorphism f of T holds f^{-1} is a homeomorphism of T.

(31) For all homeomorphisms f, g of T holds $f \cdot g$ is a homeomorphism of T.

Let T be a non empty topological structure. The group of homeomorphisms of T is a strict groupoid and is defined by the conditions (Def. 4).

(Def. 4)(i) $x \in$ the carrier of the group of homeomorphisms of T iff x is a homeomorphism of T, and

(ii) for all homeomorphisms f, g of T holds (the multiplication of the group of homeomorphisms of T)$(f, g) = g \cdot f$.

Let T be a non empty topological structure. Note that the group of homeomorphisms of T is non empty.

We now state the proposition

(32) Let f, g be homeomorphisms of T and a, b be elements of the group of homeomorphisms of T. If $f = a$ and $g = b$, then $a \cdot b = g \cdot f$.

Let T be a non empty topological structure. Note that the group of homeomorphisms of T is group-like and associative.

The following two propositions are true:

(33) $\mathrm{id}_T = 1_{\text{the group of homeomorphisms of } T}$.

(34) Let f be a homeomorphism of T and a be an element of the group of homeomorphisms of T. If $f = a$, then $a^{-1} = f^{-1}$.

Let T be a non empty topological structure. We say that T is homogeneous if and only if:

(Def. 5) For all points p, q of T there exists a homeomorphism f of T such that $f(p) = q$.

Let us note that every non empty topological structure which is trivial is also homogeneous.

Let us note that there exists a topological space which is strict, trivial, and non empty.

One can prove the following two propositions:

(35) Let T be a homogeneous non empty topological space. If there exists a point p of T such that $\{p\}$ is closed, then T is a T_1 space.

(36) Let T be a homogeneous non empty topological space. Given a point p of T such that let A be a subset of T. Suppose A is open and $p \in A$. Then there exists a subset B of T such that $p \in B$ and B is open and $\overline{B} \subseteq A$. Then T is a T_3 space.

5. On the Topological Groups

We consider topological group structures as extensions of groupoid and topological structure as systems

$\langle$ a carrier, a multiplication, a topology $\rangle$,

where the carrier is a set, the multiplication is a binary operation on the carrier, and the topology is a family of subsets of the carrier.

Let A be a non empty set, let R be a binary operation on A, and let T be a family of subsets of A. Note that $\langle A, R, T\rangle$ is non empty.

Let x be a set, let R be a binary operation on $\{x\}$, and let T be a family of subsets of $\{x\}$. One can verify that $\langle \{x\}, R, T \rangle$ is trivial.

Let us observe that every non empty groupoid which is trivial is also group-like, associative, and commutative.

Let a be a set. Observe that $\{a\}_{\mathrm{top}}$ is trivial.

Let us note that there exists a topological group structure which is strict and non empty.

One can verify that there exists a non empty topological group structure which is strict, topological space-like, and trivial.

Let G be a group-like associative non empty topological group structure. Then $\cdot_G^{-1}$ is a map from G into G.

Let G be a group-like associative non empty topological group structure. We say that G is inverse-continuous if and only if:

(Def. 6) $\cdot_G^{-1}$ is continuous.

Let G be a topological space-like topological group structure. We say that G is continuous if and only if:

(Def. 7) For every map f from $[\!: G, G :\!]$ into G such that $f =$ the multiplication of G holds f is continuous.

One can verify that there exists a topological space-like group-like associative non empty topological group structure which is strict, commutative, trivial, inverse-continuous, and continuous.

A semi topological group is a topological space-like group-like associative non empty topological group structure.

A topological group is an inverse-continuous continuous semi topological group.

Next we state several propositions:

(37) Let T be a continuous non empty topological space-like topological group structure, a, b be elements of the carrier of T, and W be a neighbourhood of $a \cdot b$. Then there exists an open neighbourhood A of a and there exists an open neighbourhood B of b such that $A \cdot B \subseteq W$.

(38) Let T be a topological space-like non empty topological group structure. Suppose that for all elements a, b of the carrier of T and for every neighbourhood W of $a \cdot b$ there exists a neighbourhood A of a and there exists a neighbourhood B of b such that $A \cdot B \subseteq W$. Then T is continuous.

(39) Let T be an inverse-continuous semi topological group, a be an element of the carrier of T, and W be a neighbourhood of a^{-1}. Then there exists an open neighbourhood A of a such that $A^{-1} \subseteq W$.

(40) Let T be a semi topological group. Suppose that for every element a of the carrier of T and for every neighbourhood W of a^{-1} there exists a neighbourhood A of a such that $A^{-1} \subseteq W$. Then T is inverse-continuous.

(41) Let T be a topological group, a, b be elements of the carrier of T, and W be a neighbourhood of $a \cdot b^{-1}$. Then there exists an open neighbourhood A of a and there exists an open neighbourhood B of b such that $A \cdot B^{-1} \subseteq W$.

(42) Let T be a semi topological group. Suppose that for all elements a, b of the carrier of T and for every neighbourhood W of $a \cdot b^{-1}$ there exists a neighbourhood A of a and there exists a neighbourhood B of b such that $A \cdot B^{-1} \subseteq W$. Then T is a topological group.

Let G be a continuous non empty topological space-like topological group structure and let a be an element of the carrier of G. One can check that $a \cdot \square$ is continuous and $\square \cdot a$ is continuous.

Next we state two propositions:

(43) Let G be a continuous semi topological group and a be an element of the carrier of G. Then $a \cdot \square$ is a homeomorphism of G.

(44) Let G be a continuous semi topological group and a be an element of the carrier of G. Then $\square \cdot a$ is a homeomorphism of G.

The following proposition is true

(45) For every inverse-continuous semi topological group G holds $\cdot_G^{-1}$ is a homeomorphism of G.

One can verify that every semi topological group which is continuous is also homogeneous.

The following two propositions are true:

(46) Let G be a continuous semi topological group, F be a closed subset of G, and a be an element of the carrier of G. Then $F \cdot a$ is closed.

(47) Let G be a continuous semi topological group, F be a closed subset of G, and a be an element of the carrier of G. Then $a \cdot F$ is closed.

We now state the proposition

(48) For every inverse-continuous semi topological group G and for every closed subset F of G holds F^{-1} is closed.

The following two propositions are true:

(49) Let G be a continuous semi topological group, O be an open subset of G, and a be an element of the carrier of G. Then $O \cdot a$ is open.

(50) Let G be a continuous semi topological group, O be an open subset of G, and a be an element of the carrier of G. Then $a \cdot O$ is open.

We now state the proposition

(51) For every inverse-continuous semi topological group G and for every open subset O of G holds O^{-1} is open.

The following two propositions are true:

(52) For every continuous semi topological group G and for all subsets A, O of G such that O is open holds $O \cdot A$ is open.

(53) For every continuous semi topological group G and for all subsets A, O of G such that O is open holds $A \cdot O$ is open.

One can prove the following propositions:

(54) Let G be an inverse-continuous semi topological group, a be a point of G, and A be a neighbourhood of a. Then A^{-1} is a neighbourhood of a^{-1}.

(55) Let G be a topological group, a be a point of G, and A be a neighbourhood of $a \cdot a^{-1}$. Then there exists an open neighbourhood B of a such that $B \cdot B^{-1} \subseteq A$.

(56) For every inverse-continuous semi topological group G and for every dense subset A of G holds A^{-1} is dense.

We now state two propositions:

(57) Let G be a continuous semi topological group, A be a dense subset of G, and a be a point of G. Then $a \cdot A$ is dense.

(58) Let G be a continuous semi topological group, A be a dense subset of G, and a be a point of G. Then $A \cdot a$ is dense.

We now state two propositions:

(59) Let G be a topological group, B be a basis of 1_G, and M be a dense subset of G. Then $\{V \cdot x; V$ ranges over subsets of the carrier of G, x ranges over points of G: $V \in B \ \wedge \ x \in M\}$ is a basis of G.

(60) Every topological group is a T_3 space.

References

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

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

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

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

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

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

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

[8] Michał Muzalewski. Categories of groups. *Formalized Mathematics*, 2(**4**):563–571, 1991.

[9] Beata Padlewska. Locally connected spaces. *Formalized Mathematics*, 2(**1**):93–96, 1991.

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

[11] Alexander Yu. Shibakov and Andrzej Trybulec. The Cantor set. *Formalized Mathematics*, 5(**2**):233–236, 1996.

[12] Andrzej Trybulec. Baire spaces, Sober spaces. *Formalized Mathematics*, 6(**2**):289–294, 1997.

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

[14] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.

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

[16] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[17] Mirosław Wysocki and Agata Darmochwał. Subsets of topological spaces. *Formalized Mathematics*, 1(**1**):231–237, 1990.
[18] Mariusz Żynel and Adam Guzowski. T_0 topological spaces. *Formalized Mathematics*, 5(**1**):75–77, 1996.

Received September 7, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

The Correspondence Between Lattices of Subalgebras of Universal Algebras and Many Sorted Algebras

Adam Naumowicz
University of Białystok

Agnieszka Julia Marasik
Warsaw University of Technology

Summary. The main goal of this paper is to show some properties of subalgebras of universal algebras and many sorted algebras, and then the isomorphic correspondence between lattices of such subalgebras.

MML Identifier: `MSSUBLAT`.

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

1. Preliminaries

In this paper a denotes a set and i denotes a natural number.

We now state several propositions:

(1) $(\square \longmapsto a)(0) = \varepsilon$.

(2) $(\square \longmapsto a)(1) = \langle a \rangle$.

(3) $(\square \longmapsto a)(2) = \langle a, a \rangle$.

(4) $(\square \longmapsto a)(3) = \langle a, a, a \rangle$.

(5) For every finite sequence f of elements of $\{0\}$ holds $f = i \mapsto 0$ iff $\mathrm{len}\, f = i$.

(6) For every finite sequence f such that $f = (\square \longmapsto 0)(i)$ holds $\mathrm{len}\, f = i$.

ISSN 1426–2630

2. Some Properties of Subalgebras of Universal and Many Sorted Algebras

We now state the proposition

(7) For all universal algebras U_1, U_2 such that U_1 is a subalgebra of U_2 holds $\mathrm{MSSign}(U_1) = \mathrm{MSSign}(U_2)$.

Let U_0 be a universal algebra. One can verify that the characteristic of U_0 is function yielding.

One can prove the following propositions:

(8) Let U_1, U_2 be universal algebras. Suppose U_1 is a subalgebra of U_2. Let B be a subset of $\mathrm{MSAlg}(U_2)$. Suppose $B =$ the sorts of $\mathrm{MSAlg}(U_1)$. Let o be an operation symbol of $\mathrm{MSSign}(U_2)$ and a be an operation symbol of $\mathrm{MSSign}(U_1)$. If $a = o$, then $\mathrm{Den}(a, \mathrm{MSAlg}(U_1)) = \mathrm{Den}(o, \mathrm{MSAlg}(U_2)) \restriction \mathrm{Args}(a, \mathrm{MSAlg}(U_1))$.

(9) For all universal algebras U_1, U_2 such that U_1 is a subalgebra of U_2 holds the sorts of $\mathrm{MSAlg}(U_1)$ are a subset of $\mathrm{MSAlg}(U_2)$.

(10) Let U_1, U_2 be universal algebras. Suppose U_1 is a subalgebra of U_2. Let B be a subset of $\mathrm{MSAlg}(U_2)$. If $B =$ the sorts of $\mathrm{MSAlg}(U_1)$, then B is operations closed.

(11) Let U_1, U_2 be universal algebras. Suppose U_1 is a subalgebra of U_2. Let B be a subset of $\mathrm{MSAlg}(U_2)$. If $B =$ the sorts of $\mathrm{MSAlg}(U_1)$, then the characteristics of $\mathrm{MSAlg}(U_1) = \mathrm{Opers}(\mathrm{MSAlg}(U_2), B)$.

(12) For all universal algebras U_1, U_2 such that U_1 is a subalgebra of U_2 holds $\mathrm{MSAlg}(U_1)$ is a subalgebra of $\mathrm{MSAlg}(U_2)$.

(13) Let U_1, U_2 be universal algebras. Suppose $\mathrm{MSAlg}(U_1)$ is a subalgebra of $\mathrm{MSAlg}(U_2)$. Then the carrier of U_1 is a subset of the carrier of U_2.

(14) Let U_1, U_2 be universal algebras. Suppose $\mathrm{MSAlg}(U_1)$ is a subalgebra of $\mathrm{MSAlg}(U_2)$. Let B be a non empty subset of the carrier of U_2. If $B =$ the carrier of U_1, then B is operations closed.

(15) Let U_1, U_2 be universal algebras. Suppose $\mathrm{MSAlg}(U_1)$ is a subalgebra of $\mathrm{MSAlg}(U_2)$. Let B be a non empty subset of the carrier of U_2. If $B =$ the carrier of U_1, then the characteristic of $U_1 = \mathrm{Opers}(U_2, B)$.

(16) For all universal algebras U_1, U_2 such that $\mathrm{MSAlg}(U_1)$ is a subalgebra of $\mathrm{MSAlg}(U_2)$ holds U_1 is a subalgebra of U_2.

In the sequel M_1 is a segmental trivial non void non empty many sorted signature and A is a non-empty algebra over M_1.

Next we state a number of propositions:

(17) For every non-empty subalgebra B of A holds the carrier of $\mathrm{Alg}_{\mathbf{1}}(B)$ is a subset of the carrier of $\mathrm{Alg}_{\mathbf{1}}(A)$.

(18) Let B be a non-empty subalgebra of A and S be a non empty subset of the carrier of $\mathrm{Alg}_{\mathbf{1}}(A)$. If $S =$ the carrier of $\mathrm{Alg}_{\mathbf{1}}(B)$, then S is operations closed.

(19) Let B be a non-empty subalgebra of A and S be a non empty subset of the carrier of $\mathrm{Alg}_{\mathbf{1}}(A)$. If $S =$ the carrier of $\mathrm{Alg}_{\mathbf{1}}(B)$, then the characteristic of $\mathrm{Alg}_{\mathbf{1}}(B) = \mathrm{Opers}(\mathrm{Alg}_{\mathbf{1}}(A), S)$.

(20) For every non-empty subalgebra B of A holds $\mathrm{Alg}_{\mathbf{1}}(B)$ is a subalgebra of $\mathrm{Alg}_{\mathbf{1}}(A)$.

(21) Let S be a non empty non void many sorted signature and A, B be algebras over S. Then A is a subalgebra of B if and only if A is a subalgebra of the algebra of B.

(22) For all universal algebras A, B holds signature A = signature B iff $\mathrm{MSSign}(A) = \mathrm{MSSign}(B)$.

(23) Let A be a non-empty algebra over M_1. Suppose the carrier of $M_1 = \{0\}$. Then $\mathrm{MSSign}(\mathrm{Alg}_{\mathbf{1}}(A))$ = the many sorted signature of M_1.

(24) Let A, B be non-empty algebras over M_1. Suppose the carrier of $M_1 = \{0\}$ and $\mathrm{Alg}_{\mathbf{1}}(A) = \mathrm{Alg}_{\mathbf{1}}(B)$. Then the algebra of A = the algebra of B.

(25) Let A be a non-empty algebra over M_1. If the carrier of $M_1 = \{0\}$, then the sorts of A = the sorts of $\mathrm{MSAlg}(\mathrm{Alg}_{\mathbf{1}}(A))$.

(26) For every non-empty algebra A over M_1 such that the carrier of $M_1 = \{0\}$ holds $\mathrm{MSAlg}(\mathrm{Alg}_{\mathbf{1}}(A))$ = the algebra of A.

(27) Let A be a universal algebra and B be a strict non-empty subalgebra of $\mathrm{MSAlg}(A)$. If the carrier of $\mathrm{MSSign}(A) = \{0\}$, then $\mathrm{Alg}_{\mathbf{1}}(B)$ is a subalgebra of A.

3. The Correspondence Between Lattices of Subalgebras of Universal and Many Sorted Algebras

We now state three propositions:

(28) Let A be a universal algebra, a_1, b_1 be strict non-empty subalgebras of A, and a_2, b_2 be strict non-empty subalgebras of $\mathrm{MSAlg}(A)$. Suppose $a_2 = \mathrm{MSAlg}(a_1)$ and $b_2 = \mathrm{MSAlg}(b_1)$. Then (the sorts of a_2) $\cup$ (the sorts of b_2) $= 0 \dot{\longmapsto}$((the carrier of a_1) $\cup$ (the carrier of b_1)).

(29) Let A be a universal algebra, a_1, b_1 be strict non-empty subalgebras of A, and a_2, b_2 be strict non-empty subalgebras of $\mathrm{MSAlg}(A)$. Suppose $a_2 = \mathrm{MSAlg}(a_1)$ and $b_2 = \mathrm{MSAlg}(b_1)$. Then (the sorts of a_2) $\cap$ (the sorts of b_2) $= 0 \dot{\longmapsto}$(the carrier of a_1) $\cap$ (the carrier of b_1).

(30) Let A be a strict universal algebra, a_1, b_1 be strict non-empty subalgebras of A, and a_2, b_2 be strict non-empty subalgebras of MSAlg(A). If $a_2 =$ MSAlg(a_1) and $b_2 =$ MSAlg(b_1), then MSAlg($a_1 \bigsqcup b_1$) $= a_2 \bigsqcup b_2$.

Let A be a universal algebra with constants. One can check that MSSign(A) is non void strict segmental and trivial and has constant operations.

One can prove the following proposition

(31) Let A be a universal algebra with constants, a_1, b_1 be strict non-empty subalgebras of A, and a_2, b_2 be strict non-empty subalgebras of MSAlg(A). If $a_2 =$ MSAlg(a_1) and $b_2 =$ MSAlg(b_1), then MSAlg($a_1 \cap b_1$) $= a_2 \cap b_2$.

Let A be a quasi total universal algebra structure. One can verify that the universal algebra structure of A is quasi total.

Let A be a partial universal algebra structure. Observe that the universal algebra structure of A is partial.

Let A be a non-empty universal algebra structure. Note that the universal algebra structure of A is non-empty.

Let A be a universal algebra with constants. Note that the universal algebra structure of A has constants.

We now state the proposition

(32) Let A be a universal algebra with constants. Then the lattice of subalgebras of the universal algebra structure of A and the lattice of subalgebras of MSAlg(the universal algebra structure of A) are isomorphic.

References

[1] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[2] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[3] Ewa Burakowska. Subalgebras of the universal algebra. Lattices of subalgebras. *Formalized Mathematics*, 4(**1**):23–27, 1993.
[4] Ewa Burakowska. Subalgebras of many sorted algebra. Lattice of subalgebras. *Formalized Mathematics*, 5(**1**):47–54, 1996.
[5] Czesław Byliński. A classical first order language. *Formalized Mathematics*, 1(**4**):669–676, 1990.
[6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[10] Jolanta Kamieńska and Jarosław Stanisław Walijewski. Homomorphisms of lattices, finite join and finite meet. *Formalized Mathematics*, 4(**1**):35–40, 1993.
[11] Jarosław Kotowicz, Beata Madras, and Małgorzata Korolkiewicz. Basic notation of universal algebra. *Formalized Mathematics*, 3(**2**):251–253, 1992.
[12] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[13] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[14] Andrzej Trybulec. Many sorted algebras. *Formalized Mathematics*, 5(**1**):37–42, 1996.
[15] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[16] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[17] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received September 22, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Introduction to Concept Lattices

Christoph Schwarzweller
University of Tübingen

Summary. In this paper we give Mizar formalization of concept lattices. Concept lattices stem from the so called formal concept analysis — a part of applied mathematics that brings mathematical methods into the field of data anylysis and knowledge processing. Our approach follows the one given in [8].

MML Identifier: `CONLAT_1`.

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

1. Formal Contexts

We consider 2-sorted as systems
⟨ objects, a Attributes ⟩,
where the objects constitute a set and the Attributes is a set.

Let C be a 2-sorted. We say that C is empty if and only if:

(Def. 1) The objects of C are empty and the Attributes of C is empty.

We say that C is quasi-empty if and only if:

(Def. 2) The objects of C are empty or the Attributes of C is empty.

Let us note that there exists a 2-sorted which is strict and non empty and there exists a 2-sorted which is strict and non quasi-empty.

One can verify that there exists a 2-sorted which is strict, empty, and quasi-empty.

We consider ContextStr as extensions of 2-sorted as systems
⟨ objects, a Attributes, a Information ⟩,
where the objects constitute a set, the Attributes is a set, and the Information is a relation between the objects and the Attributes.

ISSN 1426–2630

One can check that there exists a ContextStr which is strict and non empty and there exists a ContextStr which is strict and non quasi-empty.

A FormalContext is a non quasi-empty ContextStr.

Let C be a 2-sorted.

(Def. 3) An element of the objects of C is said to be an object of C.

(Def. 4) An element of the Attributes of C is said to be a Attribute of C.

Let C be a non quasi-empty 2-sorted. Note that the Attributes of C is non empty and the objects of C is non empty.

Let C be a non quasi-empty 2-sorted. One can check that there exists a subset of the objects of C which is non empty and there exists a subset of the Attributes of C which is non empty.

Let C be a FormalContext, let o be an object of C, and let a be a Attribute of C. We say that o is connected with a if and only if:

(Def. 5) $\langle o, a \rangle \in$ the Information of C.

We introduce o is not connected with a as an antonym of o is connected with a.

2. Derivation Operators

Let C be a FormalContext. The functor ObjectDerivation C yields a function from $2^{\text{the objects of } C}$ into $2^{\text{the Attributes of } C}$ and is defined by the condition (Def. 6).

(Def. 6) Let O be an element of $2^{\text{the objects of } C}$. Then $(\text{ObjectDerivation}\, C)(O) = \{a; a$ ranges over Attribute of C: $\bigwedge_{o\,:\,\text{object of } C} (o \in O \Rightarrow o$ is connected with $a)\}$.

Let C be a FormalContext. The functor AttributeDerivation C yields a function from $2^{\text{the Attributes of } C}$ into $2^{\text{the objects of } C}$ and is defined by the condition (Def. 7).

(Def. 7) Let A be an element of $2^{\text{the Attributes of } C}$. Then $(\text{AttributeDerivation}\, C)(A) = \{o; o$ ranges over objects of C: $\bigwedge_{a\,:\,\text{Attribute of } C} (a \in A \Rightarrow o$ is connected with $a)\}$.

The following propositions are true:

(1) Let C be a FormalContext and o be an object of C. Then $(\text{ObjectDerivation}\, C)(\{o\}) = \{a; a$ ranges over Attribute of C: o is connected with $a\}$.

(2) Let C be a FormalContext and a be a Attribute of C. Then $(\text{AttributeDerivation}\, C)(\{a\}) = \{o; o$ ranges over objects of C: o is connected with $a\}$.

(3) For every FormalContext C and for all subsets O_1, O_2 of the objects of C such that $O_1 \subseteq O_2$ holds $(\mathrm{ObjectDerivation}\, C)(O_2) \subseteq (\mathrm{ObjectDerivation}\, C)(O_1)$.

(4) For every FormalContext C and for all subsets A_1, A_2 of the Attributes of C such that $A_1 \subseteq A_2$ holds $(\mathrm{AttributeDerivation}\, C)(A_2) \subseteq (\mathrm{AttributeDerivation}\, C)(A_1)$.

(5) For every FormalContext C and for every subset O of the objects of C holds $O \subseteq (\mathrm{AttributeDerivation}\, C)((\mathrm{ObjectDerivation}\, C)(O))$.

(6) For every FormalContext C and for every subset A of the Attributes of C holds $A \subseteq (\mathrm{ObjectDerivation}\, C)((\mathrm{AttributeDerivation}\, C)(A))$.

(7) For every FormalContext C and for every subset O of the objects of C holds $(\mathrm{ObjectDerivation}\, C)(O) = (\mathrm{ObjectDerivation}\, C)$ $((\mathrm{AttributeDerivation}\, C)((\mathrm{ObjectDerivation}\, C)(O)))$.

(8) For every FormalContext C and for every subset A of the Attributes of C holds $(\mathrm{AttributeDerivation}\, C)(A) =$ $(\mathrm{AttributeDerivation}\, C)((\mathrm{ObjectDerivation}\, C)((\mathrm{AttributeDerivation}\, C)(A)))$.

(9) Let C be a FormalContext, O be a subset of the objects of C, and A be a subset of the Attributes of C. Then $O \subseteq (\mathrm{AttributeDerivation}\, C)(A)$ if and only if $[\!:O, A:\!] \subseteq$ the Information of C.

(10) Let C be a FormalContext, O be a subset of the objects of C, and A be a subset of the Attributes of C. Then $A \subseteq (\mathrm{ObjectDerivation}\, C)(O)$ if and only if $[\!:O, A:\!] \subseteq$ the Information of C.

(11) Let C be a FormalContext, O be a subset of the objects of C, and A be a subset of the Attributes of C. Then $O \subseteq (\mathrm{AttributeDerivation}\, C)(A)$ if and only if $A \subseteq (\mathrm{ObjectDerivation}\, C)(O)$.

Let C be a FormalContext. The functor $\phi(C)$ yielding a map from $2_{\subseteq}^{\text{the objects of } C}$ into $2_{\subseteq}^{\text{the Attributes of } C}$ is defined by:

(Def. 8) $\phi(C) = \mathrm{ObjectDerivation}\, C$.

Let C be a FormalContext. The functor $\mathrm{psi}\, C$ yields a map from $2_{\subseteq}^{\text{the Attributes of } C}$ into $2_{\subseteq}^{\text{the objects of } C}$ and is defined as follows:

(Def. 9) $\mathrm{psi}\, C = \mathrm{AttributeDerivation}\, C$.

We now state the proposition

(12) For every FormalContext C holds $\langle \phi(C), \mathrm{psi}\, C \rangle$ is a connection between $2_{\subseteq}^{\text{the objects of } C}$ and $2_{\subseteq}^{\text{the Attributes of } C}$.

Let P, R be non empty relational structures and let C_1 be a connection between P and R. We say that C_1 is co-Galois if and only if the condition (Def. 10) is satisfied.

(Def. 10) There exists a map f from P into R and there exists a map g from R into P such that

(i) $C_1 = \langle f, g \rangle$,
(ii) f is antitone,
(iii) g is antitone, and
(iv) for all elements p_1, p_2 of P and for all elements r_1, r_2 of R holds $p_1 \leqslant g(f(p_1))$ and $r_1 \leqslant f(g(r_1))$.

We now state several propositions:

(13) Let P, R be non empty posets, C_1 be a connection between P and R, f be a map from P into R, and g be a map from R into P. Suppose $C_1 = \langle f, g \rangle$. Then C_1 is co-Galois if and only if for every element p of P and for every element r of R holds $p \leqslant g(r)$ iff $r \leqslant f(p)$.

(14) Let P, R be non empty posets and C_1 be a connection between P and R. Suppose C_1 is co-Galois. Let f be a map from P into R and g be a map from R into P. If $C_1 = \langle f, g \rangle$, then $f = f \cdot (g \cdot f)$ and $g = g \cdot (f \cdot g)$.

(15) For every FormalContext C holds $\langle \phi(C), \mathrm{psi}\, C \rangle$ is co-Galois.

(16) For every FormalContext C and for all subsets O_1, O_2 of the objects of C holds $(\mathrm{ObjectDerivation}\, C)(O_1 \cup O_2) = (\mathrm{ObjectDerivation}\, C)(O_1) \cap (\mathrm{ObjectDerivation}\, C)(O_2)$.

(17) For every FormalContext C and for all subsets A_1, A_2 of the Attributes of C holds $(\mathrm{AttributeDerivation}\, C)(A_1 \cup A_2) = (\mathrm{AttributeDerivation}\, C)(A_1) \cap (\mathrm{AttributeDerivation}\, C)(A_2)$.

(18) For every FormalContext C holds $(\mathrm{ObjectDerivation}\, C)(\emptyset) =$ the Attributes of C.

(19) For every FormalContext C holds $(\mathrm{AttributeDerivation}\, C)(\emptyset) =$ the objects of C.

3. Formal Concepts

Let C be a 2-sorted. We introduce ConceptStr over C which are systems

⟨ a Extent, a Intent ⟩,

where the Extent is a subset of the objects of C and the Intent is a subset of the Attributes of C.

Let C be a 2-sorted and let C_2 be a ConceptStr over C. We say that C_2 is empty if and only if:

(Def. 11) The Extent of C_2 is empty and the Intent of C_2 is empty.

We say that C_2 is quasi-empty if and only if:

(Def. 12) The Extent of C_2 is empty or the Intent of C_2 is empty.

Let C be a non quasi-empty 2-sorted. Observe that there exists a ConceptStr over C which is strict and non empty and there exists a ConceptStr over C which is strict and quasi-empty.

Let C be an empty 2-sorted. Observe that every ConceptStr over C is empty.

Let C be a quasi-empty 2-sorted. Observe that every ConceptStr over C is quasi-empty.

Let C be a FormalContext and let C_2 be a ConceptStr over C. We say that C_2 is concept-like if and only if:

(Def. 13) (ObjectDerivation C)(the Extent of C_2) = the Intent of C_2 and (AttributeDerivation C)(the Intent of C_2) = the Extent of C_2.

Let C be a FormalContext. One can check that there exists a ConceptStr over C which is concept-like and non empty.

Let C be a FormalContext. A FormalConcept of C is a concept-like non empty ConceptStr over C.

Let C be a FormalContext. Note that there exists a FormalConcept of C which is strict.

Next we state four propositions:

(20) Let C be a FormalContext and O be a subset of the objects of C. Then
  (i) $\langle$(AttributeDerivation C)((ObjectDerivation C)(O)), (ObjectDerivation C)(O)$\rangle$ is a FormalConcept of C, and
  (ii) for every subset O' of the objects of C and for every subset A' of the Attributes of C such that $\langle O', A'\rangle$ is a FormalConcept of C and $O \subseteq O'$ holds (AttributeDerivation C)((ObjectDerivation C)(O)) $\subseteq O'$.

(21) Let C be a FormalContext and O be a subset of the objects of C. Then there exists a subset A of the Attributes of C such that $\langle O, A\rangle$ is a FormalConcept of C if and only if (AttributeDerivation C)((ObjectDerivation C)(O)) $= O$.

(22) Let C be a FormalContext and A be a subset of the Attributes of C. Then
  (i) $\langle$(AttributeDerivation C)(A), (ObjectDerivation C) ((AttributeDerivation C)(A))$\rangle$ is a FormalConcept of C, and
  (ii) for every subset O' of the objects of C and for every subset A' of the Attributes of C such that $\langle O', A'\rangle$ is a FormalConcept of C and $A \subseteq A'$ holds (ObjectDerivation C)((AttributeDerivation C)(A)) $\subseteq A'$.

(23) Let C be a FormalContext and A be a subset of the Attributes of C. Then there exists a subset O of the objects of C such that $\langle O, A\rangle$ is a FormalConcept of C if and only if (ObjectDerivation C)((AttributeDerivation C)(A)) $= A$.

Let C be a FormalContext and let C_2 be a ConceptStr over C. We say that C_2 is universal if and only if:

(Def. 14) The Extent of C_2 = the objects of C.

Let C be a FormalContext and let C_2 be a ConceptStr over C. We say that C_2 is co-universal if and only if:

(Def. 15) The Intent of C_2 = the Attributes of C.

Let C be a FormalContext. Note that there exists a FormalConcept of C which is strict and universal and there exists a FormalConcept of C which is strict and co-universal.

Let C be a FormalContext. The functor Concept − with − all − Objects C yields a strict universal FormalConcept of C and is defined by the condition (Def. 16).

(Def. 16) There exists a subset O of the objects of C and there exists a subset A of the Attributes of C such that Concept − with − all − Objects $C = \langle O, A\rangle$ and $O =$ (AttributeDerivation C)$(\emptyset)$ and $A =$ (ObjectDerivation C)((AttributeDerivation C)$(\emptyset)$).

Let C be a FormalContext. The functor Concept − with − all − Attributes C yielding a strict co-universal FormalConcept of C is defined by the condition (Def. 17).

(Def. 17) There exists a subset O of the objects of C and there exists a subset A of the Attributes of C such that Concept − with − all − Attributes C = $\langle O, A\rangle$ and O = (AttributeDerivation C)((ObjectDerivation C)$(\emptyset)$) and A = (ObjectDerivation C)$(\emptyset)$.

One can prove the following propositions:

(24) Let C be a FormalContext. Then the Extent of Concept − with − all − Objects C = the objects of C and the Intent of Concept − with − all − Attributes C = the Attributes of C.

(25) Let C be a FormalContext and C_2 be a FormalConcept of C. Then
(i) if the Extent of $C_2 = \emptyset$, then C_2 is co-universal, and
(ii) if the Intent of $C_2 = \emptyset$, then C_2 is universal.

(26) Let C be a FormalContext and C_2 be a strict FormalConcept of C. Then
(i) if the Extent of $C_2 = \emptyset$, then C_2 = Concept − with − all − Attributes C, and
(ii) if the Intent of $C_2 = \emptyset$, then C_2 = Concept − with − all − Objects C.

(27) Let C be a FormalContext and C_2 be a quasi-empty ConceptStr over C. Suppose C_2 is a FormalConcept of C. Then C_2 is universal or co-universal.

(28) Let C be a FormalContext and C_2 be a quasi-empty ConceptStr over C. If C_2 is a strict FormalConcept of C, then C_2 = Concept − with − all − Objects C or C_2 = Concept − with − all − Attributes C.

Let C be a FormalContext. A non empty set is called a Set of FormalConcepts of C if:

(Def. 18) For every set X such that $X \in$ it holds X is a FormalConcept of C.

Let C be a FormalContext and let F_1 be a Set of FormalConcepts of C. We see that the element of F_1 is a FormalConcept of C.

Let C be a FormalContext and let C_3, C_4 be FormalConcept of C. We say that C_3 is SubConcept of C_4 if and only if:

(Def. 19) The Extent of $C_3 \subseteq$ the Extent of C_4.

We introduce C_4 is SuperConcept of C_3 as a synonym of C_3 is SubConcept of C_4.

One can prove the following propositions:

(29) Let C be a FormalContext and C_3, C_4 be FormalConcept of C. Then C_3 is SuperConcept of C_4 if and only if C_4 is SubConcept of C_3.

(30) Let C be a FormalContext and C_3, C_4 be FormalConcept of C. Then C_3 is SubConcept of C_4 if and only if the Extent of $C_3 \subseteq$ the Extent of C_4.

(31) Let C be a FormalContext and C_3, C_4 be FormalConcept of C. Then C_3 is SubConcept of C_4 if and only if the Intent of $C_4 \subseteq$ the Intent of C_3.

(32) Let C be a FormalContext and C_3, C_4 be FormalConcept of C. Then C_3 is SuperConcept of C_4 if and only if the Extent of $C_4 \subseteq$ the Extent of C_3.

(33) Let C be a FormalContext and C_3, C_4 be FormalConcept of C. Then C_3 is SuperConcept of C_4 if and only if the Intent of $C_3 \subseteq$ the Intent of C_4.

(34) Let C be a FormalContext and C_2 be a FormalConcept of C. Then C_2 is SubConcept of $\mathrm{Concept-with-all-Objects}\,C$ and $\mathrm{Concept-with-all-Attributes}\,C$ is SubConcept of C_2.

4. Concept Lattices

Let C be a FormalContext. The functor $\mathrm{B-carrier}\,C$ yielding a non empty set is defined by the condition (Def. 20).

(Def. 20) $\mathrm{B-carrier}\,C = \{\langle E, I\rangle; E$ ranges over subsets of the objects of C, I ranges over subsets of the Attributes of C: $\langle E, I\rangle$ is non empty $\wedge$ $(\mathrm{ObjectDerivation}\,C)(E) = I \ \wedge \ (\mathrm{AttributeDerivation}\,C)(I) = E\}$.

Let C be a FormalContext. Then $\mathrm{B-carrier}\,C$ is a Set of FormalConcepts of C.

Let C be a FormalContext. One can check that $\mathrm{B-carrier}\,C$ is non empty.

One can prove the following proposition

(35) For every FormalContext C and for every set C_2 holds $C_2 \in \mathrm{B-carrier}\,C$ iff C_2 is a strict FormalConcept of C.

Let C be a FormalContext. The functor $\mathrm{B-meet}\,C$ yields a binary operation on $\mathrm{B-carrier}\,C$ and is defined by the condition (Def. 21).

(Def. 21) Let C_3, C_4 be strict FormalConcept of C. Then there exists a subset O of the objects of C and there exists a subset A of the Attributes of C such that

$(\mathrm{B}-\mathrm{meet}\,C)(C_3, C_4) = \langle O, A\rangle$ and $O =$ (the Extent of C_3) $\cap$ (the Extent of C_4) and $A =$ (ObjectDerivation C)((AttributeDerivation C)((the Intent of C_3) $\cup$ (the Intent of C_4))).

Let C be a FormalContext. The functor $\mathrm{B}-\mathrm{join}\,C$ yielding a binary operation on $\mathrm{B}-\mathrm{carrier}\,C$ is defined by the condition (Def. 22).

(Def. 22) Let C_3, C_4 be strict FormalConcept of C. Then there exists a subset O of the objects of C and there exists a subset A of the Attributes of C such that $(\mathrm{B}-\mathrm{join}\,C)(C_3, C_4) = \langle O, A\rangle$ and $O =$ (AttributeDerivation C)((ObjectDerivation C)((the Extent of C_3) $\cup$ (the Extent of C_4))) and $A =$ (the Intent of C_3) $\cap$ (the Intent of C_4).

One can prove the following propositions:

(36) For every FormalContext C and for all strict FormalConcept C_3, C_4 of C holds $(\mathrm{B}-\mathrm{meet}\,C)(C_3, C_4) = (\mathrm{B}-\mathrm{meet}\,C)(C_4, C_3)$.

(37) For every FormalContext C and for all strict FormalConcept C_3, C_4 of C holds $(\mathrm{B}-\mathrm{join}\,C)(C_3, C_4) = (\mathrm{B}-\mathrm{join}\,C)(C_4, C_3)$.

(38) For every FormalContext C and for all strict FormalConcept C_3, C_4, C_5 of C holds $(\mathrm{B}-\mathrm{meet}\,C)(C_3, (\mathrm{B}-\mathrm{meet}\,C)(C_4, C_5)) = (\mathrm{B}-\mathrm{meet}\,C)((\mathrm{B}-\mathrm{meet}\,C)(C_3, C_4), C_5)$.

(39) For every FormalContext C and for all strict FormalConcept C_3, C_4, C_5 of C holds $(\mathrm{B}-\mathrm{join}\,C)(C_3, (\mathrm{B}-\mathrm{join}\,C)(C_4, C_5)) = (\mathrm{B}-\mathrm{join}\,C)((\mathrm{B}-\mathrm{join}\,C)(C_3, C_4), C_5)$.

(40) For every FormalContext C and for all strict FormalConcept C_3, C_4 of C holds $(\mathrm{B}-\mathrm{join}\,C)((\mathrm{B}-\mathrm{meet}\,C)(C_3, C_4), C_4) = C_4$.

(41) For every FormalContext C and for all strict FormalConcept C_3, C_4 of C holds $(\mathrm{B}-\mathrm{meet}\,C)(C_3, (\mathrm{B}-\mathrm{join}\,C)(C_3, C_4)) = C_3$.

(42) For every FormalContext C and for every strict FormalConcept C_2 of C holds $(\mathrm{B}-\mathrm{meet}\,C)(C_2, \mathrm{Concept}-\mathrm{with}-\mathrm{all}-\mathrm{Objects}\,C) = C_2$.

(43) For every FormalContext C and for every strict FormalConcept C_2 of C holds $(\mathrm{B}-\mathrm{join}\,C)(C_2, \mathrm{Concept}-\mathrm{with}-\mathrm{all}-\mathrm{Objects}\,C) = \mathrm{Concept}-\mathrm{with}-\mathrm{all}-\mathrm{Objects}\,C$.

(44) For every FormalContext C and for every strict FormalConcept C_2 of C holds $(\mathrm{B}-\mathrm{join}\,C)(C_2, \mathrm{Concept}-\mathrm{with}-\mathrm{all}-\mathrm{Attributes}\,C) = C_2$.

(45) For every FormalContext C and for every strict FormalConcept C_2 of C holds $(\mathrm{B}-\mathrm{meet}\,C)(C_2, \mathrm{Concept}-\mathrm{with}-\mathrm{all}-\mathrm{Attributes}\,C) = \mathrm{Concept}-\mathrm{with}-\mathrm{all}-\mathrm{Attributes}\,C$.

Let C be a FormalContext. The functor ConceptLattice C yielding a strict non empty lattice structure is defined as follows:

(Def. 23) $\mathrm{ConceptLattice}\,C = \langle \mathrm{B}-\mathrm{carrier}\,C, \mathrm{B}-\mathrm{join}\,C, \mathrm{B}-\mathrm{meet}\,C\rangle$.

The following proposition is true

(46) For every FormalContext C holds ConceptLattice C is a lattice.

Let C be a FormalContext. One can verify that ConceptLattice C is strict non empty and lattice-like.

Let C be a FormalContext and let S be a non empty subset of the carrier of ConceptLattice C. We see that the element of S is a FormalConcept of C.

Let C be a FormalContext and let C_2 be an element of the carrier of ConceptLattice C. The functor ${C_2}^{\mathrm{T}}$ yielding a strict FormalConcept of C is defined as follows:

(Def. 24) ${C_2}^{\mathrm{T}} = C_2$.

One can prove the following two propositions:

(47) Let C be a FormalContext and C_3, C_4 be elements of the carrier of ConceptLattice C. Then $C_3 \sqsubseteq C_4$ if and only if ${C_3}^{\mathrm{T}}$ is SubConcept of ${C_4}^{\mathrm{T}}$.

(48) For every FormalContext C holds ConceptLattice C is a complete lattice.

Let C be a FormalContext. Observe that ConceptLattice C is complete.

References

[1] Grzegorz Bancerek. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.
[2] Grzegorz Bancerek. Directed sets, nets, ideals, filters, and maps. *Formalized Mathematics*, 6(**1**):93–107, 1997.
[3] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[7] Czesław Byliński. Galois connections. *Formalized Mathematics*, 6(**1**):131–143, 1997.
[8] Bernhard Ganter and Rudolf Wille. *Formal Concept Analysis*. Springer Verlag, Berlin, Heidelberg, Ney York, 1996. (written in German).
[9] Adam Grabowski and Robert Milewski. Boolean posets, posets under inclusion and products of relational structures. *Formalized Mathematics*, 6(**1**):117–121, 1997.
[10] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[11] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[12] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[13] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[14] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[15] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

Received October 2, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

A Theory of Partitions. Part I

Shunichi Kobayashi
Shinshu University
Nagano

Kui Jia
Shinshu University
Nagano

Summary. In this paper, we define join and meet operations between partitions. The properties of these operations are proved. Then we introduce the correspondence between partitions and equivalence relations which preserve join and meet operations. The properties of these relationships are proved.

MML Identifier: `PARTIT1`.

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

1. Preliminaries

For simplicity, we use the following convention: Y is a non empty set, P_1, P_2 are partitions of Y, A, B are subsets of Y, i is a natural number, x, y, x_1, x_2, z_0 are sets, and X, V, d, t, S_1, S_2 are sets.

The following proposition is true

(1) If $X \in P_1$ and $V \in P_1$ and $X \subseteq V$, then $X = V$.

Let us consider S_1, S_2. We introduce $S_1 \Subset S_2$ and $S_2 \Supset S_1$ as synonyms of S_1 is finer than S_2.

We now state several propositions:

(2) For every partition P_1 of Y holds $P_1 \Supset P_1$.

(3) $\bigcup(S_1 \setminus \{\emptyset\}) = \bigcup S_1$.

(4) For all partitions P_1, P_2 of Y such that $P_1 \Supset P_2$ and $P_2 \Supset P_1$ holds $P_2 \subseteq P_1$.

(5) For all partitions P_1, P_2 of Y such that $P_1 \Supset P_2$ and $P_2 \Supset P_1$ holds $P_1 = P_2$.

ISSN 1426–2630

(7)[1] For all partitions P_1, P_2 of Y such that $P_1 \Supset P_2$ holds P_1 is coarser than P_2.

Let us consider Y, let P_1 be a partition of Y, and let b be a set. We say that b is a dependent set of P_1 if and only if:

(Def. 1) There exists a set B such that $B \subseteq P_1$ and $B \neq \emptyset$ and $b = \bigcup B$.

Let us consider Y, let P_1, P_2 be partitions of Y, and let b be a set. We say that b is a minimal dependent set of P_1 and P_2 if and only if the conditions (Def. 2) are satisfied.

(Def. 2)(i) b is a dependent set of P_1 and a dependent set of P_2, and

(ii) for every set d such that $d \subseteq b$ and d is a dependent set of P_1 and a dependent set of P_2 holds $d = b$.

We now state several propositions:

(8) For all partitions P_1, P_2 of Y such that $P_1 \Supset P_2$ and for every set b such that $b \in P_1$ holds b is a dependent set of P_2.

(9) For every partition P_1 of Y holds Y is a dependent set of P_1.

(10) Let F be a family of subsets of Y. Suppose $\mathrm{Intersect}(F) \neq \emptyset$ and for every X such that $X \in F$ holds X is a dependent set of P_1. Then $\mathrm{Intersect}(F)$ is a dependent set of P_1.

(11) Let X_0, X_1 be subsets of Y. Suppose X_0 is a dependent set of P_1 and X_1 is a dependent set of P_1 and X_0 meets X_1. Then $X_0 \cap X_1$ is a dependent set of P_1.

(12) For every subset X of Y such that X is a dependent set of P_1 and $X \neq Y$ holds X^{c} is a dependent set of P_1.

(13) For every element y of Y there exists a subset X of Y such that $y \in X$ and X is a minimal dependent set of P_1 and P_2.

(14) For every partition P of Y and for every element y of Y there exists a subset A of Y such that $y \in A$ and $A \in P$.

Let Y be a non empty set. One can verify that every partition of Y is non empty.

Let Y be a set. The functor $\mathrm{PARTITIONS}(Y)$ is defined by:

(Def. 3) For every set x holds $x \in \mathrm{PARTITIONS}(Y)$ iff x is a partition of Y.

Let Y be a set. One can check that $\mathrm{PARTITIONS}(Y)$ is non empty.

2. Join and Meet Operation Between Partitions

Let us consider Y and let P_1, P_2 be partitions of Y. The functor $P_1 \wedge P_2$ yielding a partition of Y is defined by:

[1]The proposition (6) has been removed.

(Def. 4) $P_1 \wedge P_2 = P_1 \Cap P_2 \setminus \{\emptyset\}$.

Let us observe that the functor $P_1 \wedge P_2$ is commutative.

One can prove the following propositions:

(15) For every partition P_1 of Y holds $P_1 \wedge P_1 = P_1$.

(16) For all partitions P_1, P_2, P_3 of Y holds $P_1 \wedge P_2 \wedge P_3 = P_1 \wedge P_2 \wedge P_3$.

(17) For all partitions P_1, P_2 of Y holds $P_1 \Supset P_1 \wedge P_2$.

(18) For all partitions P_1, P_2, P_3 of Y such that $P_1 \Supset P_2$ and $P_2 \Supset P_3$ holds $P_1 \Supset P_3$.

Let us consider Y and let P_1, P_2 be partitions of Y. The functor $P_1 \vee P_2$ yielding a partition of Y is defined by:

(Def. 5) For every d holds $d \in P_1 \vee P_2$ iff d is a minimal dependent set of P_1 and P_2.

Let us observe that the functor $P_1 \vee P_2$ is commutative.

One can prove the following propositions:

(19) For all partitions P_1, P_2 of Y holds $P_1 \Subset P_1 \vee P_2$.

(20) For every partition P_1 of Y holds $P_1 \vee P_1 = P_1$.

(21) For all partitions P_1, P_3 of Y such that $P_1 \Subset P_3$ and $x \in P_3$ and $z_0 \in P_1$ and $t \in x$ and $t \in z_0$ holds $z_0 \subseteq x$.

(22) For all partitions P_1, P_2 of Y such that $x \in P_1 \vee P_2$ and $z_0 \in P_1$ and $t \in x$ and $t \in z_0$ holds $z_0 \subseteq x$.

3. Partitions and Equivalence Relations

We now state the proposition

(23) Let P_1 be a partition of Y. Then there exists an equivalence relation R_1 of Y such that for all x, y holds $\langle x, y\rangle \in R_1$ if and only if the following conditions are satisfied:
  - (i) $x \in Y$,
  - (ii) $y \in Y$, and
  - (iii) there exists A such that $A \in P_1$ and $x \in A$ and $y \in A$.

Let us consider Y. The functor $\mathrm{Rel}(Y)$ yields a function and is defined by the conditions (Def. 6).

(Def. 6)(i) $\mathrm{dom}\,\mathrm{Rel}(Y) = \mathrm{PARTITIONS}(Y)$, and

(ii) for every x such that $x \in \mathrm{PARTITIONS}(Y)$ there exists an equivalence relation R_1 of Y such that $(\mathrm{Rel}(Y))(x) = R_1$ and for all sets x_1, x_2 holds $\langle x_1, x_2\rangle \in R_1$ iff $x_1 \in Y$ and $x_2 \in Y$ and there exists A such that $A \in x$ and $x_1 \in A$ and $x_2 \in A$.

Let Y be a non empty set and let P_1 be a partition of Y. The functor $\equiv_{(P_1)}$ yielding an equivalence relation of Y is defined as follows:

(Def. 7) $\equiv_{(P_1)} = (\mathrm{Rel}(Y))(P_1)$.

The following propositions are true:

(24) For all partitions P_1, P_2 of Y holds $P_1 \Subset P_2$ iff $\equiv_{(P_1)} \subseteq \equiv_{(P_2)}$.

(25) Let P_1, P_2 be partitions of Y, p_0, x, y be sets, and f be a finite sequence of elements of Y. Suppose that

(i) $p_0 \subseteq Y$,
(ii) $x \in p_0$,
(iii) $f(1) = x$,
(iv) $f(\mathrm{len}\, f) = y$,
(v) $1 \leqslant \mathrm{len}\, f$,
(vi) for every i such that $1 \leqslant i$ and $i < \mathrm{len}\, f$ there exist sets p_2, p_3, u such that $p_2 \in P_1$ and $p_3 \in P_2$ and $f(i) \in p_2$ and $u \in p_2$ and $u \in p_3$ and $f(i+1) \in p_3$, and
(vii) p_0 is a dependent set of P_1 and a dependent set of P_2.

Then $y \in p_0$.

(26) Let R_2, R_3 be equivalence relations of Y, f be a finite sequence of elements of Y, and x, y be sets. Suppose that

(i) $x \in Y$,
(ii) $y \in Y$,
(iii) $f(1) = x$,
(iv) $f(\mathrm{len}\, f) = y$,
(v) $1 \leqslant \mathrm{len}\, f$, and
(vi) for every i such that $1 \leqslant i$ and $i < \mathrm{len}\, f$ there exists a set u such that $u \in Y$ and $\langle f(i), u\rangle \in R_2 \cup R_3$ and $\langle u, f(i+1)\rangle \in R_2 \cup R_3$.

Then $\langle x, y\rangle \in R_2 \sqcup R_3$.

(27) For all partitions P_1, P_2 of Y holds $\equiv_{P_1 \vee P_2} = \equiv_{(P_1)} \sqcup \equiv_{(P_2)}$.

(28) For all partitions P_1, P_2 of Y holds $\equiv_{P_1 \wedge P_2} = \equiv_{(P_1)} \cap \equiv_{(P_2)}$.

(29) For all partitions P_1, P_2 of Y such that $\equiv_{(P_1)} = \equiv_{(P_2)}$ holds $P_1 = P_2$.

(30) For all partitions P_1, P_2, P_3 of Y holds $P_1 \vee P_2 \vee P_3 = P_1 \vee P_2 \vee P_3$.

(31) For all partitions P_1, P_2 of Y holds $P_1 \wedge P_1 \vee P_2 = P_1$.

(32) For all partitions P_1, P_2 of Y holds $P_1 \vee P_1 \wedge P_2 = P_1$.

(33) For all partitions P_1, P_2, P_3 of Y such that $P_1 \Subset P_3$ and $P_2 \Subset P_3$ holds $P_1 \vee P_2 \Subset P_3$.

(34) For all partitions P_1, P_2, P_3 of Y such that $P_1 \Supset P_3$ and $P_2 \Supset P_3$ holds $P_1 \wedge P_2 \Supset P_3$.

Let us consider Y. The functor $\mathcal{I}(Y)$ yielding a partition of Y is defined as follows:

(Def. 8) $\mathcal{I}(Y) = \mathrm{SmallestPartition}(Y)$.

Let us consider Y. The functor $\mathcal{O}(Y)$ yielding a partition of Y is defined by:

(Def. 9) $\mathcal{O}(Y) = \{Y\}$.

The following propositions are true:

(35) $\mathcal{I}(Y) = \{B : \bigvee_{x : \mathrm{set}} (B = \{x\} \ \wedge \ x \in Y)\}$.

(36) For every partition P_1 of Y holds $\mathcal{O}(Y) \Supset P_1$ and $P_1 \Supset \mathcal{I}(Y)$.

(37) $\equiv_{\mathcal{O}(Y)} = \nabla_Y$.

(38) $\equiv_{\mathcal{I}(Y)} = \triangle_Y$.

(39) $\mathcal{I}(Y) \Subset \mathcal{O}(Y)$.

(40) For every partition P_1 of Y holds $\mathcal{O}(Y) \vee P_1 = \mathcal{O}(Y)$ and $\mathcal{O}(Y) \wedge P_1 = P_1$.

(41) For every partition P_1 of Y holds $\mathcal{I}(Y) \vee P_1 = P_1$ and $\mathcal{I}(Y) \wedge P_1 = \mathcal{I}(Y)$.

References

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

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

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

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

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

[6] Alexander Yu. Shibakov and Andrzej Trybulec. The Cantor set. *Formalized Mathematics*, 5(**2**):233–236, 1996.

[7] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

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

[9] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

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

Received October 5, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

A Theory of Boolean Valued Functions and Partitions

Shunichi Kobayashi
Shinshu University
Nagano

Kui Jia
Shinshu University
Nagano

Summary. In this paper, we define Boolean valued functions. Some of their algebraic properties are proved. We also introduce and examine the infimum and supremum of Boolean valued functions and their properties. In the last section, relations between Boolean valued functions and partitions are discussed.

MML Identifier: BVFUNC_1.

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

1. Boolean Operations

In this paper Y denotes a non empty set.

Let k, l be elements of *Boolean*. The functor $k \Rightarrow l$ is defined by:

(Def. 1) $k \Rightarrow l = \neg k \vee l$.

The functor $k \Leftrightarrow l$ is defined as follows:

(Def. 2) $k \Leftrightarrow l = \neg(k \oplus l)$.

Let k, l be elements of *Boolean*. The predicate $k \Subset l$ is defined by:

(Def. 3) $k \Rightarrow l = \mathit{true}$.

Let us note that the predicate $k \Subset l$ is reflexive.

One can prove the following three propositions:

(1) For all elements k, l of *Boolean* and for all natural numbers n_1, n_2 such that $k = n_1$ and $l = n_2$ holds $k \Subset l$ iff $n_1 \leqslant n_2$.

ISSN 1426–2630

(2) For all elements k, l of *Boolean* such that $k \Subset l$ and $l \Subset k$ holds $k = l$.

(3) For all elements k, l, m of *Boolean* such that $k \Subset l$ and $l \Subset m$ holds $k \Subset m$.

2. Boolean Valued Functions

Let us consider Y. The functor $\mathrm{BVF}(Y)$ is defined by:

(Def. 4) $\mathrm{BVF}(Y) = \mathit{Boolean}^Y$.

Let Y be a non empty set. Observe that $\mathrm{BVF}(Y)$ is functional and non empty.

Let us consider Y, let a be an element of $\mathrm{BVF}(Y)$, and let x be an element of Y. The functor $\mathrm{Pj}(a, x)$ yields an element of *Boolean* and is defined by:

(Def. 5) $\mathrm{Pj}(a, x) = a(x)$.

Let us consider Y and let a, b be elements of $\mathrm{BVF}(Y)$. The functor $a \wedge b$ yields an element of $\mathrm{BVF}(Y)$ and is defined by:

(Def. 6) For every element x of Y holds $\mathrm{Pj}(a \wedge b, x) = \mathrm{Pj}(a, x) \wedge \mathrm{Pj}(b, x)$.

Let us notice that the functor $a \wedge b$ is commutative.

Let us consider Y and let a, b be elements of $\mathrm{BVF}(Y)$. The functor $a \vee b$ yields an element of $\mathrm{BVF}(Y)$ and is defined by:

(Def. 7) For every element x of Y holds $\mathrm{Pj}(a \vee b, x) = \mathrm{Pj}(a, x) \vee \mathrm{Pj}(b, x)$.

Let us notice that the functor $a \vee b$ is commutative.

Let us consider Y and let a be an element of $\mathrm{BVF}(Y)$. The functor $\neg a$ yielding an element of $\mathrm{BVF}(Y)$ is defined as follows:

(Def. 8) For every element x of Y holds $\mathrm{Pj}(\neg a, x) = \neg \mathrm{Pj}(a, x)$.

Let us consider Y and let a, b be elements of $\mathrm{BVF}(Y)$. The functor $a \oplus b$ yields an element of $\mathrm{BVF}(Y)$ and is defined as follows:

(Def. 9) For every element x of Y holds $\mathrm{Pj}(a \oplus b, x) = \mathrm{Pj}(a, x) \oplus \mathrm{Pj}(b, x)$.

Let us note that the functor $a \oplus b$ is commutative.

Let us consider Y and let a, b be elements of $\mathrm{BVF}(Y)$. The functor $a \Rightarrow b$ yields an element of $\mathrm{BVF}(Y)$ and is defined by:

(Def. 10) For every element x of Y holds $\mathrm{Pj}(a \Rightarrow b, x) = \neg \mathrm{Pj}(a, x) \vee \mathrm{Pj}(b, x)$.

Let us consider Y and let a, b be elements of $\mathrm{BVF}(Y)$. The functor $a \Leftrightarrow b$ yielding an element of $\mathrm{BVF}(Y)$ is defined as follows:

(Def. 11) For every element x of Y holds $\mathrm{Pj}(a \Leftrightarrow b, x) = \neg(\mathrm{Pj}(a, x) \oplus \mathrm{Pj}(b, x))$.

Let us observe that the functor $a \Leftrightarrow b$ is commutative.

Let us consider Y. The functor $\mathit{false}(Y)$ yielding an element of $\mathrm{BVF}(Y)$ is defined by:

(Def. 12) For every element x of Y holds $\mathrm{Pj}(\mathit{false}(Y), x) = \mathit{false}$.

Let us consider Y. The functor $true(Y)$ yielding an element of $\mathrm{BVF}(Y)$ is defined as follows:

(Def. 13) For every element x of Y holds $\mathrm{Pj}(true(Y), x) = true$.

The following propositions are true:

(4) For every element a of $\mathrm{BVF}(Y)$ holds $\neg\neg a = a$.

(5) For every element a of $\mathrm{BVF}(Y)$ holds $\neg\, true(Y) = false(Y)$ and $\neg\, false(Y) = true(Y)$.

(6) For all elements a, b of $\mathrm{BVF}(Y)$ holds $a \wedge a = a$.

(7) For all elements a, b, c of $\mathrm{BVF}(Y)$ holds $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.

(8) For every element a of $\mathrm{BVF}(Y)$ holds $a \wedge false(Y) = false(Y)$.

(9) For every element a of $\mathrm{BVF}(Y)$ holds $a \wedge true(Y) = a$.

(10) For every element a of $\mathrm{BVF}(Y)$ holds $a \vee a = a$.

(11) For all elements a, b, c of $\mathrm{BVF}(Y)$ holds $(a \vee b) \vee c = a \vee (b \vee c)$.

(12) For every element a of $\mathrm{BVF}(Y)$ holds $a \vee false(Y) = a$.

(13) For every element a of $\mathrm{BVF}(Y)$ holds $a \vee true(Y) = true(Y)$.

(14) For all elements a, b, c of $\mathrm{BVF}(Y)$ holds $a \wedge b \vee c = (a \vee c) \wedge (b \vee c)$.

(15) For all elements a, b, c of $\mathrm{BVF}(Y)$ holds $(a \vee b) \wedge c = a \wedge c \vee b \wedge c$.

(16) For all elements a, b of $\mathrm{BVF}(Y)$ holds $\neg(a \vee b) = \neg a \wedge \neg b$.

(17) For all elements a, b of $\mathrm{BVF}(Y)$ holds $\neg(a \wedge b) = \neg a \vee \neg b$.

Let us consider Y and let a, b be elements of $\mathrm{BVF}(Y)$. The predicate $a \Subset b$ is defined by:

(Def. 14) For every element x of Y such that $\mathrm{Pj}(a, x) = true$ holds $\mathrm{Pj}(b, x) = true$.

Let us note that the predicate $a \Subset b$ is reflexive.

The following four propositions are true:

(18) For all elements a, b, c of $\mathrm{BVF}(Y)$ holds if $a \Subset b$ and $b \Subset a$, then $a = b$ and if $a \Subset b$ and $b \Subset c$, then $a \Subset c$.

(19) For all elements a, b of $\mathrm{BVF}(Y)$ holds $a \Rightarrow b = true(Y)$ iff $a \Subset b$.

(20) For all elements a, b of $\mathrm{BVF}(Y)$ holds $a \Leftrightarrow b = true(Y)$ iff $a = b$.

(21) For every element a of $\mathrm{BVF}(Y)$ holds $false(Y) \Subset a$ and $a \Subset true(Y)$.

3. Infimum and Supremum

Let us consider Y and let a be an element of $\mathrm{BVF}(Y)$. The functor $\mathrm{INF}\, a$ yields an element of $\mathrm{BVF}(Y)$ and is defined as follows:

(Def. 15) $\mathrm{INF}\, a = \begin{cases} true(Y), & \text{if for every element } x \text{ of } Y \text{ holds } \mathrm{Pj}(a, x) = true, \\ false(Y), & \text{otherwise.} \end{cases}$

The functor $\mathrm{SUP}\, a$ yielding an element of $\mathrm{BVF}(Y)$ is defined by:

(Def. 16) $\mathrm{SUP}\, a = \begin{cases} \mathit{false}(Y), & \text{if for every element } x \text{ of } Y \text{ holds } \mathrm{Pj}(a, x) = \mathit{false}, \\ \mathit{true}(Y), & \text{otherwise.} \end{cases}$

Next we state two propositions:

(22) For every element a of $\mathrm{BVF}(Y)$ holds $\neg\, \mathrm{INF}\, a = \mathrm{SUP} \neg a$ and $\neg\, \mathrm{SUP}\, a = \mathrm{INF} \neg a$.

(23) $\mathrm{INF}\, \mathit{false}(Y) = \mathit{false}(Y)$ and $\mathrm{INF}\, \mathit{true}(Y) = \mathit{true}(Y)$ and $\mathrm{SUP}\, \mathit{false}(Y) = \mathit{false}(Y)$ and $\mathrm{SUP}\, \mathit{true}(Y) = \mathit{true}(Y)$.

Let us consider Y. Observe that $\mathit{false}(Y)$ is constant.

Let us consider Y. One can verify that $\mathit{true}(Y)$ is constant.

Let Y be a non empty set. Observe that there exists an element of $\mathrm{BVF}(Y)$ which is constant.

We now state several propositions:

(24) For every constant element a of $\mathrm{BVF}(Y)$ holds $a = \mathit{false}(Y)$ or $a = \mathit{true}(Y)$.

(25) For every constant element d of $\mathrm{BVF}(Y)$ holds $\mathrm{INF}\, d = d$ and $\mathrm{SUP}\, d = d$.

(26) For all elements a, b of $\mathrm{BVF}(Y)$ holds $\mathrm{INF}(a \wedge b) = \mathrm{INF}\, a \wedge \mathrm{INF}\, b$ and $\mathrm{SUP}(a \vee b) = \mathrm{SUP}\, a \vee \mathrm{SUP}\, b$.

(27) For every element a of $\mathrm{BVF}(Y)$ and for every constant element d of $\mathrm{BVF}(Y)$ holds $\mathrm{INF}(d \Rightarrow a) = d \Rightarrow \mathrm{INF}\, a$ and $\mathrm{INF}(a \Rightarrow d) = \mathrm{SUP}\, a \Rightarrow d$.

(28) For every element a of $\mathrm{BVF}(Y)$ and for every constant element d of $\mathrm{BVF}(Y)$ holds $\mathrm{INF}(d \vee a) = d \vee \mathrm{INF}\, a$ and $\mathrm{SUP}(d \wedge a) = d \wedge \mathrm{SUP}\, a$ and $\mathrm{SUP}(a \wedge d) = \mathrm{SUP}\, a \wedge d$.

(29) For every element a of $\mathrm{BVF}(Y)$ and for every element x of Y holds $\mathrm{Pj}(\mathrm{INF}\, a, x) \Subset \mathrm{Pj}(a, x)$.

(30) For every element a of $\mathrm{BVF}(Y)$ and for every element x of Y holds $\mathrm{Pj}(a, x) \Subset \mathrm{Pj}(\mathrm{SUP}\, a, x)$.

4. Boolean Valued Functions and Partitions

Let us consider Y, let a be an element of $\mathrm{BVF}(Y)$, and let P_1 be a partition of Y. We say that a is dependent of P_1 if and only if:

(Def. 17) For every set F such that $F \in P_1$ and for all sets x_1, x_2 such that $x_1 \in F$ and $x_2 \in F$ holds $a(x_1) = a(x_2)$.

The following two propositions are true:

(31) For every element a of $\mathrm{BVF}(Y)$ holds a is dependent of $\mathcal{I}(Y)$.

(32) For every constant element a of $\mathrm{BVF}(Y)$ holds a is dependent of $\mathcal{O}(Y)$.

Let us consider Y and let P_1 be a partition of Y. We see that the element of P_1 is a subset of Y.

Let us consider Y, let x be an element of Y, and let P_1 be a partition of Y. Then $\mathrm{EqClass}(x, P_1)$ is an element of P_1. We introduce $\mathrm{Lift}(x, P_1)$ as a synonym of $\mathrm{EqClass}(x, P_1)$.

Let us consider Y, let a be an element of $\mathrm{BVF}(Y)$, and let P_1 be a partition of Y. The functor $\mathrm{INF}(a, P_1)$ yields an element of $\mathrm{BVF}(Y)$ and is defined by the condition (Def. 18).

(Def. 18) Let y be an element of Y. Then

(i) if for every element x of Y such that $x \in \mathrm{EqClass}(y, P_1)$ holds $\mathrm{Pj}(a, x) = \mathit{true}$, then $\mathrm{Pj}(\mathrm{INF}(a, P_1), y) = \mathit{true}$, and

(ii) if it is not true that for every element x of Y such that $x \in \mathrm{EqClass}(y, P_1)$ holds $\mathrm{Pj}(a, x) = \mathit{true}$, then $\mathrm{Pj}(\mathrm{INF}(a, P_1), y) = \mathit{false}$.

Let us consider Y, let a be an element of $\mathrm{BVF}(Y)$, and let P_1 be a partition of Y. The functor $\mathrm{SUP}(a, P_1)$ yielding an element of $\mathrm{BVF}(Y)$ is defined by the condition (Def. 19).

(Def. 19) Let y be an element of Y. Then

(i) if there exists an element x of Y such that $x \in \mathrm{EqClass}(y, P_1)$ and $\mathrm{Pj}(a, x) = \mathit{true}$, then $\mathrm{Pj}(\mathrm{SUP}(a, P_1), y) = \mathit{true}$, and

(ii) if it is not true that there exists an element x of Y such that $x \in \mathrm{EqClass}(y, P_1)$ and $\mathrm{Pj}(a, x) = \mathit{true}$, then $\mathrm{Pj}(\mathrm{SUP}(a, P_1), y) = \mathit{false}$.

Next we state a number of propositions:

(33) For every element a of $\mathrm{BVF}(Y)$ and for every partition P_1 of Y holds $\mathrm{INF}(a, P_1)$ is dependent of P_1.

(34) For every element a of $\mathrm{BVF}(Y)$ and for every partition P_1 of Y holds $\mathrm{SUP}(a, P_1)$ is dependent of P_1.

(35) For every element a of $\mathrm{BVF}(Y)$ and for every partition P_1 of Y holds $\mathrm{INF}(a, P_1) \Subset a$.

(36) For every element a of $\mathrm{BVF}(Y)$ and for every partition P_1 of Y holds $a \Subset \mathrm{SUP}(a, P_1)$.

(37) For every element a of $\mathrm{BVF}(Y)$ and for every partition P_1 of Y holds $\neg\,\mathrm{INF}(a, P_1) = \mathrm{SUP}(\neg a, P_1)$.

(38) For every element a of $\mathrm{BVF}(Y)$ holds $\mathrm{INF}(a, \mathcal{O}(Y)) = \mathrm{INF}\, a$.

(39) For every element a of $\mathrm{BVF}(Y)$ holds $\mathrm{SUP}(a, \mathcal{O}(Y)) = \mathrm{SUP}\, a$.

(40) For every element a of $\mathrm{BVF}(Y)$ holds $\mathrm{INF}(a, \mathcal{I}(Y)) = a$.

(41) For every element a of $\mathrm{BVF}(Y)$ holds $\mathrm{SUP}(a, \mathcal{I}(Y)) = a$.

(42) For all elements a, b of $\mathrm{BVF}(Y)$ and for every partition P_1 of Y holds $\mathrm{INF}(a \wedge b, P_1) = \mathrm{INF}(a, P_1) \wedge \mathrm{INF}(b, P_1)$.

(43) For all elements a, b of $\mathrm{BVF}(Y)$ and for every partition P_1 of Y holds $\mathrm{SUP}(a \vee b, P_1) = \mathrm{SUP}(a, P_1) \vee \mathrm{SUP}(b, P_1)$.

Let us consider Y and let f be an element of $\mathrm{BVF}(Y)$. The functor $\mathrm{GPart}\, f$ yields a partition of Y and is defined by:

(Def. 20) $\mathrm{GPart}\, f = \{\{x; x$ ranges over elements of $Y\colon f(x) = \mathit{true}\}, \{x'; x'$ ranges over elements of $Y\colon f(x') = \mathit{false}\}\} \setminus \{\emptyset\}$.

The following propositions are true:

(44) For every element a of $\mathrm{BVF}(Y)$ holds a is dependent of $\mathrm{GPart}\, a$.

(45) For every element a of $\mathrm{BVF}(Y)$ and for every partition P_1 of Y such that a is dependent of P_1 holds P_1 is finer than $\mathrm{GPart}\, a$.

References

[1] Shunichi Kobayashi and Kui Jia. A theory of partitions. Part I. *Formalized Mathematics*, 7(**2**):243–247, 1998.
[2] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.
[3] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[4] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.
[5] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[6] Edmund Woronowicz. Many–argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

Received October 22, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Trigonometric Functions and Existence of Circle Ratio

Yuguang Yang
Shinshu University
Nagano

Yasunari Shidama
Shinshu University
Nagano

Summary. In this article, we defined *sinus* and *cosine* as the real part and the imaginary part of the exponential function on complex, and also give their series expression. Then we proved the differentiablity of *sinus*, *cosine* and the exponential function of real. Finally, we showed the existence of the circle ratio, and some formulas of *sinus*, *cosine*.

MML Identifier: `SIN_COS`.

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

1. Some Definitions and Properties of Complex Sequence

For simplicity, we adopt the following rules: p, q, r, t_1, t_2, t_3 are elements of $\mathbb{R}$, w, z, z_1, z_2 are elements of $\mathbb{C}$, k, l, m, n are natural numbers, s_1 is a complex sequence, and r_1 is a sequence of real numbers.

Let m, k be natural numbers. Let us assume that $k \leqslant m$. The functor $\mathrm{PN}(m,k)$ yielding an element of $\mathbb{N}$ is defined by:

(Def. 1) $\mathrm{PN}(m,k) = m - k$.

Let m, k be natural numbers. The functor $\mathrm{CHK}(m,k)$ yields an element of $\mathbb{C}$ and is defined by:

(Def. 2) $\mathrm{CHK}(m,k) = \begin{cases} 1_{\mathbb{C}}, & \text{if } m \leqslant k, \\ 0_{\mathbb{C}}, & \text{otherwise.} \end{cases}$

ISSN 1426–2630

The functor $\mathrm{RHK}(m,k)$ yields an element of $\mathbb{R}$ and is defined as follows:

(Def. 3) $\mathrm{RHK}(m,k) = \begin{cases} 1, & \text{if } m \leqslant k, \\ 0, & \text{otherwise.} \end{cases}$

In this article we present several logical schemes. The scheme *ExComplex CASE* deals with a binary functor $\mathcal{F}$ yielding an element of $\mathbb{C}$, and states that:

For every k there exists s_1 such that for every n holds if $n \leqslant k$, then $s_1(n) = \mathcal{F}(k,n)$ and if $n > k$, then $s_1(n) = 0_{\mathbb{C}}$

for all values of the parameter.

The scheme *ExReal CASE* deals with a binary functor $\mathcal{F}$ yielding an element of $\mathbb{R}$, and states that:

For every k there exists r_1 such that for every n holds if $n \leqslant k$, then $r_1(n) = \mathcal{F}(k,n)$ and if $n > k$, then $r_1(n) = 0$

for all values of the parameter.

The complex sequence Prod_complex_n is defined by:

(Def. 4) $(\mathrm{Prod\_complex\_n})(0) = 1_{\mathbb{C}}$ and for every n holds $(\mathrm{Prod\_complex\_n})(n+1) = (\mathrm{Prod\_complex\_n})(n) \cdot ((n+1)+0i)$.

The sequence Prod_real_n of real numbers is defined by:

(Def. 5) $(\mathrm{Prod\_real\_n})(0) = 1$ and for every n holds $(\mathrm{Prod\_real\_n})(n+1) = (\mathrm{Prod\_real\_n})(n) \cdot (n+1)$.

Let n be a natural number. The functor $n!c$ yields an element of $\mathbb{C}$ and is defined as follows:

(Def. 6) $n!c = (\mathrm{Prod\_complex\_n})(n)$.

Let n be a natural number. Then $n!$ is a real number and it can be characterized by the condition:

(Def. 7) $n! = (\mathrm{Prod\_real\_n})(n)$.

Let z be an element of $\mathbb{C}$. The functor $z\,\mathrm{ExpSeq}$ yields a complex sequence and is defined as follows:

(Def. 8) For every n holds $z\,\mathrm{ExpSeq}(n) = \frac{z_{\mathbb{N}}^n}{n!c}$.

Let a be an element of $\mathbb{R}$. The functor $a\,\mathrm{ExpSeq}$ yielding a sequence of real numbers is defined as follows:

(Def. 9) For every n holds $a\,\mathrm{ExpSeq}(n) = \frac{a_{\mathbb{N}}^n}{n!}$.

The following propositions are true:

(1) If $0 < n$, then $n+0i \neq 0_{\mathbb{C}}$ and $0!c = 1_{\mathbb{C}}$ and $n!c \neq 0_{\mathbb{C}}$ and $n+1!c = n!c \cdot ((n+1)+0i)$.

(2) $n! \neq 0$ and $(n+1)! = n! \cdot (n+1)$.

(3) For every k such that $0 < k$ holds $\mathrm{PN}(k,1)!c \cdot (k+0i) = k!c$ and for all m, k such that $k \leqslant m$ holds $\mathrm{PN}(m,k)!c \cdot (((m+1)-k)+0i) = \mathrm{PN}(m+1,k)!c$.

Let n be a natural number. The functor $\mathrm{Coef}\,n$ yielding a complex sequence is defined by:

(Def. 10) For every natural number k holds if $k \leqslant n$, then $(\mathrm{Coef}\, n)(k) = \frac{n!_{\mathbb{C}}}{k!_{\mathbb{C}} \cdot \mathrm{PN}(n,k)!_{\mathbb{C}}}$ and if $k > n$, then $(\mathrm{Coef}\, n)(k) = 0_{\mathbb{C}}$.

Let n be a natural number. The functor Coef_e n yields a complex sequence and is defined as follows:

(Def. 11) For every natural number k holds if $k \leqslant n$, then $(\mathrm{Coef\_e}\, n)(k) = \frac{1_{\mathbb{C}}}{k!_{\mathbb{C}} \cdot \mathrm{PN}(n,k)!_{\mathbb{C}}}$ and if $k > n$, then $(\mathrm{Coef\_e}\, n)(k) = 0_{\mathbb{C}}$.

Let us consider s_1. The functor Sift s_1 yielding a complex sequence is defined as follows:

(Def. 12) $(\mathrm{Sift}\, s_1)(0) = 0_{\mathbb{C}}$ and for every natural number k holds $(\mathrm{Sift}\, s_1)(k+1) = s_1(k)$.

Let us consider n and let z, w be elements of $\mathbb{C}$. The functor $\mathrm{Expan}(n, z, w)$ yields a complex sequence and is defined as follows:

(Def. 13) For every natural number k holds if $k \leqslant n$, then $(\mathrm{Expan}(n, z, w))(k) = (\mathrm{Coef}\, n)(k) \cdot z_{\mathbb{N}}^{k} \cdot w_{\mathbb{N}}^{\mathrm{PN}(n,k)}$ and if $n < k$, then $(\mathrm{Expan}(n, z, w))(k) = 0_{\mathbb{C}}$.

Let us consider n and let z, w be elements of $\mathbb{C}$. The functor $\mathrm{Expan\_e}(n, z, w)$ yielding a complex sequence is defined by:

(Def. 14) For every natural number k holds if $k \leqslant n$, then $(\mathrm{Expan\_e}(n, z, w))(k) = (\mathrm{Coef\_e}\, n)(k) \cdot z_{\mathbb{N}}^{k} \cdot w_{\mathbb{N}}^{\mathrm{PN}(n,k)}$ and if $n < k$, then $(\mathrm{Expan\_e}(n, z, w))(k) = 0_{\mathbb{C}}$.

Let us consider n and let z, w be elements of $\mathbb{C}$. The functor $\mathrm{Alfa}(n, z, w)$ yielding a complex sequence is defined by:

(Def. 15) For every natural number k holds if $k \leqslant n$, then $(\mathrm{Alfa}(n, z, w))(k) = z\,\mathrm{ExpSeq}(k) \cdot (\sum_{\alpha=0}^{\kappa} w\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(\mathrm{PN}(n, k))$ and if $n < k$, then $(\mathrm{Alfa}(n, z, w))(k) = 0_{\mathbb{C}}$.

Let a, b be elements of $\mathbb{R}$ and let n be a natural number. The functor $\mathrm{Conj}(n, a, b)$ yielding a sequence of real numbers is defined as follows:

(Def. 16) For every natural number k holds if $k \leqslant n$, then $(\mathrm{Conj}(n, a, b))(k) = a\,\mathrm{ExpSeq}(k) \cdot ((\sum_{\alpha=0}^{\kappa} b\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(n) - (\sum_{\alpha=0}^{\kappa} b\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(\mathrm{PN}(n, k)))$ and if $n < k$, then $(\mathrm{Conj}(n, a, b))(k) = 0$.

Let z, w be elements of $\mathbb{C}$ and let n be a natural number. The functor $\mathrm{Conj}(n, z, w)$ yielding a complex sequence is defined by:

(Def. 17) For every natural number k holds if $k \leqslant n$, then $(\mathrm{Conj}(n, z, w))(k) = z\,\mathrm{ExpSeq}(k) \cdot ((\sum_{\alpha=0}^{\kappa} w\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(n) - (\sum_{\alpha=0}^{\kappa} w\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(\mathrm{PN}(n, k)))$ and if $n < k$, then $(\mathrm{Conj}(n, z, w))(k) = 0_{\mathbb{C}}$.

The following propositions are true:

(4) $z\,\mathrm{ExpSeq}(n + 1) = \frac{z\,\mathrm{ExpSeq}(n) \cdot z}{(n+1)+0i}$ and $z\,\mathrm{ExpSeq}(0) = 1_{\mathbb{C}}$ and $|z\,\mathrm{ExpSeq}(n)| = |z|\,\mathrm{ExpSeq}(n)$.

(5) If $0 < k$, then $(\mathrm{Sift}\, s_1)(k) = s_1(\mathrm{PN}(k, 1))$.

(6) $(\sum_{\alpha=0}^{\kappa} (s_1)(\alpha))_{\kappa \in \mathbb{N}}(k) = (\sum_{\alpha=0}^{\kappa} (\mathrm{Sift}\, s_1)(\alpha))_{\kappa \in \mathbb{N}}(k) + s_1(k)$.

(7) $(z + w)_{\mathbb{N}}^{n} = (\sum_{\alpha=0}^{\kappa} (\mathrm{Expan}(n, z, w))(\alpha))_{\kappa \in \mathbb{N}}(n)$.

(8) $\mathrm{Expan\_e}(n, z, w) = \frac{1_{\mathbb{C}}}{n!c} \mathrm{Expan}(n, z, w)$.

(9) $\frac{(z+w)^n_{\mathbb{N}}}{n!c} = (\sum_{\alpha=0}^{\kappa} (\mathrm{Expan\_e}(n, z, w))(\alpha))_{\kappa \in \mathbb{N}}(n)$.

(10) $0_{\mathbb{C}}\,\mathrm{ExpSeq}$ is absolutely summable and $\sum(0_{\mathbb{C}}\,\mathrm{ExpSeq}) = 1_{\mathbb{C}}$.

Let us consider z. One can verify that $z\,\mathrm{ExpSeq}$ is absolutely summable.

Next we state a number of propositions:

(11) $z\,\mathrm{ExpSeq}(0) = 1_{\mathbb{C}}$ and $(\mathrm{Expan}(0, z, w))(0) = 1_{\mathbb{C}}$.

(12) If $l \leqslant k$, then $(\mathrm{Alfa}(k+1, z, w))(l) = (\mathrm{Alfa}(k, z, w))(l) + (\mathrm{Expan\_e}(k+1, z, w))(l)$.

(13) $(\sum_{\alpha=0}^{\kappa} (\mathrm{Alfa}(k+1, z, w))(\alpha))_{\kappa \in \mathbb{N}}(k) = (\sum_{\alpha=0}^{\kappa} (\mathrm{Alfa}(k, z, w))(\alpha))_{\kappa \in \mathbb{N}}(k) + (\sum_{\alpha=0}^{\kappa} (\mathrm{Expan\_e}(k+1, z, w))(\alpha))_{\kappa \in \mathbb{N}}(k)$.

(14) $z\,\mathrm{ExpSeq}(k) = (\mathrm{Expan\_e}(k, z, w))(k)$.

(15) $(\sum_{\alpha=0}^{\kappa} z + w\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(n) = (\sum_{\alpha=0}^{\kappa} (\mathrm{Alfa}(n, z, w))(\alpha))_{\kappa \in \mathbb{N}}(n)$.

(16) $(\sum_{\alpha=0}^{\kappa} z\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(k) \cdot (\sum_{\alpha=0}^{\kappa} w\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(k) - (\sum_{\alpha=0}^{\kappa} z + w\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(k) = (\sum_{\alpha=0}^{\kappa} (\mathrm{Conj}(k, z, w))(\alpha))_{\kappa \in \mathbb{N}}(k)$.

(17) $|(\sum_{\alpha=0}^{\kappa} z\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(k)| \leqslant (\sum_{\alpha=0}^{\kappa} |z|\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(k)$ and $(\sum_{\alpha=0}^{\kappa} |z|\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(k) \leqslant \sum(|z|\,\mathrm{ExpSeq})$ and $|(\sum_{\alpha=0}^{\kappa} z\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(k)| \leqslant \sum(|z|\,\mathrm{ExpSeq})$.

(18) $1 \leqslant \sum(|z|\,\mathrm{ExpSeq})$.

(19) $0 \leqslant |z|\,\mathrm{ExpSeq}(n)$.

(20) $|(\sum_{\alpha=0}^{\kappa} |z|\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(n)| = (\sum_{\alpha=0}^{\kappa} |z|\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(n)$ and if $n \leqslant m$, then $|(\sum_{\alpha=0}^{\kappa} |z|\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(m) - (\sum_{\alpha=0}^{\kappa} |z|\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(n)| = (\sum_{\alpha=0}^{\kappa} |z|\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(m) - (\sum_{\alpha=0}^{\kappa} |z|\,\mathrm{ExpSeq}(\alpha))_{\kappa \in \mathbb{N}}(n)$.

(21) $|(\sum_{\alpha=0}^{\kappa} |\mathrm{Conj}(k, z, w)|(\alpha))_{\kappa \in \mathbb{N}}(n)| = (\sum_{\alpha=0}^{\kappa} |\mathrm{Conj}(k, z, w)|(\alpha))_{\kappa \in \mathbb{N}}(n)$.

(22) For every p such that $p > 0$ there exists n such that for every k such that $n \leqslant k$ holds $|(\sum_{\alpha=0}^{\kappa} |\mathrm{Conj}(k, z, w)|(\alpha))_{\kappa \in \mathbb{N}}(k)| < p$.

(23) For every s_1 such that for every k holds $s_1(k) = (\sum_{\alpha=0}^{\kappa} (\mathrm{Conj}(k, z, w))(\alpha))_{\kappa \in \mathbb{N}}(k)$ holds s_1 is convergent and $\lim s_1 = 0_{\mathbb{C}}$.

2. Definition of Exponential Function on Complex

The partial function exp from $\mathbb{C}$ to $\mathbb{C}$ is defined as follows:

(Def. 18) $\mathrm{dom}\exp = \mathbb{C}$ and for every element z of $\mathbb{C}$ holds $(\exp)(z) = \sum(z\,\mathrm{ExpSeq})$.

Let us consider z. The functor $\exp z$ yielding an element of $\mathbb{C}$ is defined by:

(Def. 19) $\exp z = (\exp)(z)$.

The following proposition is true

(24) For all z_1, z_2 holds $\exp z_1 + z_2 = \exp z_1 \cdot \exp z_2$.

3. Definition of Sinus, Cosine, and Exponential Function on $\mathbb{R}$

The partial function sin from $\mathbb{R}$ to $\mathbb{R}$ is defined as follows:

(Def. 20) dom sin $= \mathbb{R}$ and for every real number d holds $(\sin)(d) = \Im(\sum(0 + d i \operatorname{ExpSeq}))$.

Let us consider t_1. The functor $\sin t_1$ yielding an element of $\mathbb{R}$ is defined by:

(Def. 21) $\sin t_1 = (\sin)(t_1)$.

Next we state the proposition

(25) sin is a function from $\mathbb{R}$ into $\mathbb{R}$.

The partial function cos from $\mathbb{R}$ to $\mathbb{R}$ is defined by:

(Def. 22) dom cos $= \mathbb{R}$ and for every real number d holds $(\cos)(d) = \Re(\sum(0 + d i \operatorname{ExpSeq}))$.

Let us consider t_1. The functor $\cos t_1$ yields an element of $\mathbb{R}$ and is defined by:

(Def. 23) $\cos t_1 = (\cos)(t_1)$.

One can prove the following propositions:

(26) cos is a function from $\mathbb{R}$ into $\mathbb{R}$.

(27) dom sin $= \mathbb{R}$ and dom cos $= \mathbb{R}$.

(28) $\exp 0 + t_1 i = \cos t_1 + \sin t_1 i$.

(29) $(\exp 0 + t_1 i)^* = \exp -(0 + t_1 i)$.

(30) $|\exp 0 + t_1 i| = 1$ and $|\sin t_1| \leqslant 1$ and $|\cos t_1| \leqslant 1$.

(31) $(\cos)(t_1)^{\mathbf{2}} + (\sin)(t_1)^{\mathbf{2}} = 1$ and $(\cos)(t_1) \cdot (\cos)(t_1) + (\sin)(t_1) \cdot (\sin)(t_1) = 1$.

(32) $(\cos t_1)^{\mathbf{2}} + (\sin t_1)^{\mathbf{2}} = 1$ and $\cos t_1 \cdot \cos t_1 + \sin t_1 \cdot \sin t_1 = 1$.

(33) $(\cos)(0) = 1$ and $(\sin)(0) = 0$ and $(\cos)(-t_1) = (\cos)(t_1)$ and $(\sin)(-t_1) = -(\sin)(t_1)$.

(34) $\cos 0 = 1$ and $\sin 0 = 0$ and $\cos -t_1 = \cos t_1$ and $\sin -t_1 = -\sin t_1$.

Let t_1 be an element of $\mathbb{R}$. The functor t_1 P_sin yielding a sequence of real numbers is defined by:

(Def. 24) For every n holds $t_1 \operatorname{P\_sin}(n) = \frac{((-1)^n_{\mathbb{N}}) \cdot {t_1}^{2 \cdot n+1}_{\mathbb{N}}}{(2 \cdot n+1)!}$.

Let t_1 be an element of $\mathbb{R}$. The functor t_1 P_cos yielding a sequence of real numbers is defined by:

(Def. 25) For every n holds $t_1 \operatorname{P\_cos}(n) = \frac{((-1)^n_{\mathbb{N}}) \cdot {t_1}^{2 \cdot n}_{\mathbb{N}}}{(2 \cdot n)!}$.

The following propositions are true:

(35) For all z, k holds $z^{2 \cdot k}_{\mathbb{N}} = (z^k_{\mathbb{N}})^2_{\mathbb{N}}$ and $z^{2 \cdot k}_{\mathbb{N}} = (z^2_{\mathbb{N}})^k_{\mathbb{N}}$.

(36) For all k, t_1 holds $(0 + t_1 i)^{2 \cdot k}_{\mathbb{N}} = ((-1)^k_{\mathbb{N}}) \cdot {t_1}^{2 \cdot k}_{\mathbb{N}} + 0i$ and $(0 + t_1 i)^{2 \cdot k+1}_{\mathbb{N}} = 0 + (((-1)^k_{\mathbb{N}}) \cdot {t_1}^{2 \cdot k+1}_{\mathbb{N}})i$.

(37) For every n holds $n!c = n! + 0i$.

(38) For all t_1, n holds $(\sum_{\alpha=0}^{\kappa} t_1 \mathrm{P\_sin}(\alpha))_{\kappa\in\mathbb{N}}(n) = (\sum_{\alpha=0}^{\kappa} \Im(0 + t_1 i \,\mathrm{ExpSeq})(\alpha))_{\kappa\in\mathbb{N}}(2\cdot n+1)$ and $(\sum_{\alpha=0}^{\kappa} t_1 \mathrm{P\_cos}(\alpha))_{\kappa\in\mathbb{N}}(n) = (\sum_{\alpha=0}^{\kappa} \Re(0+ t_1 i \,\mathrm{ExpSeq})(\alpha))_{\kappa\in\mathbb{N}}(2\cdot n)$.

(39) For every t_1 holds $(\sum_{\alpha=0}^{\kappa} t_1 \mathrm{P\_sin}(\alpha))_{\kappa\in\mathbb{N}}$ is convergent and $\sum(t_1 \mathrm{P\_sin}) = \Im(\sum(0 + t_1 i \,\mathrm{ExpSeq}))$ and $(\sum_{\alpha=0}^{\kappa} t_1 \mathrm{P\_cos}(\alpha))_{\kappa\in\mathbb{N}}$ is convergent and $\sum(t_1 \mathrm{P\_cos}) = \Re(\sum(0 + t_1 i \,\mathrm{ExpSeq}))$.

(40) For every t_1 holds $(\cos)(t_1) = \sum(t_1 \mathrm{P\_cos})$ and $(\sin)(t_1) = \sum(t_1 \mathrm{P\_sin})$.

(41) For all p, t_1, r_1 such that r_1 is convergent and $\lim r_1 = t_1$ and for every n holds $r_1(n) \geqslant p$ holds $t_1 \geqslant p$.

(42) For all n, k, m such that $n < k$ holds $m! > 0$ and $n! \leqslant k!$.

(43) For all t_1, n, k such that $0 \leqslant t_1$ and $t_1 \leqslant 1$ and $n \leqslant k$ holds ${t_1}^k_{\mathbb{N}} \leqslant {t_1}^n_{\mathbb{N}}$.

(44) For all t_1, n holds $(t_1 + 0i)^n_{\mathbb{N}} = ({t_1}^n_{\mathbb{N}}) + 0i$.

(45) For all t_1, n holds $\frac{(t_1+0i)^n_{\mathbb{N}}}{n!c} = \frac{{t_1}^n_{\mathbb{N}}}{n!} + 0i$.

(46) $\Im(\sum(p + 0i \,\mathrm{ExpSeq})) = 0$.

(47) $(\cos)(1) > 0$ and $(\sin)(1) > 0$ and $(\cos)(1) < (\sin)(1)$.

(48) For every t_1 holds $t_1 \,\mathrm{ExpSeq} = \Re(t_1 + 0i \,\mathrm{ExpSeq})$.

(49) For every t_1 holds $t_1 \,\mathrm{ExpSeq}$ is summable and $\sum(t_1 \,\mathrm{ExpSeq}) = \Re(\sum(t_1+ 0i \,\mathrm{ExpSeq}))$.

(50) For all p, q holds $\sum(p + q \,\mathrm{ExpSeq}) = \sum(p \,\mathrm{ExpSeq}) \cdot \sum(q \,\mathrm{ExpSeq})$.

The partial function exp from $\mathbb{R}$ to $\mathbb{R}$ is defined by:

(Def. 26) $\mathrm{dom}\exp = \mathbb{R}$ and for every real number d holds $(\exp)(d) = \sum(d \,\mathrm{ExpSeq})$.

Let us consider t_1. The functor $\exp t_1$ yields an element of $\mathbb{R}$ and is defined as follows:

(Def. 27) $\exp t_1 = (\exp)(t_1)$.

We now state a number of propositions:

(51) $\mathrm{dom}\exp = \mathbb{R}$.

(52) For every element d of $\mathbb{R}$ holds $(\exp)(d) = \sum(d \,\mathrm{ExpSeq})$.

(53) For every t_1 holds $(\exp)(t_1) = \Re(\sum(t_1 + 0i \,\mathrm{ExpSeq}))$.

(54) $\exp t_1 + 0i = \exp t_1 + 0i$.

(55) $\exp p + q = \exp p \cdot \exp q$.

(56) $\exp 0 = 1$.

(57) For every t_1 such that $t_1 > 0$ holds $(\exp)(t_1) \geqslant 1$.

(58) For every t_1 such that $t_1 < 0$ holds $0 < (\exp)(t_1)$ and $(\exp)(t_1) \leqslant 1$.

(59) For every t_1 holds $(\exp)(t_1) > 0$.

(60) For every t_1 holds $\exp t_1 > 0$.

4. Differential of Sinus, Cosine, and Exponential Function

Let z be an element of $\mathbb{C}$. The functor $z\,\mathrm{P\_dt}$ yields a complex sequence and is defined as follows:

(Def. 28) For every n holds $z\,\mathrm{P\_dt}(n) = \frac{z_{\mathbb{N}}^{n+1}}{n+2!c}$.

Let z be an element of $\mathbb{C}$. The functor $z\,\mathrm{P\_t}$ yielding a complex sequence is defined by:

(Def. 29) For every n holds $z\,\mathrm{P\_t}(n) = \frac{z_{\mathbb{N}}^{n}}{n+2!c}$.

Next we state a number of propositions:

(61) For every z holds $z\,\mathrm{P\_dt}$ is absolutely summable.

(62) For every z holds $z \cdot \sum(z\,\mathrm{P\_dt}) = \sum(z\,\mathrm{ExpSeq}) - 1_{\mathbb{C}} - z$.

(63) For every p such that $p > 0$ there exists r such that $r > 0$ and for every z such that $|z| < r$ holds $|\sum(z\,\mathrm{P\_dt})| < p$.

(64) For all z, z_1 holds $\sum(z_1 + z\,\mathrm{ExpSeq}) - \sum(z_1\,\mathrm{ExpSeq}) = \sum(z_1\,\mathrm{ExpSeq}) \cdot z + z \cdot \sum(z\,\mathrm{P\_dt}) \cdot \sum(z_1\,\mathrm{ExpSeq})$.

(65) For all p, q holds $(\cos)(p+q) - (\cos)(p) = -q \cdot (\sin)(p) - q \cdot \Im(\sum(0 + qi\,\mathrm{P\_dt}) \cdot ((\cos)(p) + (\sin)(p)i))$.

(66) For all p, q holds $(\sin)(p+q) - (\sin)(p) = q \cdot (\cos)(p) + q \cdot \Re(\sum(0 + qi\,\mathrm{P\_dt}) \cdot ((\cos)(p) + (\sin)(p)i))$.

(67) For all p, q holds $(\exp)(p+q) - (\exp)(p) = q \cdot (\exp)(p) + q \cdot (\exp)(p) \cdot \Re(\sum(q + 0i\,\mathrm{P\_dt}))$.

(68) For every p holds cos is differentiable in p and $(\cos)'(p) = -(\sin)(p)$.

(69) For every p holds sin is differentiable in p and $(\sin)'(p) = (\cos)(p)$.

(70) For every p holds exp is differentiable in p and $(\exp)'(p) = (\exp)(p)$.

(71) exp is differentiable on $\mathbb{R}$ and for every t_1 such that $t_1 \in \mathbb{R}$ holds $(\exp)'(t_1) = (\exp)(t_1)$.

(72) cos is differentiable on $\mathbb{R}$ and for every t_1 such that $t_1 \in \mathbb{R}$ holds $(\cos)'(t_1) = -(\sin)(t_1)$.

(73) sin is differentiable on $\mathbb{R}$ and for every t_1 holds $(\sin)'(t_1) = (\cos)(t_1)$.

(74) For every t_1 such that $t_1 \in [0,1]$ holds $0 < (\cos)(t_1)$ and $(\cos)(t_1) \geqslant \frac{1}{2}$.

(75) $[0,1] \subseteq \mathrm{dom}(\frac{\sin}{\cos})$ and $]0,1[\subseteq \mathrm{dom}(\frac{\sin}{\cos})$.

(76) $\frac{\sin}{\cos}$ is continuous on $[0,1]$.

(77) For all t_2, t_3 such that $t_2 \in]0,1[$ and $t_3 \in]0,1[$ and $(\frac{\sin}{\cos})(t_2) = (\frac{\sin}{\cos})(t_3)$ holds $t_2 = t_3$.

5. Existence of Circle Ratio

The element Pai of $\mathbb{R}$ is defined as follows:

(Def. 30) $(\frac{\sin}{\cos})(\frac{\text{Pai}}{4}) = 1$ and Pai $\in]0, 4[$.

We now state the proposition

(78) $(\sin)(\frac{\text{Pai}}{4}) = (\cos)(\frac{\text{Pai}}{4})$.

6. Formulas of Sinus, Cosine

Next we state several propositions:

(79) $(\sin)(t_2+t_3) = (\sin)(t_2)\cdot(\cos)(t_3)+(\cos)(t_2)\cdot(\sin)(t_3)$ and $(\cos)(t_2+t_3) = (\cos)(t_2)\cdot(\cos)(t_3) - (\sin)(t_2)\cdot(\sin)(t_3)$.

(80) $\sin t_2 + t_3 = \sin t_2 \cdot \cos t_3 + \cos t_2 \cdot \sin t_3$ and $\cos t_2 + t_3 = \cos t_2 \cdot \cos t_3 - \sin t_2 \cdot \sin t_3$.

(81) $(\cos)(\frac{\text{Pai}}{2}) = 0$ and $(\sin)(\frac{\text{Pai}}{2}) = 1$ and $(\cos)(\text{Pai}) = -1$ and $(\sin)(\text{Pai}) = 0$ and $(\cos)(\text{Pai}+\frac{\text{Pai}}{2}) = 0$ and $(\sin)(\text{Pai}+\frac{\text{Pai}}{2}) = -1$ and $(\cos)(2\cdot\text{Pai}) = 1$ and $(\sin)(2\cdot\text{Pai}) = 0$.

(82) $\cos\frac{\text{Pai}}{2} = 0$ and $\sin\frac{\text{Pai}}{2} = 1$ and $\cos\text{Pai} = -1$ and $\sin\text{Pai} = 0$ and $\cos\text{Pai}+\frac{\text{Pai}}{2} = 0$ and $\sin\text{Pai}+\frac{\text{Pai}}{2} = -1$ and $\cos 2\cdot\text{Pai} = 1$ and $\sin 2\cdot\text{Pai} = 0$.

(83)(i) $(\sin)(t_1 + 2\cdot\text{Pai}) = (\sin)(t_1)$,

(ii) $(\cos)(t_1 + 2\cdot\text{Pai}) = (\cos)(t_1)$,

(iii) $(\sin)(\frac{\text{Pai}}{2} - t_1) = (\cos)(t_1)$,

(iv) $(\cos)(\frac{\text{Pai}}{2} - t_1) = (\sin)(t_1)$,

(v) $(\sin)(\frac{\text{Pai}}{2} + t_1) = (\cos)(t_1)$,

(vi) $(\cos)(\frac{\text{Pai}}{2} + t_1) = -(\sin)(t_1)$,

(vii) $(\sin)(\text{Pai}+t_1) = -(\sin)(t_1)$, and

(viii) $(\cos)(\text{Pai}+t_1) = -(\cos)(t_1)$.

(84) $\sin t_1 + 2\cdot\text{Pai} = \sin t_1$ and $\cos t_1 + 2\cdot\text{Pai} = \cos t_1$ and $\sin\frac{\text{Pai}}{2} - t_1 = \cos t_1$ and $\cos\frac{\text{Pai}}{2} - t_1 = \sin t_1$ and $\sin\frac{\text{Pai}}{2} + t_1 = \cos t_1$ and $\cos\frac{\text{Pai}}{2} + t_1 = -\sin t_1$ and $\sin\text{Pai}+t_1 = -\sin t_1$ and $\cos\text{Pai}+t_1 = -\cos t_1$.

(85) For every t_1 such that $t_1 \in]0, \frac{\text{Pai}}{2}[$ holds $(\cos)(t_1) > 0$.

(86) For every t_1 such that $t_1 \in]0, \frac{\text{Pai}}{2}[$ holds $\cos t_1 > 0$.

References

[1] Agnieszka Banachowicz and Anna Winnicka. Complex sequences. *Formalized Mathematics*, 4(**1**):121–124, 1993.

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

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

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

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

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

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

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

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

[10] Adam Naumowicz. Conjugate sequences, bounded complex sequences and convergent complex sequences. *Formalized Mathematics*, 6(**2**):265–268, 1997.

[11] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

[12] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

[13] Konrad Raczkowski and Andrzej Nędzusiak. Serieses. *Formalized Mathematics*, 2(**4**):449–452, 1991.

[14] Konrad Raczkowski and Paweł Sadowski. Real function continuity. *Formalized Mathematics*, 1(**4**):787–791, 1990.

[15] Konrad Raczkowski and Paweł Sadowski. Real function differentiability. *Formalized Mathematics*, 1(**4**):797–801, 1990.

[16] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.

[17] Yasunari Shidama and Artur Korniłowicz. Convergence and the limit of complex sequences. Serieses. *Formalized Mathematics*, 6(**3**):403–410, 1997.

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

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

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

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

Received October 22, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Some Properties of Special Polygonal Curves

Andrzej Trybulec
University of Białystok

Yatsuka Nakamura
Shinshu University
Nagano

Summary. In the paper some auxiliary theorems are proved, needed in the proof of the second part of the Jordan curve theorem for special polygons. They deal mostly with characteristic points of plane non empty compacts introduced in [5], operation *mid* introduced in [19] and the predicate "f is in the area of g" (f and g : finite sequences of points of the plane) introduced in [28].

MML Identifier: `SPRECT_3`.

The notation and terminology used here are introduced in the following papers: [21], [32], [6], [22], [24], [7], [2], [3], [30], [4], [27], [15], [16], [20], [26], [19], [9], [18], [11], [12], [13], [1], [23], [5], [10], [14], [17], [29], [28], [31], [25], [8], and [33].

1. Preliminaries

In this paper i, j, k, n are natural numbers.

The following propositions are true:

(1) For all sets A, B, C such that A misses B holds $A \cap (B \cup C) = A \cap C$.

(2) For all sets A, B, C, p such that $A \subseteq B$ and $B \cap C = \{p\}$ and $p \in A$ holds $A \cap C = \{p\}$.

(3) For all real numbers q, r, s, t such that $t \geqslant 0$ and $t \leqslant 1$ and $s = (1-t) \cdot q + t \cdot r$ and $q \leqslant s$ and $r < s$ holds $t = 0$.

(4) For all real numbers q, r, s, t such that $t \geqslant 0$ and $t \leqslant 1$ and $s = (1-t) \cdot q + t \cdot r$ and $q \geqslant s$ and $r > s$ holds $t = 0$.

(5) If $i -' k \leqslant j$, then $i \leqslant j + k$.

ISSN 1426–2630

(6) If $i \leqslant j + k$, then $i -' k \leqslant j$.

(7) If $i \leqslant j -' k$ and $k \leqslant j$, then $i + k \leqslant j$.

(8) If $j + k \leqslant i$, then $k \leqslant i -' j$.

(9) If $k \leqslant i$ and $i < j$, then $i -' k < j -' k$.

(10) If $i < j$ and $k < j$, then $i -' k < j -' k$.

(11) Let D be a non empty set, f be a non empty finite sequence of elements of D, and g be a finite sequence of elements of D. Then $\pi_{\mathrm{len}(g \frown f)}(g \frown f) = \pi_{\mathrm{len}\, f} f$.

(12) For all sets a, b, c, d holds the indices of $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle\}$.

2. Euclidean Space

We now state four propositions:

(13) For all points p, q of $\mathcal{E}^n_{\mathrm{T}}$ and for every real number r such that $0 < r$ and $p = (1 - r) \cdot p + r \cdot q$ holds $p = q$.

(14) For all points p, q of $\mathcal{E}^n_{\mathrm{T}}$ and for every real number r such that $r < 1$ and $p = (1 - r) \cdot q + r \cdot p$ holds $p = q$.

(15) For all points p, q of $\mathcal{E}^n_{\mathrm{T}}$ such that $p = \frac{1}{2} \cdot (p + q)$ holds $p = q$.

(16) For all points p, q, r of $\mathcal{E}^n_{\mathrm{T}}$ such that $q \in \mathcal{L}(p, r)$ and $r \in \mathcal{L}(p, q)$ holds $q = r$.

3. Euclidean Plane

One can prove the following propositions:

(17) Let A be a non empty subset of $\mathcal{E}^2_{\mathrm{T}}$, p be an element of the carrier of $\mathcal{E}^2$, and r be a real number. If $A = \mathrm{Ball}(p, r)$, then A is connected.

(18) For all subsets A, B of $\mathcal{E}^2_{\mathrm{T}}$ such that A is open and B is a component of A holds B is open.

(19) For all points p, q, r of $\mathcal{E}^2_{\mathrm{T}}$ such that $\mathcal{L}(p, q)$ is horizontal and $r \in \mathcal{L}(p, q)$ holds $p_{\mathbf{2}} = r_{\mathbf{2}}$.

(20) For all points p, q, r of $\mathcal{E}^2_{\mathrm{T}}$ such that $\mathcal{L}(p, q)$ is vertical and $r \in \mathcal{L}(p, q)$ holds $p_{\mathbf{1}} = r_{\mathbf{1}}$.

(21) For all points p, q, r, s of $\mathcal{E}^2_{\mathrm{T}}$ such that $\mathcal{L}(p, q)$ is horizontal and $\mathcal{L}(r, s)$ is horizontal and $\mathcal{L}(p, q)$ meets $\mathcal{L}(r, s)$ holds $p_{\mathbf{2}} = r_{\mathbf{2}}$.

(22) For all points p, q, r of $\mathcal{E}^2_{\mathrm{T}}$ such that $\mathcal{L}(p,q)$ is vertical and $\mathcal{L}(q,r)$ is horizontal holds $\mathcal{L}(p,q) \cap \mathcal{L}(q,r) = \{q\}$.

(23) For all points p, q, r, s of $\mathcal{E}^2_{\mathrm{T}}$ such that $\mathcal{L}(p,q)$ is horizontal and $\mathcal{L}(s,r)$ is vertical and $r \in \mathcal{L}(p,q)$ holds $\mathcal{L}(p,q) \cap \mathcal{L}(s,r) = \{r\}$.

4. Miscellaneous

In the sequel p, q denote points of $\mathcal{E}^2_{\mathrm{T}}$ and G denotes a Go-board.

Next we state two propositions:

(24) If $1 \leqslant j$ and $j \leqslant k$ and $k \leqslant \operatorname{width} G$ and $1 \leqslant i$ and $i \leqslant \operatorname{len} G$, then $(G_{i,j})_{\mathbf{2}} \leqslant (G_{i,k})_{\mathbf{2}}$.

(25) If $1 \leqslant j$ and $j \leqslant \operatorname{width} G$ and $1 \leqslant i$ and $i \leqslant k$ and $k \leqslant \operatorname{len} G$, then $(G_{i,j})_{\mathbf{1}} \leqslant (G_{k,j})_{\mathbf{1}}$.

In the sequel C denotes a subset of $\mathcal{E}^2_{\mathrm{T}}$.

We now state a number of propositions:

(26) $\mathcal{L}(\text{NW-corner}\, C, \text{NE-corner}\, C) \subseteq \widetilde{\mathcal{L}}(\text{SpStSeq}\, C)$.

(27) $\text{N-most}\, C \subseteq \mathcal{L}(\text{NW-corner}\, C, \text{NE-corner}\, C)$.

(28) For every non empty compact subset C of $\mathcal{E}^2_{\mathrm{T}}$ holds $\text{N-min}\, C \in \mathcal{L}(\text{NW-corner}\, C, \text{NE-corner}\, C)$.

(29) $\mathcal{L}(\text{NW-corner}\, C, \text{NE-corner}\, C)$ is horizontal.

(30) Let f be a finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$ and i, j be natural numbers. Suppose f is a special sequence and $1 \leqslant i$ and $i \leqslant j$ and $j \leqslant \operatorname{len} f$. Then LE $\pi_i f$, $\pi_j f$, $\widetilde{\mathcal{L}}(f)$, $\pi_1 f$, $\pi_{\operatorname{len} f} f$.

(31) Let g be a finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$ and p be a point of $\mathcal{E}^2_{\mathrm{T}}$. Suppose $\pi_1 g \neq p$ and $(\pi_1 g)_{\mathbf{1}} = p_{\mathbf{1}}$ or $(\pi_1 g)_{\mathbf{2}} = p_{\mathbf{2}}$ and g is a special sequence and $\mathcal{L}(p, \pi_1 g) \cap \widetilde{\mathcal{L}}(g) = \{\pi_1 g\}$. Then $\langle p \rangle \frown g$ is a special sequence.

(32) Let g be a finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$ and p be a point of $\mathcal{E}^2_{\mathrm{T}}$. Suppose $\pi_{\operatorname{len} g} g \neq p$ and $(\pi_{\operatorname{len} g} g)_{\mathbf{1}} = p_{\mathbf{1}}$ or $(\pi_{\operatorname{len} g} g)_{\mathbf{2}} = p_{\mathbf{2}}$ and g is a special sequence and $\mathcal{L}(p, \pi_{\operatorname{len} g} g) \cap \widetilde{\mathcal{L}}(g) = \{\pi_{\operatorname{len} g} g\}$. Then $g \frown \langle p \rangle$ is a special sequence.

(33) Let f be a S-sequence in $\mathbb{R}^2$ and p be a point of $\mathcal{E}^2_{\mathrm{T}}$. If $1 < j$ and $j \leqslant \operatorname{len} f$ and $p \in \widetilde{\mathcal{L}}(\operatorname{mid}(f, 1, j))$, then LE p, $\pi_j f$, $\widetilde{\mathcal{L}}(f)$, $\pi_1 f$, $\pi_{\operatorname{len} f} f$.

(34) For every finite sequence h of elements of $\mathcal{E}^2_{\mathrm{T}}$ such that $i \in \operatorname{dom} h$ and $j \in \operatorname{dom} h$ holds $\widetilde{\mathcal{L}}(\operatorname{mid}(h, i, j)) \subseteq \widetilde{\mathcal{L}}(h)$.

(35) If $1 \leqslant i$ and $i < j$, then for every finite sequence f of elements of $\mathcal{E}^2_{\mathrm{T}}$ such that $j \leqslant \operatorname{len} f$ holds $\widetilde{\mathcal{L}}(\operatorname{mid}(f, i, j)) = \mathcal{L}(f, i) \cup \widetilde{\mathcal{L}}(\operatorname{mid}(f, i+1, j))$.

(36) Let f be a finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$. If $1 \leqslant i$, then if $i < j$ and $j \leqslant \operatorname{len} f$, then $\widetilde{\mathcal{L}}(\operatorname{mid}(f, i, j)) = \widetilde{\mathcal{L}}(\operatorname{mid}(f, i, j -' 1)) \cup \mathcal{L}(f, j -' 1)$.

(37) Let g be a finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$ and p be a point of $\mathcal{E}^2_{\mathrm{T}}$. Suppose g is a special sequence and $p_{\mathbf{1}} = (\pi_1 g)_{\mathbf{1}}$ or $p_{\mathbf{2}} = (\pi_1 g)_{\mathbf{2}}$ and $\mathcal{L}(p, \pi_1 g) \cap \widetilde{\mathcal{L}}(g) = \{\pi_1 g\}$ and $p \neq \pi_1 g$. Then $\langle p \rangle \frown g$ is a special sequence.

(38) Let f, g be finite sequences of elements of $\mathcal{E}^2_{\mathrm{T}}$. Suppose that
 (i) f is a special sequence,
 (ii) g is a special sequence,
 (iii) $(\pi_{\mathrm{len}\, f} f)_{\mathbf{1}} = (\pi_1 g)_{\mathbf{1}}$ or $(\pi_{\mathrm{len}\, f} f)_{\mathbf{2}} = (\pi_1 g)_{\mathbf{2}}$,
 (iv) $\widetilde{\mathcal{L}}(f)$ misses $\widetilde{\mathcal{L}}(g)$,
 (v) $\mathcal{L}(\pi_{\mathrm{len}\, f} f, \pi_1 g) \cap \widetilde{\mathcal{L}}(f) = \{\pi_{\mathrm{len}\, f} f\}$, and
 (vi) $\mathcal{L}(\pi_{\mathrm{len}\, f} f, \pi_1 g) \cap \widetilde{\mathcal{L}}(g) = \{\pi_1 g\}$.

Then $f \frown g$ is a special sequence.

(39) For every S-sequence f in $\mathbb{R}^2$ and for every point p of $\mathcal{E}^2_{\mathrm{T}}$ such that $p \in \widetilde{\mathcal{L}}(f)$ holds $\pi_1 \downharpoonleft f, p = \pi_1 f$.

(40) Let f be a S-sequence in $\mathbb{R}^2$ and p, q be points of $\mathcal{E}^2_{\mathrm{T}}$. If $1 \leqslant j$ and $j < \mathrm{len}\, f$ and $p \in \mathcal{L}(f, j)$ and $q \in \mathcal{L}(\pi_j f, p)$, then LE q, p, $\widetilde{\mathcal{L}}(f)$, $\pi_1 f$, $\pi_{\mathrm{len}\, f} f$.

5. Special Circular Sequences

Next we state the proposition

(41) For every non constant standard special circular sequence f holds LeftComp(f) is open and RightComp(f) is open.

Let f be a non constant standard special circular sequence. One can verify the following observations:

* $\widetilde{\mathcal{L}}(f)$ is non vertical and non horizontal,
* LeftComp(f) is region, and
* RightComp(f) is region.

One can prove the following propositions:

(42) For every non constant standard special circular sequence f holds RightComp(f) misses $\widetilde{\mathcal{L}}(f)$.

(43) For every non constant standard special circular sequence f holds LeftComp(f) misses $\widetilde{\mathcal{L}}(f)$.

(44) For every non constant standard special circular sequence f holds $\mathrm{i}_{\mathrm{WN}}\, f < \mathrm{i}_{\mathrm{EN}}\, f$.

(45) Let f be a non constant standard special circular sequence. Then there exists i such that $1 \leqslant i$ and $i < \mathrm{len}$ the Go-board of f and N-min $\widetilde{\mathcal{L}}(f) =$ (the Go-board of $f)_{i, \mathrm{width\,the\,Go\text{-}board\,of}\,f}$.

(46) Let f be a clockwise oriented non constant standard special circular sequence. Suppose $i \in \operatorname{dom}$ the Go-board of f and $\pi_1 f =$ (the Go-board of $f)_{i,\text{width the Go-board of } f}$ and $\pi_1 f = \text{N-min}\,\widetilde{\mathcal{L}}(f)$. Then $\pi_2 f =$ (the Go-board of $f)_{i+1,\text{width the Go-board of } f}$ and $\pi_{\operatorname{len} f -' 1} f =$ (the Go-board of $f)_{i,\text{width the Go-board of } f -' 1}$.

(47) Let f be a non constant standard special circular sequence. If $1 \leqslant i$ and $i < j$ and $j \leqslant \operatorname{len} f$ and $\pi_1 f \in \widetilde{\mathcal{L}}(\operatorname{mid}(f, i, j))$, then $i = 1$ or $j = \operatorname{len} f$.

(48) Let f be a clockwise oriented non constant standard special circular sequence. If $\pi_1 f = \text{N-min}\,\widetilde{\mathcal{L}}(f)$, then $\mathcal{L}(\pi_1 f, \pi_2 f) \subseteq \widetilde{\mathcal{L}}(\text{SpStSeq}\,\widetilde{\mathcal{L}}(f))$.

6. Rectangular Sequences

We now state the proposition

(49) Let f be a rectangular finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$ and p be a point of $\mathcal{E}^2_{\mathrm{T}}$. If $p \in \widetilde{\mathcal{L}}(f)$, then $p_{\mathbf{1}} = \text{W-bound}\,\widetilde{\mathcal{L}}(f)$ or $p_{\mathbf{1}} = \text{E-bound}\,\widetilde{\mathcal{L}}(f)$ or $p_{\mathbf{2}} = \text{S-bound}\,\widetilde{\mathcal{L}}(f)$ or $p_{\mathbf{2}} = \text{N-bound}\,\widetilde{\mathcal{L}}(f)$.

One can check that there exists a special circular sequence which is rectangular.

The following propositions are true:

(50) Let f be a rectangular special circular sequence and g be a S-sequence in $\mathbb{R}^2$. If $\pi_1 g \in \text{LeftComp}(f)$ and $\pi_{\operatorname{len} g} g \in \text{RightComp}(f)$, then $\widetilde{\mathcal{L}}(f)$ meets $\widetilde{\mathcal{L}}(g)$.

(51) For every rectangular special circular sequence f holds $\text{SpStSeq}\,\widetilde{\mathcal{L}}(f) = f$.

(52) Let f be a rectangular special circular sequence. Then $\widetilde{\mathcal{L}}(f) = \{p; p$ ranges over points of $\mathcal{E}^2_{\mathrm{T}}$: $p_{\mathbf{1}} = \text{W-bound}\,\widetilde{\mathcal{L}}(f) \wedge p_{\mathbf{2}} \leqslant \text{N-bound}\,\widetilde{\mathcal{L}}(f) \wedge p_{\mathbf{2}} \geqslant \text{S-bound}\,\widetilde{\mathcal{L}}(f) \vee p_{\mathbf{1}} \leqslant \text{E-bound}\,\widetilde{\mathcal{L}}(f) \wedge p_{\mathbf{1}} \geqslant \text{W-bound}\,\widetilde{\mathcal{L}}(f) \wedge p_{\mathbf{2}} = \text{N-bound}\,\widetilde{\mathcal{L}}(f) \vee p_{\mathbf{1}} \leqslant \text{E-bound}\,\widetilde{\mathcal{L}}(f) \wedge p_{\mathbf{1}} \geqslant \text{W-bound}\,\widetilde{\mathcal{L}}(f) \wedge p_{\mathbf{2}} = \text{S-bound}\,\widetilde{\mathcal{L}}(f) \vee p_{\mathbf{1}} = \text{E-bound}\,\widetilde{\mathcal{L}}(f) \wedge p_{\mathbf{2}} \leqslant \text{N-bound}\,\widetilde{\mathcal{L}}(f) \wedge p_{\mathbf{2}} \geqslant \text{S-bound}\,\widetilde{\mathcal{L}}(f)\}$.

(53) For every rectangular special circular sequence f holds the Go-board of $f = \begin{pmatrix} \pi_4 f & \pi_1 f \\ \pi_3 f & \pi_2 f \end{pmatrix}$.

(54) Let f be a rectangular special circular sequence. Then $\text{LeftComp}(f) = \{p : \text{W-bound}\,\widetilde{\mathcal{L}}(f) \nleqslant p_{\mathbf{1}} \vee p_{\mathbf{1}} \nleqslant \text{E-bound}\,\widetilde{\mathcal{L}}(f) \vee \text{S-bound}\,\widetilde{\mathcal{L}}(f) \nleqslant p_{\mathbf{2}} \vee p_{\mathbf{2}} \nleqslant \text{N-bound}\,\widetilde{\mathcal{L}}(f)\}$ and $\text{RightComp}(f) = \{q : \text{W-bound}\,\widetilde{\mathcal{L}}(f) < q_{\mathbf{1}} \wedge q_{\mathbf{1}} < \text{E-bound}\,\widetilde{\mathcal{L}}(f) \wedge \text{S-bound}\,\widetilde{\mathcal{L}}(f) < q_{\mathbf{2}} \wedge q_{\mathbf{2}} < \text{N-bound}\,\widetilde{\mathcal{L}}(f)\}$.

One can check that there exists a rectangular special circular sequence which is clockwise oriented.

One can check that every rectangular special circular sequence is clockwise oriented.

Next we state four propositions:

(55) Let f be a rectangular special circular sequence and g be a S-sequence in $\mathbb{R}^2$. If $\pi_1 g \in \mathrm{LeftComp}(f)$ and $\pi_{\mathrm{len}\, g} g \in \mathrm{RightComp}(f)$, then $\mathrm{LPoint}(\widetilde{\mathcal{L}}(g), \pi_1 g, \pi_{\mathrm{len}\, g} g, \widetilde{\mathcal{L}}(f)) \neq \text{NW-corner}\, \widetilde{\mathcal{L}}(f)$.

(56) Let f be a rectangular special circular sequence and g be a S-sequence in $\mathbb{R}^2$. If $\pi_1 g \in \mathrm{LeftComp}(f)$ and $\pi_{\mathrm{len}\, g} g \in \mathrm{RightComp}(f)$, then $\mathrm{LPoint}(\widetilde{\mathcal{L}}(g), \pi_1 g, \pi_{\mathrm{len}\, g} g, \widetilde{\mathcal{L}}(f)) \neq \text{SE-corner}\, \widetilde{\mathcal{L}}(f)$.

(57) Let f be a rectangular special circular sequence and p be a point of $\mathcal{E}^2_{\mathrm{T}}$. If $\text{W-bound}\, \widetilde{\mathcal{L}}(f) > p_{\mathbf{1}}$ or $p_{\mathbf{1}} > \text{E-bound}\, \widetilde{\mathcal{L}}(f)$ or $\text{S-bound}\, \widetilde{\mathcal{L}}(f) > p_{\mathbf{2}}$ or $p_{\mathbf{2}} > \text{N-bound}\, \widetilde{\mathcal{L}}(f)$, then $p \in \mathrm{LeftComp}(f)$.

(58) For every clockwise oriented non constant standard special circular sequence f such that $\pi_1 f = \text{N-min}\, \widetilde{\mathcal{L}}(f)$ holds $\mathrm{LeftComp}(\mathrm{SpStSeq}\, \widetilde{\mathcal{L}}(f)) \subseteq \mathrm{LeftComp}(f)$.

7. In the Area

Next we state a number of propositions:

(59) Let f be a finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$ and p, q be points of $\mathcal{E}^2_{\mathrm{T}}$. Then $\langle p, q \rangle$ is in the area of f if and only if $\langle p \rangle$ is in the area of f and $\langle q \rangle$ is in the area of f.

(60) Let f be a rectangular finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$ and p be a point of $\mathcal{E}^2_{\mathrm{T}}$. Suppose $\langle p \rangle$ is in the area of f but $p_{\mathbf{1}} = \text{W-bound}\, \widetilde{\mathcal{L}}(f)$ or $p_{\mathbf{1}} = \text{E-bound}\, \widetilde{\mathcal{L}}(f)$ or $p_{\mathbf{2}} = \text{S-bound}\, \widetilde{\mathcal{L}}(f)$ or $p_{\mathbf{2}} = \text{N-bound}\, \widetilde{\mathcal{L}}(f)$. Then $p \in \widetilde{\mathcal{L}}(f)$.

(61) Let f be a finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$, p, q be points of $\mathcal{E}^2_{\mathrm{T}}$, and r be a real number. Suppose $0 \leqslant r$ and $r \leqslant 1$ and $\langle p, q \rangle$ is in the area of f. Then $\langle (1-r) \cdot p + r \cdot q \rangle$ is in the area of f.

(62) Let f, g be finite sequences of elements of $\mathcal{E}^2_{\mathrm{T}}$. If g is in the area of f and $i \in \mathrm{dom}\, g$, then $\langle \pi_i g \rangle$ is in the area of f.

(63) Let f, g be finite sequences of elements of $\mathcal{E}^2_{\mathrm{T}}$ and p be a point of $\mathcal{E}^2_{\mathrm{T}}$. If g is in the area of f and $p \in \widetilde{\mathcal{L}}(g)$, then $\langle p \rangle$ is in the area of f.

(64) Let f be a rectangular finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$ and p, q be points of $\mathcal{E}^2_{\mathrm{T}}$. If $q \notin \widetilde{\mathcal{L}}(f)$ and $\langle p, q \rangle$ is in the area of f, then $\mathcal{L}(p, q) \cap \widetilde{\mathcal{L}}(f) \subseteq \{p\}$.

(65) Let f be a rectangular finite sequence of elements of $\mathcal{E}^2_{\mathrm{T}}$ and p, q be points of $\mathcal{E}^2_{\mathrm{T}}$. If $p \in \widetilde{\mathcal{L}}(f)$ and $q \notin \widetilde{\mathcal{L}}(f)$ and $\langle q \rangle$ is in the area of f, then $\mathcal{L}(p, q) \cap \widetilde{\mathcal{L}}(f) = \{p\}$.

(66) Let f be a non constant standard special circular sequence. Suppose $1 \leqslant i$ and $i \leqslant \operatorname{len}$ the Go-board of f and $1 \leqslant j$ and $j \leqslant \operatorname{width}$ the Go-board of f. Then $\langle(\text{the Go-board of } f)_{i,j}\rangle$ is in the area of f.

(67) Let g be a finite sequence of elements of $\mathcal{E}^2_{\rm T}$ and p, q be points of $\mathcal{E}^2_{\rm T}$. If $\langle p, q\rangle$ is in the area of g, then $\langle \frac{1}{2} \cdot (p+q)\rangle$ is in the area of g.

(68) For all finite sequences f, g of elements of $\mathcal{E}^2_{\rm T}$ such that g is in the area of f holds $\operatorname{Rev}(g)$ is in the area of f.

(69) Let f, g be finite sequences of elements of $\mathcal{E}^2_{\rm T}$ and p be a point of $\mathcal{E}^2_{\rm T}$. Suppose that

(i) g is in the area of f,

(ii) $\langle p\rangle$ is in the area of f,

(iii) g is a special sequence, and

(iv) there exists a natural number i such that $1 \leqslant i$ and $i+1 \leqslant \operatorname{len} g$ and $p \in \mathcal{L}(g, i)$.

Then $\downharpoonleft g, p$ is in the area of f.

(70) Let f be a non constant standard special circular sequence and g be a finite sequence of elements of $\mathcal{E}^2_{\rm T}$. Then g is in the area of f if and only if g is in the area of $\operatorname{SpStSeq} \widetilde{\mathcal{L}}(f)$.

(71) Let f be a rectangular special circular sequence and g be a S-sequence in $\mathbb{R}^2$. If $\pi_1 g \in \operatorname{LeftComp}(f)$ and $\pi_{\operatorname{len} g} g \in \operatorname{RightComp}(f)$, then $\downharpoonright \operatorname{LPoint}(\widetilde{\mathcal{L}}(g), \pi_1 g, \pi_{\operatorname{len} g} g, \widetilde{\mathcal{L}}(f)), g$ is in the area of f.

(72) Let f be a non constant standard special circular sequence. Suppose $1 \leqslant i$ and $i < \operatorname{len}$ the Go-board of f and $1 \leqslant j$ and $j < \operatorname{width}$ the Go-board of f. Then $\operatorname{Int} \operatorname{cell}(\text{the Go-board of } f, i, j)$ misses $\widetilde{\mathcal{L}}(\operatorname{SpStSeq} \widetilde{\mathcal{L}}(f))$.

References

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

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

[3] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[4] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(**2**):241–245, 1996.

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

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

[7] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.

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

[9] Adam Grabowski and Yatsuka Nakamura. The ordering of points on a curve. Part II. *Formalized Mathematics*, 6(**4**):467–473, 1997.

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

[11] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.

[12] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Formalized Mathematics*, 2(**5**):711–717, 1991.
[13] Stanisława Kanas, Adam Lecko, and Mariusz Startek. Metric spaces. *Formalized Mathematics*, 1(**3**):607–610, 1990.
[14] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.
[15] Jarosław Kotowicz and Yatsuka Nakamura. Introduction to Go-board - part I. *Formalized Mathematics*, 3(**1**):107–115, 1992.
[16] Jarosław Kotowicz and Yatsuka Nakamura. Introduction to Go-board - part II. *Formalized Mathematics*, 3(**1**):117–121, 1992.
[17] Yatsuka Nakamura and Czesław Byliński. Extremal properties of vertices on special polygons. Part I. *Formalized Mathematics*, 5(**1**):97–102, 1996.
[18] Yatsuka Nakamura and Adam Grabowski. Bounding boxes for special sequences in $\mathcal{E}^2$. *Formalized Mathematics*, 7(**1**):115–121, 1998.
[19] Yatsuka Nakamura and Roman Matuszewski. Reconstructions of special sequences. *Formalized Mathematics*, 6(**2**):255–263, 1997.
[20] Yatsuka Nakamura and Andrzej Trybulec. Decomposing a Go-board into cells. *Formalized Mathematics*, 5(**3**):323–328, 1996.
[21] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[22] Beata Padlewska. Connected spaces. *Formalized Mathematics*, 1(**1**):239–244, 1990.
[23] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[24] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[25] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[26] Andrzej Trybulec. Left and right component of the complement of a special closed curve. *Formalized Mathematics*, 5(**4**):465–468, 1996.
[27] Andrzej Trybulec. On the decomposition of finite sequences. *Formalized Mathematics*, 5(**3**):317–322, 1996.
[28] Andrzej Trybulec and Yatsuka Nakamura. On the order on a special polygon. *Formalized Mathematics*, 6(**4**):541–548, 1997.
[29] Andrzej Trybulec and Yatsuka Nakamura. On the rectangular finite sequences of the points of the plane. *Formalized Mathematics*, 6(**4**):531–539, 1997.
[30] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[32] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[33] Mirosław Wysocki and Agata Darmochwał. Subsets of topological spaces. *Formalized Mathematics*, 1(**1**):231–237, 1990.

Received October 22, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Real Linear-Metric Space and Isometric Functions

Robert Milewski
University of Białystok

MML Identifier: VECTMETR.

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

1. Convex and Internal Metric Spaces

Let V be a non empty metric structure. We say that V is convex if and only if the condition (Def. 1) is satisfied.

(Def. 1) Let x, y be elements of the carrier of V and r be a real number. Suppose $0 \leqslant r$ and $r \leqslant 1$. Then there exists an element z of the carrier of V such that $\rho(x, z) = r \cdot \rho(x, y)$ and $\rho(z, y) = (1 - r) \cdot \rho(x, y)$.

Let V be a non empty metric structure. We say that V is internal if and only if the condition (Def. 2) is satisfied.

(Def. 2) Let x, y be elements of the carrier of V and p, q be real numbers. Suppose $p > 0$ and $q > 0$. Then there exists a finite sequence f of elements of the carrier of V such that

(i) $\pi_1 f = x$,

(ii) $\pi_{\mathrm{len}\, f} f = y$,

(iii) for every natural number i such that $1 \leqslant i$ and $i \leqslant \mathrm{len}\, f - 1$ holds $\rho(\pi_i f, \pi_{i+1} f) < p$, and

(iv) for every finite sequence F of elements of $\mathbb{R}$ such that $\mathrm{len}\, F = \mathrm{len}\, f - 1$ and for every natural number i such that $1 \leqslant i$ and $i \leqslant \mathrm{len}\, F$ holds $\pi_i F = \rho(\pi_i f, \pi_{i+1} f)$ holds $|\rho(x, y) - \sum F| < q$.

One can prove the following proposition

ISSN 1426–2630

(1) Let V be a non empty metric space. Suppose V is convex. Let x, y be elements of the carrier of V and p be a real number. Suppose $p > 0$. Then there exists a finite sequence f of elements of the carrier of V such that

(i) $\pi_1 f = x$,

(ii) $\pi_{\operatorname{len} f} f = y$,

(iii) for every natural number i such that $1 \leqslant i$ and $i \leqslant \operatorname{len} f - 1$ holds $\rho(\pi_i f, \pi_{i+1} f) < p$, and

(iv) for every finite sequence F of elements of $\mathbb{R}$ such that $\operatorname{len} F = \operatorname{len} f - 1$ and for every natural number i such that $1 \leqslant i$ and $i \leqslant \operatorname{len} F$ holds $\pi_i F = \rho(\pi_i f, \pi_{i+1} f)$ holds $\rho(x, y) = \sum F$.

Let us observe that every non empty metric space which is convex is also internal.

One can verify that there exists a non empty metric space which is convex.

A Geometry is a Reflexive discernible symmetric triangle internal non empty metric structure.

2. Isometric Functions

Let V be a non empty metric structure and let f be a map from V into V. We say that f is isometric if and only if:

(Def. 3) $\operatorname{rng} f =$ the carrier of V and for all elements x, y of the carrier of V holds $\rho(x, y) = \rho(f(x), f(y))$.

Let V be a non empty metric structure. The functor $\mathrm{ISOM}\, V$ yields a set and is defined as follows:

(Def. 4) For every set x holds $x \in \mathrm{ISOM}\, V$ iff there exists a map f from V into V such that $f = x$ and f is isometric.

Let V be a non empty metric structure. Then $\mathrm{ISOM}\, V$ is a subset of (the carrier of V)$^{\text{the carrier of } V}$.

One can prove the following proposition

(2) Let V be a discernible Reflexive non empty metric structure and f be a map from V into V. If f is isometric, then f is one-to-one.

Let V be a discernible Reflexive non empty metric structure. One can check that every map from V into V which is isometric is also one-to-one.

Let V be a non empty metric structure. Observe that there exists a map from V into V which is isometric.

The following three propositions are true:

(3) Let V be a discernible Reflexive non empty metric structure and f be an isometric map from V into V. Then f^{-1} is isometric.

(4) For every non empty metric structure V and for all isometric maps f, g from V into V holds $f \cdot g$ is isometric.

(5) For every non empty metric structure V holds id_V is isometric.

Let V be a non empty metric structure. Note that $\mathrm{ISOM}\,V$ is non empty.

3. Real Linear-Metric Spaces

We introduce RLSMetrStruct which are extensions of RLS structure and metric structure and are systems

$\langle$ a carrier, a distance, a zero, an addition, an external multiplication $\rangle$,

where the carrier is a set, the distance is a function from $[\!:$ the carrier, the carrier $:\!]$ into $\mathbb{R}$, the zero is an element of the carrier, the addition is a binary operation on the carrier, and the external multiplication is a function from $[\!: \mathbb{R}$, the carrier $:\!]$ into the carrier.

One can verify that there exists a RLSMetrStruct which is non empty and strict.

Let X be a non empty set, let F be a function from $[\!: X, X :\!]$ into $\mathbb{R}$, let O be an element of X, let B be a binary operation on X, and let G be a function from $[\!: \mathbb{R}, X :\!]$ into X. One can verify that $\langle X, F, O, B, G\rangle$ is non empty.

Let V be a non empty RLSMetrStruct. We say that V is homogeneous if and only if:

(Def. 5) For every real number r and for all elements v, w of the carrier of V holds $\rho(r \cdot v, r \cdot w) = |r| \cdot \rho(v, w)$.

Let V be a non empty RLSMetrStruct. We say that V is translatible if and only if:

(Def. 6) For all elements u, w, v of the carrier of V holds $\rho(v, w) = \rho(v+u, w+u)$.

Let V be a non empty RLSMetrStruct and let v be an element of the carrier of V. The functor $\mathrm{Norm}\,v$ yielding a real number is defined as follows:

(Def. 7) $\mathrm{Norm}\,v = \rho(0_V, v)$.

Let us note that there exists a non empty RLSMetrStruct which is strict, Abelian, add-associative, right zeroed, right complementable, real linear space-like, Reflexive, discernible, symmetric, triangle, homogeneous, and translatible.

A RealLinearMetrSpace is an Abelian add-associative right zeroed right complementable real linear space-like Reflexive discernible symmetric triangle homogeneous translatible non empty RLSMetrStruct.

We now state three propositions:

(6) Let V be a homogeneous Abelian add-associative right zeroed right complementable real linear space-like non empty RLSMetrStruct, r be a real number, and v be an element of the carrier of V. Then $\mathrm{Norm}(r \cdot v) = |r| \cdot \mathrm{Norm}\,v$.

(7) Let V be a translatible Abelian add-associative right zeroed right complementable triangle non empty RLSMetrStruct and v, w be elements of the carrier of V. Then $\mathrm{Norm}(v + w) \leqslant \mathrm{Norm}\, v + \mathrm{Norm}\, w$.

(8) Let V be a translatible add-associative right zeroed right complementable non empty RLSMetrStruct and v, w be elements of the carrier of V. Then $\rho(v, w) = \mathrm{Norm}(w - v)$.

Let n be a natural number. The functor RLMSpace n yielding a strict RealLinearMetrSpace is defined by the conditions (Def. 8).

(Def. 8)(i) The carrier of RLMSpace $n = \mathcal{R}^n$,

(ii) the distance of RLMSpace $n = \rho^n$,

(iii) the zero of RLMSpace $n = \langle\underbrace{0, \ldots, 0}_{n}\rangle$,

(iv) for all elements x, y of $\mathcal{R}^n$ holds (the addition of RLMSpace n)(x, y) $= x + y$, and

(v) for every element x of $\mathcal{R}^n$ and for every element r of $\mathbb{R}$ holds (the external multiplication of RLMSpace n)(r, x) $= r \cdot x$.

Next we state the proposition

(9) For every natural number n and for every isometric map f from RLMSpace n into RLMSpace n holds $\mathrm{rng}\, f = \mathcal{R}^n$.

4. Groups of Isometric Functions

Let n be a natural number. The functor IsomGroup n yielding a strict groupoid is defined by the conditions (Def. 9).

(Def. 9)(i) The carrier of IsomGroup n = ISOM RLMSpace n, and

(ii) for all functions f, g such that $f \in$ ISOM RLMSpace n and $g \in$ ISOM RLMSpace n holds (the multiplication of IsomGroup n)(f, g) $= f \cdot g$.

Let n be a natural number. Note that IsomGroup n is non empty.

Let n be a natural number. Note that IsomGroup n is associative and group-like.

The following two propositions are true:

(10) For every natural number n holds $1_{\mathrm{IsomGroup}\, n} = \mathrm{id}_{\mathrm{RLMSpace}\, n}$.

(11) Let n be a natural number, f be an element of IsomGroup n, and g be a map from RLMSpace n into RLMSpace n. If $f = g$, then $f^{-1} = g^{-1}$.

Let n be a natural number and let G be a subgroup of IsomGroup n. The functor SubIsomGroupRel G yielding a binary relation on the carrier of RLMSpace n is defined by the condition (Def. 10).

(Def. 10) Let A, B be elements of RLMSpace n. Then $\langle A, B \rangle \in$ SubIsomGroupRel G if and only if there exists a function f such that $f \in$ the carrier of G and $f(A) = B$.

Let n be a natural number and let G be a subgroup of IsomGroup n. Observe that SubIsomGroupRel G is equivalence relation-like.

References

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

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

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

[4] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

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

[6] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.

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

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

[9] Michał Muzalewski. Categories of groups. *Formalized Mathematics*, 2(**4**):563–571, 1991.

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

[11] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

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

[13] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

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

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

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

Received November 3, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Introduction to Meet-Continuous Topological Lattices[1]

Artur Korniłowicz
University of Białystok

MML Identifier: YELLOW13.

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

1. Preliminaries

Let S be a finite 1-sorted structure. One can verify that the carrier of S is finite.

Let S be a trivial 1-sorted structure. One can check that the carrier of S is trivial.

One can check that every set which is trivial is also finite.

One can verify that every 1-sorted structure which is trivial is also finite.

Let us mention that every 1-sorted structure which is non trivial is also non empty.

One can check the following observations:

* there exists a 1-sorted structure which is strict, non empty, and trivial,
* there exists a relational structure which is strict, non empty, and trivial, and
* there exists a FR-structure which is strict, non empty, and trivial.

We now state the proposition

(1) For every T_1 non empty topological space T holds every finite subset of T is closed.

[1]This work has been supported by KBN Grant 8 T11C 018 12.

ISSN 1426–2630

Let T be a compact topological structure. Observe that Ω_T is compact.

Let us observe that there exists a topological space which is strict, non empty, and trivial.

Let us mention that every non empty topological space which is finite and T_1 is also discrete.

Let us observe that every topological space which is finite is also compact.

One can prove the following propositions:

(2) Every discrete non empty topological space is a T_4 space.

(3) Every discrete non empty topological space is a T_3 space.

(4) Every discrete non empty topological space is a T_2 space.

(5) Every discrete non empty topological space is a T_1 space.

One can check that every non empty topological space which is T_4 and T_1 is also T_3.

Let us observe that every non empty topological space which is T_3 and T_1 is also T_2.

Let us note that every topological space which is T_2 is also T_1.

One can check that every topological space which is T_1 is also T_0.

Next we state three propositions:

(6) Let S be a reflexive relational structure, T be a reflexive transitive relational structure, f be a map from S into T, and X be a subset of S. Then $\downarrow(f^\circ X) \subseteq \downarrow(f^\circ \downarrow X)$.

(7) Let S be a reflexive relational structure, T be a reflexive transitive relational structure, f be a map from S into T, and X be a subset of S. If f is monotone, then $\downarrow(f^\circ X) = \downarrow(f^\circ \downarrow X)$.

(8) For every non empty poset N holds $\mathrm{IdsMap}(N)$ is one-to-one.

One can prove the following proposition

(9) For every finite lattice N holds $\mathrm{SupMap}(N)$ is one-to-one.

We now state three propositions:

(10) For every finite lattice N holds N and $\langle \mathrm{Ids}(N), \subseteq \rangle$ are isomorphic.

(11) Let N be a complete non empty poset, x be an element of N, and X be a non empty subset of N. Then $x \sqcap \Box$ preserves inf of X.

(12) For every complete non empty poset N and for every element x of N holds $x \sqcap \Box$ is meet-preserving.

2. On the Basis of Topological Spaces

Next we state several propositions:

(13) Let T be an anti-discrete non empty topological structure and p be a point of T. Then $\{$the carrier of $T\}$ is a basis of p.

(14) Let T be an anti-discrete non empty topological structure, p be a point of T, and D be a basis of p. Then $D = \{$the carrier of $T\}$.

(15) Let T be a non empty topological space, P be a basis of T, and p be a point of T. Then $\{A; A$ ranges over subsets of T: $A \in P \ \wedge \ p \in A\}$ is a basis of p.

(16) Let T be a non empty topological structure, A be a subset of T, and p be a point of T. Then $p \in \overline{A}$ if and only if for every basis K of p and for every subset Q of T such that $Q \in K$ holds $A \cap Q \neq \emptyset$.

(17) Let T be a non empty topological structure, A be a subset of T, and p be a point of T. Then $p \in \overline{A}$ if and only if there exists a basis K of p such that for every subset Q of T such that $Q \in K$ holds $A \cap Q \neq \emptyset$.

Let T be a topological structure and let p be a point of T. A family of subsets of T is said to be a generalized basis of p if:

(Def. 1) For every subset A of T such that $p \in \operatorname{Int} A$ there exists a subset P of T such that $P \in$ it and $p \in \operatorname{Int} P$ and $P \subseteq A$.

Let T be a non empty topological space and let p be a point of T. Let us note that the generalized basis of p can be characterized by the following (equivalent) condition:

(Def. 2) For every neighbourhood A of p there exists a neighbourhood P of p such that $P \in$ it and $P \subseteq A$.

The following propositions are true:

(18) Let T be a topological structure and p be a point of T. Then $2^{\text{the carrier of } T}$ is a generalized basis of p.

(19) For every non empty topological space T and for every point p of T holds every generalized basis of p is non empty.

Let T be a topological structure and let p be a point of T. Observe that there exists a generalized basis of p which is non empty.

Let T be a topological structure, let p be a point of T, and let P be a generalized basis of p. We say that P is correct if and only if:

(Def. 3) For every subset A of T holds $A \in P$ iff $p \in \operatorname{Int} A$.

Let T be a topological structure and let p be a point of T. Note that there exists a generalized basis of p which is correct.

One can prove the following proposition

(20) Let T be a topological structure and p be a point of T. Then $\{A; A$ ranges over subsets of T: $p \in \operatorname{Int} A\}$ is a correct generalized basis of p.

Let T be a non empty topological space and let p be a point of T. Observe that there exists a generalized basis of p which is non empty and correct.

One can prove the following three propositions:

(21) Let T be an anti-discrete non empty topological structure and p be a point of T. Then $\{$the carrier of $T\}$ is a correct generalized basis of p.

(22) Let T be an anti-discrete non empty topological structure, p be a point of T, and D be a correct generalized basis of p. Then $D = \{$the carrier of $T\}$.

(23) For every non empty topological space T and for every point p of T holds every basis of p is a generalized basis of p.

Let T be a topological structure. A family of subsets of T is said to be a generalized basis of T if:

(Def. 4) For every point p of T holds it is a generalized basis of p.

Next we state two propositions:

(24) For every topological structure T holds $2^{\text{the carrier of } T}$ is a generalized basis of T.

(25) For every non empty topological space T holds every generalized basis of T is non empty.

Let T be a topological structure. Note that there exists a generalized basis of T which is non empty.

Next we state two propositions:

(26) For every non empty topological space T and for every generalized basis P of T holds the topology of $T \subseteq \operatorname{UniCl}(\operatorname{Int} P)$.

(27) For every topological space T holds every basis of T is a generalized basis of T.

Let T be a non empty topological space-like FR-structure. We say that T is topological semilattice if and only if:

(Def. 5) For every map f from $[\!:T, (T$ **qua** topological space$)\,:\!]$ into T such that $f = \sqcap_T$ holds f is continuous.

Let us note that every non empty topological space-like FR-structure which is reflexive and trivial is also topological semilattice.

Let us mention that there exists a FR-structure which is reflexive, trivial, non empty, and topological space-like.

We now state the proposition

(28) Let T be a topological semilattice non empty topological space-like FR-structure and x be an element of T. Then $x \sqcap \square$ is continuous.

References

[1] Grzegorz Bancerek. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.
[2] Grzegorz Bancerek. Directed sets, nets, ideals, filters, and maps. *Formalized Mathematics*, 6(**1**):93–107, 1997.
[3] Józef Białas and Yatsuka Nakamura. Dyadic numbers and T_4 topological spaces. *Formalized Mathematics*, 5(**3**):361–366, 1996.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Czesław Byliński. Galois connections. *Formalized Mathematics*, 6(**1**):131–143, 1997.
[6] Agata Darmochwał. Compact spaces. *Formalized Mathematics*, 1(**2**):383–386, 1990.
[7] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[8] Adam Grabowski. On the category of posets. *Formalized Mathematics*, 5(**4**):501–505, 1996.
[9] Adam Grabowski and Robert Milewski. Boolean posets, posets under inclusion and products of relational structures. *Formalized Mathematics*, 6(**1**):117–121, 1997.
[10] Zbigniew Karno. The lattice of domains of an extremally disconnected space. *Formalized Mathematics*, 3(**2**):143–149, 1992.
[11] Zbigniew Karno and Toshihiko Watanabe. Completeness of the lattices of domains of a topological space. *Formalized Mathematics*, 3(**1**):71–79, 1992.
[12] Artur Korniłowicz. On the topological properties of meet-continuous lattices. *Formalized Mathematics*, 6(**2**):269–277, 1997.
[13] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[14] Alexander Yu. Shibakov and Andrzej Trybulec. The Cantor set. *Formalized Mathematics*, 5(**2**):233–236, 1996.
[15] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[16] Andrzej Trybulec. Baire spaces, Sober spaces. *Formalized Mathematics*, 6(**2**):289–294, 1997.
[17] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[18] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[20] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[21] Mirosław Wysocki and Agata Darmochwał. Subsets of topological spaces. *Formalized Mathematics*, 1(**1**):231–237, 1990.
[22] Mariusz Żynel and Czesław Byliński. Properties of relational structures, posets, lattices and maps. *Formalized Mathematics*, 6(**1**):123–130, 1997.

Received November 3, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Bases of Continuous Lattices[1]

Robert Milewski
University of Białystok

Summary. The article is a Mizar formalization of [7, 168–169]. We show definition and fundamental theorems from theory of basis of continuous lattices.

MML Identifier: `WAYBEL23`.

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

1. Preliminaries

The following proposition is true

(1) For every non empty poset L and for every element x of L holds compactbelow$(x) = {\downarrow}x \cap$ the carrier of CompactSublatt(L).

Let L be a non empty reflexive transitive relational structure and let X be a subset of $\langle \mathrm{Ids}(L), \subseteq \rangle$. Then $\bigcup X$ is a subset of L.

The following propositions are true:

(2) For every non empty relational structure L and for all subsets X, Y of the carrier of L such that $X \subseteq Y$ holds finsups$(X) \subseteq$ finsups(Y).

(3) Let L be a non empty transitive relational structure, S be a sups-inheriting non empty full relational substructure of L, X be a subset of the carrier of L, and Y be a subset of the carrier of S. If $X = Y$, then finsups$(X) \subseteq$ finsups(Y).

(4) Let L be a complete transitive antisymmetric non empty relational structure, S be a sups-inheriting non empty full relational substructure of L, X be a subset of the carrier of L, and Y be a subset of the carrier of S. If $X = Y$, then finsups$(X) =$ finsups(Y).

[1]This work has been supported by KBN Grant 8 T11C 018 12.

ISSN 1426–2630

(5) Let L be a complete sup-semilattice and S be a join-inheriting non empty full relational substructure of L. Suppose $\bot_L \in$ the carrier of S. Let X be a subset of L and Y be a subset of S. If $X = Y$, then $\mathrm{finsups}(Y) \subseteq \mathrm{finsups}(X)$.

(6) For every lower-bounded sup-semilattice L and for every subset X of $\langle \mathrm{Ids}(L), \subseteq \rangle$ holds $\sup X = {\downarrow}\mathrm{finsups}(\bigcup X)$.

(7) For every reflexive transitive relational structure L and for every subset X of L holds ${\downarrow}{\downarrow}X = {\downarrow}X$.

(8) For every reflexive transitive relational structure L and for every subset X of L holds ${\uparrow}{\uparrow}X = {\uparrow}X$.

(9) For every non empty reflexive transitive relational structure L and for every element x of L holds ${\downarrow}{\downarrow}x = {\downarrow}x$.

(10) For every non empty reflexive transitive relational structure L and for every element x of L holds ${\uparrow}{\uparrow}x = {\uparrow}x$.

(11) Let L be a non empty relational structure, S be a non empty relational substructure of L, X be a subset of L, and Y be a subset of S. If $X = Y$, then ${\downarrow}Y \subseteq {\downarrow}X$.

(12) Let L be a non empty relational structure, S be a non empty relational substructure of L, X be a subset of L, and Y be a subset of S. If $X = Y$, then ${\uparrow}Y \subseteq {\uparrow}X$.

(13) Let L be a non empty relational structure, S be a non empty relational substructure of L, x be an element of L, and y be an element of S. If $x = y$, then ${\downarrow}y \subseteq {\downarrow}x$.

(14) Let L be a non empty relational structure, S be a non empty relational substructure of L, x be an element of L, and y be an element of S. If $x = y$, then ${\uparrow}y \subseteq {\uparrow}x$.

2. Relational Subsets

Let L be a non empty relational structure and let S be a subset of L. We say that S is meet-closed if and only if:

(Def. 1) $\mathrm{sub}(S)$ is meet-inheriting.

Let L be a non empty relational structure and let S be a subset of L. We say that S is join-closed if and only if:

(Def. 2) $\mathrm{sub}(S)$ is join-inheriting.

Let L be a non empty relational structure and let S be a subset of L. We say that S is infs-closed if and only if:

(Def. 3) $\mathrm{sub}(S)$ is infs-inheriting.

Let L be a non empty relational structure and let S be a subset of L. We say that S is sups-closed if and only if:

(Def. 4) $\operatorname{sub}(S)$ is sups-inheriting.

Let L be a non empty relational structure. Observe that every subset of L which is infs-closed is also meet-closed and every subset of L which is sups-closed is also join-closed.

Let L be a non empty relational structure. One can verify that there exists a subset of L which is infs-closed, sups-closed, and non empty.

One can prove the following propositions:

(15) Let L be a non empty relational structure and S be a subset of L. Then S is meet-closed if and only if for all elements x, y of L such that $x \in S$ and $y \in S$ and inf $\{x, y\}$ exists in L holds $\inf\{x, y\} \in S$.

(16) Let L be a non empty relational structure and S be a subset of L. Then S is join-closed if and only if for all elements x, y of L such that $x \in S$ and $y \in S$ and sup $\{x, y\}$ exists in L holds $\sup\{x, y\} \in S$.

(17) Let L be an antisymmetric relational structure with g.l.b.'s and S be a subset of L. Then S is meet-closed if and only if for all elements x, y of L such that $x \in S$ and $y \in S$ holds $\inf\{x, y\} \in S$.

(18) Let L be an antisymmetric relational structure with l.u.b.'s and S be a subset of L. Then S is join-closed if and only if for all elements x, y of L such that $x \in S$ and $y \in S$ holds $\sup\{x, y\} \in S$.

(19) Let L be a non empty relational structure and S be a subset of L. Then S is infs-closed if and only if for every subset X of S such that inf X exists in L holds $\bigsqcap_L X \in S$.

(20) Let L be a non empty relational structure and S be a subset of L. Then S is sups-closed if and only if for every subset X of S such that sup X exists in L holds $\bigsqcup_L X \in S$.

(21) Let L be a non empty transitive relational structure, S be an infs-closed non empty subset of L, and X be a subset of S. If inf X exists in L, then inf X exists in $\operatorname{sub}(S)$ and $\bigsqcap_{\operatorname{sub}(S)} X = \bigsqcap_L X$.

(22) Let L be a non empty transitive relational structure, S be a sups-closed non empty subset of L, and X be a subset of S. If sup X exists in L, then sup X exists in $\operatorname{sub}(S)$ and $\bigsqcup_{\operatorname{sub}(S)} X = \bigsqcup_L X$.

(23) Let L be a non empty transitive relational structure, S be a meet-closed non empty subset of L, and x, y be elements of S. Suppose inf $\{x, y\}$ exists in L. Then inf $\{x, y\}$ exists in $\operatorname{sub}(S)$ and $\bigsqcap_{\operatorname{sub}(S)}\{x, y\} = \bigsqcap_L\{x, y\}$.

(24) Let L be a non empty transitive relational structure, S be a join-closed non empty subset of L, and x, y be elements of S. Suppose sup $\{x, y\}$ exists in L. Then sup $\{x, y\}$ exists in $\operatorname{sub}(S)$ and $\bigsqcup_{\operatorname{sub}(S)}\{x, y\} = \bigsqcup_L\{x, y\}$.

(25) Let L be an antisymmetric transitive relational structure with g.l.b.'s and S be a non empty meet-closed subset of L. Then $\mathrm{sub}(S)$ has g.l.b.'s.

(26) Let L be an antisymmetric transitive relational structure with l.u.b.'s and S be a non empty join-closed subset of L. Then $\mathrm{sub}(S)$ has l.u.b.'s.

Let L be an antisymmetric transitive relational structure with g.l.b.'s and let S be a non empty meet-closed subset of L. Observe that $\mathrm{sub}(S)$ has g.l.b.'s.

Let L be an antisymmetric transitive relational structure with l.u.b.'s and let S be a non empty join-closed subset of L. Observe that $\mathrm{sub}(S)$ has l.u.b.'s.

The following four propositions are true:

(27) Let L be a complete transitive antisymmetric non empty relational structure, S be an infs-closed non empty subset of L, and X be a subset of S. Then $\bigsqcap_{\mathrm{sub}(S)} X = \bigsqcap_L X$.

(28) Let L be a complete transitive antisymmetric non empty relational structure, S be a sups-closed non empty subset of L, and X be a subset of S. Then $\bigsqcup_{\mathrm{sub}(S)} X = \bigsqcup_L X$.

(29) For every semilattice L holds every meet-closed subset of L is filtered.

(30) For every sup-semilattice L holds every join-closed subset of L is directed.

Let L be a semilattice. Observe that every subset of L which is meet-closed is also filtered.

Let L be a sup-semilattice. One can check that every subset of L which is join-closed is also directed.

The following propositions are true:

(31) Let L be a semilattice and S be an upper non empty subset of L. Then S is a filter of L if and only if S is meet-closed.

(32) Let L be a sup-semilattice and S be a lower non empty subset of L. Then S is an ideal of L if and only if S is join-closed.

(33) For every non empty relational structure L and for all join-closed subsets S_1, S_2 of L holds $S_1 \cap S_2$ is join-closed.

(34) For every non empty relational structure L and for all meet-closed subsets S_1, S_2 of L holds $S_1 \cap S_2$ is meet-closed.

(35) For every sup-semilattice L and for every element x of the carrier of L holds $\downarrow x$ is join-closed.

(36) For every semilattice L and for every element x of the carrier of L holds $\downarrow x$ is meet-closed.

(37) For every sup-semilattice L and for every element x of the carrier of L holds $\uparrow x$ is join-closed.

(38) For every semilattice L and for every element x of the carrier of L holds $\uparrow x$ is meet-closed.

Let L be a sup-semilattice and let x be an element of L. Observe that $\downarrow x$ is join-closed and $\uparrow x$ is join-closed.

Let L be a semilattice and let x be an element of L. Note that $\downarrow x$ is meet-closed and $\uparrow x$ is meet-closed.

Next we state three propositions:

(39) For every sup-semilattice L and for every element x of L holds $\twoheaddownarrow x$ is join-closed.

(40) For every semilattice L and for every element x of L holds $\twoheaddownarrow x$ is meet-closed.

(41) For every sup-semilattice L and for every element x of L holds $\twoheaduparrow x$ is join-closed.

Let L be a sup-semilattice and let x be an element of L. Note that $\twoheaddownarrow x$ is join-closed and $\twoheaduparrow x$ is join-closed.

Let L be a semilattice and let x be an element of L. Observe that $\twoheaddownarrow x$ is meet-closed.

3. About Bases of Continuous Lattices

Let T be a topological structure. The functor weight T yields a cardinal number and is defined as follows:

(Def. 5) $\operatorname{weight} T = \bigcap\{\overline{\overline{B}} : B$ ranges over bases of $T\}$.

Let T be a topological structure. We say that T is second-countable if and only if:

(Def. 6) $\operatorname{weight} T \subseteq \omega$.

Let L be a continuous sup-semilattice. A subset of L is called a CLbasis of L if:

(Def. 7) It is join-closed and for every element x of L holds $x = \sup(\twoheaddownarrow x \cap \mathrm{it})$.

Let L be a non empty relational structure and let S be a subset of L. We say that S has bottom if and only if:

(Def. 8) $\perp_L \in S$.

Let L be a non empty relational structure and let S be a subset of L. We say that S has top if and only if:

(Def. 9) $\top_L \in S$.

Let L be a non empty relational structure. Note that every subset of L which has bottom is non empty.

Let L be a non empty relational structure. Observe that every subset of L which has top is non empty.

Let L be a non empty relational structure. Note that there exists a subset of L which has bottom and there exists a subset of L which has top.

Let L be a continuous sup-semilattice. One can verify that there exists a CLbasis of L which has bottom and there exists a CLbasis of L which has top.

One can prove the following proposition

(42) Let L be a lower-bounded antisymmetric non empty relational structure and S be a subset of L with bottom. Then $\mathrm{sub}(S)$ is lower-bounded.

Let L be a lower-bounded antisymmetric non empty relational structure and let S be a subset of L with bottom. One can verify that $\mathrm{sub}(S)$ is lower-bounded.

Let L be a continuous sup-semilattice. Observe that every CLbasis of L is join-closed.

One can check that there exists a continuous lattice which is bounded and non trivial.

Let L be a lower-bounded non trivial continuous sup-semilattice. One can verify that every CLbasis of L is non empty.

One can prove the following propositions:

(43) For every sup-semilattice L holds the carrier of $\mathrm{CompactSublatt}(L)$ is a join-closed subset of L.

(44) For every algebraic lower-bounded lattice L holds the carrier of $\mathrm{CompactSublatt}(L)$ is a CLbasis of L with bottom.

(45) Let L be a continuous lower-bounded sup-semilattice. If the carrier of $\mathrm{CompactSublatt}(L)$ is a CLbasis of L, then L is algebraic.

(46) Let L be a continuous lower-bounded lattice and B be a join-closed subset of L. Then B is a CLbasis of L if and only if for all elements x, y of L such that $y \nleqslant x$ there exists an element b of L such that $b \in B$ and $b \nleqslant x$ and $b \ll y$.

(47) Let L be a continuous lower-bounded lattice and B be a join-closed subset of L. Suppose $\perp_L \in B$. Then B is a CLbasis of L if and only if for all elements x, y of L such that $x \ll y$ there exists an element b of L such that $b \in B$ and $x \leqslant b$ and $b \ll y$.

(48) Let L be a continuous lower-bounded lattice and B be a join-closed subset of L. Suppose $\perp_L \in B$. Then B is a CLbasis of L if and only if the following conditions are satisfied:

(i) the carrier of $\mathrm{CompactSublatt}(L) \subseteq B$, and

(ii) for all elements x, y of L such that $y \nleqslant x$ there exists an element b of L such that $b \in B$ and $b \nleqslant x$ and $b \leqslant y$.

(49) Let L be a continuous lower-bounded lattice and B be a join-closed subset of L. Suppose $\perp_L \in B$. Then B is a CLbasis of L if and only if for all elements x, y of L such that $y \nleqslant x$ there exists an element b of L such that $b \in B$ and $b \nleqslant x$ and $b \leqslant y$.

(50) Let L be a lower-bounded sup-semilattice and S be a non empty full relational substructure of L. Suppose $\perp_L \in$ the carrier of S and the carrier

of S is a join-closed subset of L. Let x be an element of L. Then $\downarrow x \cap$ the carrier of S is an ideal of S.

Let L be a non empty reflexive transitive relational structure and let S be a non empty full relational substructure of L. The functor supMap S yielding a map from $\langle \mathrm{Ids}(S), \subseteq \rangle$ into L is defined by:

(Def. 10) For every ideal I of S holds $(\mathrm{supMap}\, S)(I) = \bigsqcup_L I$.

Let L be a non empty reflexive transitive relational structure and let S be a non empty full relational substructure of L. The functor idsMap S yields a map from $\langle \mathrm{Ids}(S), \subseteq \rangle$ into $\langle \mathrm{Ids}(L), \subseteq \rangle$ and is defined by:

(Def. 11) For every ideal I of S there exists a subset J of L such that $I = J$ and $(\mathrm{idsMap}\, S)(I) = \downarrow J$.

Let L be a non empty relational structure and let B be a non empty subset of the carrier of L. Observe that $\mathrm{sub}(B)$ is non empty.

Let L be a reflexive relational structure and let B be a subset of the carrier of L. Note that $\mathrm{sub}(B)$ is reflexive.

Let L be a transitive relational structure and let B be a subset of the carrier of L. Note that $\mathrm{sub}(B)$ is transitive.

Let L be an antisymmetric relational structure and let B be a subset of the carrier of L. Observe that $\mathrm{sub}(B)$ is antisymmetric.

Let L be a lower-bounded continuous sup-semilattice and let B be a CLbasis of L with bottom. The functor baseMap B yielding a map from L into $\langle \mathrm{Ids}(\mathrm{sub}(B)), \subseteq \rangle$ is defined as follows:

(Def. 12) For every element x of L holds $(\mathrm{baseMap}\, B)(x) = \downarrow x \cap B$.

We now state a number of propositions:

(51) Let L be a non empty reflexive transitive relational structure and S be a non empty full relational substructure of L. Then $\mathrm{dom}\, \mathrm{supMap}\, S = \mathrm{Ids}(S)$ and $\mathrm{rng}\, \mathrm{supMap}\, S$ is a subset of L.

(52) Let L be a non empty reflexive transitive relational structure, S be a non empty full relational substructure of L, and x be a set. Then $x \in \mathrm{dom}\, \mathrm{supMap}\, S$ if and only if x is an ideal of S.

(53) Let L be a non empty reflexive transitive relational structure and S be a non empty full relational substructure of L. Then $\mathrm{dom}\, \mathrm{idsMap}\, S = \mathrm{Ids}(S)$ and $\mathrm{rng}\, \mathrm{idsMap}\, S$ is a subset of $\mathrm{Ids}(L)$.

(54) Let L be a non empty reflexive transitive relational structure, S be a non empty full relational substructure of L, and x be a set. Then $x \in \mathrm{dom}\, \mathrm{idsMap}\, S$ if and only if x is an ideal of S.

(55) Let L be a non empty reflexive transitive relational structure, S be a non empty full relational substructure of L, and x be a set. If $x \in \mathrm{rng}\, \mathrm{idsMap}\, S$, then x is an ideal of L.

(56) Let L be a lower-bounded continuous sup-semilattice and B be a CLbasis of L with bottom. Then $\mathrm{dom}\,\mathrm{baseMap}\,B =$ the carrier of L and $\mathrm{rng}\,\mathrm{baseMap}\,B$ is a subset of $\mathrm{Ids}(\mathrm{sub}(B))$.

(57) Let L be a lower-bounded continuous sup-semilattice, B be a CLbasis of L with bottom, and x be a set. If $x \in \mathrm{rng}\,\mathrm{baseMap}\,B$, then x is an ideal of $\mathrm{sub}(B)$.

(58) For every up-complete non empty poset L and for every non empty full relational substructure S of L holds $\mathrm{supMap}\,S$ is monotone.

(59) Let L be a non empty reflexive transitive relational structure and S be a non empty full relational substructure of L. Then $\mathrm{idsMap}\,S$ is monotone.

(60) For every lower-bounded continuous sup-semilattice L and for every CLbasis B of L with bottom holds $\mathrm{baseMap}\,B$ is monotone.

Let L be an up-complete non empty poset and let S be a non empty full relational substructure of L. Observe that $\mathrm{supMap}\,S$ is monotone.

Let L be a non empty reflexive transitive relational structure and let S be a non empty full relational substructure of L. One can check that $\mathrm{idsMap}\,S$ is monotone.

Let L be a lower-bounded continuous sup-semilattice and let B be a CLbasis of L with bottom. One can check that $\mathrm{baseMap}\,B$ is monotone.

The following propositions are true:

(61) Let L be a lower-bounded continuous sup-semilattice and B be a CLbasis of L with bottom. Then $\mathrm{idsMap}\,\mathrm{sub}(B)$ is sups-preserving.

(62) For every up-complete non empty poset L and for every non empty full relational substructure S of L holds $\mathrm{supMap}\,S = \mathrm{SupMap}(L) \cdot \mathrm{idsMap}\,S$.

(63) For every lower-bounded continuous sup-semilattice L and for every CLbasis B of L with bottom holds $\langle \mathrm{supMap}\,\mathrm{sub}(B), \mathrm{baseMap}\,B \rangle$ is Galois.

(64) Let L be a lower-bounded continuous sup-semilattice and B be a CLbasis of L with bottom. Then $\mathrm{supMap}\,\mathrm{sub}(B)$ is upper adjoint and $\mathrm{baseMap}\,B$ is lower adjoint.

(65) Let L be a lower-bounded continuous sup-semilattice and B be a CLbasis of L with bottom. Then $\mathrm{rng}\,\mathrm{supMap}\,\mathrm{sub}(B) =$ the carrier of L.

(66) Let L be a lower-bounded continuous sup-semilattice and B be a CLbasis of L with bottom. Then $\mathrm{supMap}\,\mathrm{sub}(B)$ is infs-preserving and sups-preserving.

(67) Let L be a lower-bounded continuous sup-semilattice and B be a CLbasis of L with bottom. Then $\mathrm{baseMap}\,B$ is sups-preserving.

Let L be a lower-bounded continuous sup-semilattice and let B be a CLbasis of L with bottom. One can verify that $\mathrm{supMap}\,\mathrm{sub}(B)$ is infs-preserving and sups-preserving and $\mathrm{baseMap}\,B$ is sups-preserving.

One can prove the following propositions:

(69)[2] Let L be a lower-bounded continuous sup-semilattice and B be a CLbasis of L with bottom. Then the carrier of CompactSublatt($\langle \mathrm{Ids}(\mathrm{sub}(B)), \subseteq \rangle$) = $\{\downarrow b : b$ ranges over elements of sub$(B)\}$.

(70) Let L be a lower-bounded continuous sup-semilattice and B be a CLbasis of L with bottom. Then CompactSublatt($\langle \mathrm{Ids}(\mathrm{sub}(B)), \subseteq \rangle$) and sub($B$) are isomorphic.

(71) Let L be a continuous lower-bounded lattice and B be a CLbasis of L with bottom. Suppose that for every CLbasis B_1 of L with bottom holds $B \subseteq B_1$. Let J be an element of $\langle \mathrm{Ids}(\mathrm{sub}(B)), \subseteq \rangle$. Then $J = \twoheaddownarrow \bigsqcup_L J \cap B$.

(72) Let L be a continuous lower-bounded lattice. Then L is algebraic if and only if the following conditions are satisfied:

(i) the carrier of CompactSublatt(L) is a CLbasis of L with bottom, and

(ii) for every CLbasis B of L with bottom holds the carrier of CompactSublatt(L) $\subseteq B$.

(73) Let L be a continuous lower-bounded lattice. Then L is algebraic if and only if there exists a CLbasis B of L with bottom such that for every CLbasis B_1 of L with bottom holds $B \subseteq B_1$.

References

[1] Grzegorz Bancerek. Complete lattices. *Formalized Mathematics*, 2(**5**):719–725, 1991.
[2] Grzegorz Bancerek. Bounds in posets and relational substructures. *Formalized Mathematics*, 6(**1**):81–91, 1997.
[3] Grzegorz Bancerek. Directed sets, nets, ideals, filters, and maps. *Formalized Mathematics*, 6(**1**):93–107, 1997.
[4] Grzegorz Bancerek. The "way-below" relation. *Formalized Mathematics*, 6(**1**):169–176, 1997.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Galois connections. *Formalized Mathematics*, 6(**1**):131–143, 1997.
[7] G. Gierz, K.H. Hofmann, K. Keimel, J.D. Lawson, M. Mislove, and D.S. Scott. *A Compendium of Continuous Lattices*. Springer-Verlag, Berlin, Heidelberg, New York, 1980.
[8] Adam Grabowski. On the category of posets. *Formalized Mathematics*, 5(**4**):501–505, 1996.
[9] Adam Grabowski and Robert Milewski. Boolean posets, posets under inclusion and products of relational structures. *Formalized Mathematics*, 6(**1**):117–121, 1997.
[10] Robert Milewski. Algebraic lattices. *Formalized Mathematics*, 6(**2**):249–254, 1997.
[11] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[12] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[13] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[14] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[2] The proposition (68) has been removed.

[15] Mariusz Żynel and Czesław Byliński. Properties of relational structures, posets, lattices and maps. *Formalized Mathematics*, 6(**1**):123–130, 1997.

Received November 28, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

The Construction of SCM over Ring

Artur Korniłowicz
University of Białystok

MML Identifier: SCMRING1.

The terminology and notation used in this paper have been introduced in the following articles: [6], [11], [2], [3], [9], [4], [5], [7], [1], [10], and [8].

For simplicity, we follow the rules: i, k are natural numbers, I is an element of $\mathbb{Z}_8$, i_1 is an element of Instr-Loc$_{\rm SCM}$, d_1 is an element of Data-Loc$_{\rm SCM}$, and S is a non empty 1-sorted structure.

Let us observe that every non empty loop structure which is trivial is also Abelian, add-associative, right zeroed, and right complementable and every non empty double loop structure which is trivial is also right unital and right-distributive.

Let us note that every element of Data-Loc$_{\rm SCM}$ is natural.

One can check the following observations:

* Data-Loc$_{\rm SCM}$ is non trivial,
* Instr$_{\rm SCM}$ is non trivial, and
* Instr-Loc$_{\rm SCM}$ is non trivial.

Let S be a non empty 1-sorted structure. The functor Instr$_{\rm SCM}(S)$ yields a subset of $[\!:\mathbb{Z}_8, (\bigcup\{\text{the carrier of } S\} \cup \mathbb{N})^*:\!]$ and is defined by the condition (Def. 1).

(Def. 1) Instr$_{\rm SCM}(S) = \{\langle 0, \varepsilon\rangle\} \cup \{\langle I, \langle a, b\rangle\rangle; I$ ranges over elements of $\mathbb{Z}_8$, a ranges over elements of Data-Loc$_{\rm SCM}$, b ranges over elements of Data-Loc$_{\rm SCM}$: $I \in \{1,2,3,4\}\} \cup \{\langle 6, \langle i\rangle\rangle : i$ ranges over elements of Instr-Loc$_{\rm SCM}\} \cup \{\langle 7, \langle i, a\rangle\rangle : i$ ranges over elements of Instr-Loc$_{\rm SCM}$, a ranges over elements of Data-Loc$_{\rm SCM}\} \cup \{\langle 5, \langle a, r\rangle\rangle : a$ ranges over elements of Data-Loc$_{\rm SCM}$, r ranges over elements of the carrier of $S\}$.

Let S be a non empty 1-sorted structure. Note that Instr$_{\rm SCM}(S)$ is non trivial.

ISSN 1426–2630

Let S be a non empty 1-sorted structure. We say that S is good if and only if:

(Def. 2) The carrier of $S \neq \text{Instr-Loc}_{\text{SCM}}$ and the carrier of $S \neq \text{Instr}_{\text{SCM}}(S)$.

One can verify that every non empty 1-sorted structure which is trivial is also good.

Let us observe that there exists a 1-sorted structure which is strict, trivial, and non empty.

Let us observe that there exists a double loop structure which is strict, trivial, and non empty.

One can check that there exists a ring which is strict and trivial.

In the sequel G denotes a good non empty 1-sorted structure.

Let S be a non empty 1-sorted structure. The functor $\text{OK}_{\text{SCM}}(S)$ yielding a function from $\mathbb{N}$ into $\{\text{the carrier of } S\} \cup \{\text{Instr}_{\text{SCM}}(S), \text{Instr-Loc}_{\text{SCM}}\}$ is defined as follows:

(Def. 3) $(\text{OK}_{\text{SCM}}(S))(0) = \text{Instr-Loc}_{\text{SCM}}$ and for every natural number k holds $(\text{OK}_{\text{SCM}}(S))(2 \cdot k + 1) =$ the carrier of S and $(\text{OK}_{\text{SCM}}(S))(2 \cdot k + 2) = \text{Instr}_{\text{SCM}}(S)$.

Let S be a non empty 1-sorted structure. An **SCM**-state over S is an element of $\prod \text{OK}_{\text{SCM}}(S)$.

Next we state several propositions:

(1) $\text{Instr-Loc}_{\text{SCM}} \neq \text{Instr}_{\text{SCM}}(S)$.

(2) $(\text{OK}_{\text{SCM}}(G))(i) = \text{Instr-Loc}_{\text{SCM}}$ iff $i = 0$.

(3) $(\text{OK}_{\text{SCM}}(G))(i) =$ the carrier of G iff there exists k such that $i = 2 \cdot k + 1$.

(4) $(\text{OK}_{\text{SCM}}(G))(i) = \text{Instr}_{\text{SCM}}(G)$ iff there exists k such that $i = 2 \cdot k + 2$.

(5) $(\text{OK}_{\text{SCM}}(G))(d_1) =$ the carrier of G.

(6) $(\text{OK}_{\text{SCM}}(G))(i_1) = \text{Instr}_{\text{SCM}}(G)$.

(7) $\pi_0 \prod \text{OK}_{\text{SCM}}(S) = \text{Instr-Loc}_{\text{SCM}}$.

(8) $\pi_{d_1} \prod \text{OK}_{\text{SCM}}(G) =$ the carrier of G.

(9) $\pi_{i_1} \prod \text{OK}_{\text{SCM}}(G) = \text{Instr}_{\text{SCM}}(G)$.

Let S be a non empty 1-sorted structure and let s be an **SCM**-state over S. The functor $\mathbf{IC}_s$ yielding an element of $\text{Instr-Loc}_{\text{SCM}}$ is defined by:

(Def. 4) $\mathbf{IC}_s = s(0)$.

Let R be a good non empty 1-sorted structure, let s be an **SCM**-state over R, and let u be an element of $\text{Instr-Loc}_{\text{SCM}}$. The functor $\text{Chg}_{\text{SCM}}(s, u)$ yielding an **SCM**-state over R is defined by:

(Def. 5) $\text{Chg}_{\text{SCM}}(s, u) = s {+\cdot} (0 \,\dot{\longmapsto}\, u)$.

The following three propositions are true:

(10) For every **SCM**-state s over G and for every element u of $\text{Instr-Loc}_{\text{SCM}}$ holds $(\text{Chg}_{\text{SCM}}(s, u))(0) = u$.

(11) For every **SCM**-state s over G and for every element u of $\text{Instr-Loc}_{\text{SCM}}$ and for every element m_1 of $\text{Data-Loc}_{\text{SCM}}$ holds $(\text{Chg}_{\text{SCM}}(s,u))(m_1) = s(m_1)$.

(12) For every **SCM**-state s over G and for all elements u, v of $\text{Instr-Loc}_{\text{SCM}}$ holds $(\text{Chg}_{\text{SCM}}(s,u))(v) = s(v)$.

Let R be a good non empty 1-sorted structure, let s be an **SCM**-state over R, let t be an element of $\text{Data-Loc}_{\text{SCM}}$, and let u be an element of the carrier of R. The functor $\text{Chg}_{\text{SCM}}(s,t,u)$ yielding an **SCM**-state over R is defined as follows:

(Def. 6) $\text{Chg}_{\text{SCM}}(s,t,u) = s+\cdot(t \mapsto u)$.

One can prove the following propositions:

(13) Let s be an **SCM**-state over G, t be an element of $\text{Data-Loc}_{\text{SCM}}$, and u be an element of the carrier of G. Then $(\text{Chg}_{\text{SCM}}(s,t,u))(0) = s(0)$.

(14) Let s be an **SCM**-state over G, t be an element of $\text{Data-Loc}_{\text{SCM}}$, and u be an element of the carrier of G. Then $(\text{Chg}_{\text{SCM}}(s,t,u))(t) = u$.

(15) Let s be an **SCM**-state over G, t be an element of $\text{Data-Loc}_{\text{SCM}}$, u be an element of the carrier of G, and m_1 be an element of $\text{Data-Loc}_{\text{SCM}}$. If $m_1 \neq t$, then $(\text{Chg}_{\text{SCM}}(s,t,u))(m_1) = s(m_1)$.

(16) Let s be an **SCM**-state over G, t be an element of $\text{Data-Loc}_{\text{SCM}}$, u be an element of the carrier of G, and v be an element of $\text{Instr-Loc}_{\text{SCM}}$. Then $(\text{Chg}_{\text{SCM}}(s,t,u))(v) = s(v)$.

Let R be a good non empty 1-sorted structure, let s be an **SCM**-state over R, and let a be an element of $\text{Data-Loc}_{\text{SCM}}$. Then $s(a)$ is an element of R.

Let S be a non empty 1-sorted structure and let x be an element of $\text{Instr}_{\text{SCM}}(S)$. Let us assume that there exist elements m_1, m_2 of $\text{Data-Loc}_{\text{SCM}}$ and I such that $x = \langle I, \langle m_1, m_2 \rangle \rangle$. The functor $x\,\text{address}_1$ yielding an element of $\text{Data-Loc}_{\text{SCM}}$ is defined by:

(Def. 7) There exists a finite sequence f of elements of $\text{Data-Loc}_{\text{SCM}}$ such that $f = x_{\mathbf{2}}$ and $x\,\text{address}_1 = \pi_1 f$.

The functor $x\,\text{address}_2$ yields an element of $\text{Data-Loc}_{\text{SCM}}$ and is defined by:

(Def. 8) There exists a finite sequence f of elements of $\text{Data-Loc}_{\text{SCM}}$ such that $f = x_{\mathbf{2}}$ and $x\,\text{address}_2 = \pi_2 f$.

One can prove the following proposition

(17) For every element x of $\text{Instr}_{\text{SCM}}(S)$ and for all elements m_1, m_2 of $\text{Data-Loc}_{\text{SCM}}$ such that $x = \langle I, \langle m_1, m_2 \rangle \rangle$ holds $x\,\text{address}_1 = m_1$ and $x\,\text{address}_2 = m_2$.

Let R be a non empty 1-sorted structure and let x be an element of $\text{Instr}_{\text{SCM}}(R)$. Let us assume that there exist an element m_1 of $\text{Instr-Loc}_{\text{SCM}}$ and I such that $x = \langle I, \langle m_1 \rangle \rangle$. The functor $x\,\text{address}_{\text{j}}$ yielding an element of $\text{Instr-Loc}_{\text{SCM}}$ is defined as follows:

(Def. 9) There exists a finite sequence f of elements of $\text{Instr-Loc}_{\text{SCM}}$ such that $f = x_{\mathbf{2}}$ and $x\,\text{address}_{\text{j}} = \pi_1 f$.

Next we state the proposition

(18) For every element x of $\text{Instr}_{\text{SCM}}(S)$ and for every element m_1 of $\text{Instr-Loc}_{\text{SCM}}$ such that $x = \langle I, \langle m_1 \rangle \rangle$ holds $x\,\text{address}_{\text{j}} = m_1$.

Let S be a non empty 1-sorted structure and let x be an element of $\text{Instr}_{\text{SCM}}(S)$. Let us assume that there exist an element m_1 of $\text{Instr-Loc}_{\text{SCM}}$, an element m_2 of $\text{Data-Loc}_{\text{SCM}}$, and I such that $x = \langle I, \langle m_1, m_2 \rangle \rangle$. The functor $x\,\text{address}_{\text{j}}$ yields an element of $\text{Instr-Loc}_{\text{SCM}}$ and is defined as follows:

(Def. 10) There exists an element m_1 of $\text{Instr-Loc}_{\text{SCM}}$ and there exists an element m_2 of $\text{Data-Loc}_{\text{SCM}}$ such that $\langle m_1, m_2 \rangle = x_{\mathbf{2}}$ and $x\,\text{address}_{\text{j}} = \pi_1 \langle m_1, m_2 \rangle$.

The functor $x\,\text{address}_{\text{c}}$ yields an element of $\text{Data-Loc}_{\text{SCM}}$ and is defined as follows:

(Def. 11) There exists an element m_1 of $\text{Instr-Loc}_{\text{SCM}}$ and there exists an element m_2 of $\text{Data-Loc}_{\text{SCM}}$ such that $\langle m_1, m_2 \rangle = x_{\mathbf{2}}$ and $x\,\text{address}_{\text{c}} = \pi_2 \langle m_1, m_2 \rangle$.

We now state the proposition

(19) Let x be an element of $\text{Instr}_{\text{SCM}}(S)$, m_1 be an element of $\text{Instr-Loc}_{\text{SCM}}$, and m_2 be an element of $\text{Data-Loc}_{\text{SCM}}$. If $x = \langle I, \langle m_1, m_2 \rangle \rangle$, then $x\,\text{address}_{\text{j}} = m_1$ and $x\,\text{address}_{\text{c}} = m_2$.

Let S be a non empty 1-sorted structure, let d be an element of $\text{Data-Loc}_{\text{SCM}}$, and let s be an element of the carrier of S. Then $\langle d, s \rangle$ is a finite sequence of elements of $\text{Data-Loc}_{\text{SCM}} \cup$ the carrier of S.

Let S be a non empty 1-sorted structure and let x be an element of $\text{Instr}_{\text{SCM}}(S)$. Let us assume that there exist an element m_1 of $\text{Data-Loc}_{\text{SCM}}$, an element r of the carrier of S, and I such that $x = \langle I, \langle m_1, r \rangle \rangle$. The functor $x\,\text{const\_address}$ yields an element of $\text{Data-Loc}_{\text{SCM}}$ and is defined as follows:

(Def. 12) There exists a finite sequence f of elements of $\text{Data-Loc}_{\text{SCM}} \cup$ the carrier of S such that $f = x_{\mathbf{2}}$ and $x\,\text{const\_address} = \pi_1 f$.

The functor $x\,\text{const\_value}$ yields an element of the carrier of S and is defined by:

(Def. 13) There exists a finite sequence f of elements of $\text{Data-Loc}_{\text{SCM}} \cup$ the carrier of S such that $f = x_{\mathbf{2}}$ and $x\,\text{const\_value} = \pi_2 f$.

We now state the proposition

(20) Let x be an element of $\text{Instr}_{\text{SCM}}(S)$, m_1 be an element of $\text{Data-Loc}_{\text{SCM}}$, and r be an element of the carrier of S. If $x = \langle I, \langle m_1, r \rangle \rangle$, then $x\,\text{const\_address} = m_1$ and $x\,\text{const\_value} = r$.

Let R be a good ring, let x be an element of $\text{Instr}_{\text{SCM}}(R)$, and let s be an **SCM**-state over R. The functor $\text{Exec-Res}_{\text{SCM}}(x, s)$ yields an **SCM**-state over

R and is defined by:

(Def. 14) $\text{Exec-Res}_{\text{SCM}}(x,s) =$

$$\begin{cases} \text{Chg}_{\text{SCM}}(\text{Chg}_{\text{SCM}}(s, x\,\text{address}_1, s(x\,\text{address}_2)), \text{Next}(\mathbf{IC}_s)), \text{ if there} \\ \quad \text{exist elements } m_1, m_2 \text{ of Data-Loc}_{\text{SCM}} \text{ such that } x = \langle 1, \langle m_1, m_2 \rangle \rangle, \\ \text{Chg}_{\text{SCM}}(\text{Chg}_{\text{SCM}}(s, x\,\text{address}_1, s(x\,\text{address}_1) + s(x\,\text{address}_2)), \text{Next}(\mathbf{IC}_s)), \\ \quad \text{if there exist elements } m_1, m_2 \text{ of Data-Loc}_{\text{SCM}} \text{ such that } x = \langle 2, \langle m_1, m_2 \rangle \rangle, \\ \text{Chg}_{\text{SCM}}(\text{Chg}_{\text{SCM}}(s, x\,\text{address}_1, s(x\,\text{address}_1) - s(x\,\text{address}_2)), \text{Next}(\mathbf{IC}_s)), \\ \quad \text{if there exist elements } m_1, m_2 \text{ of Data-Loc}_{\text{SCM}} \text{ such that } x = \langle 3, \langle m_1, m_2 \rangle \rangle, \\ \text{Chg}_{\text{SCM}}(\text{Chg}_{\text{SCM}}(s, x\,\text{address}_1, s(x\,\text{address}_1) \cdot s(x\,\text{address}_2)), \text{Next}(\mathbf{IC}_s)), \\ \quad \text{if there exist elements } m_1, m_2 \text{ of Data-Loc}_{\text{SCM}} \text{ such that } x = \langle 4, \langle m_1, m_2 \rangle \rangle, \\ \text{Chg}_{\text{SCM}}(s, x\,\text{address}_{\text{j}}), \text{ if there exists an element } m_1 \text{ of Instr-Loc}_{\text{SCM}} \\ \quad \text{such that } x = \langle 6, \langle m_1 \rangle \rangle, \\ \text{Chg}_{\text{SCM}}(s, (s(x\,\text{address}_{\text{c}}) = 0_R \to x\,\text{address}_{\text{j}}, \text{Next}(\mathbf{IC}_s))), \text{ if there exists} \\ \quad \text{an element } m_1 \text{ of Instr-Loc}_{\text{SCM}} \text{ and there exists an element } m_2 \\ \quad \text{of Data-Loc}_{\text{SCM}} \text{ such that } x = \langle 7, \langle m_1, m_2 \rangle \rangle, \\ \text{Chg}_{\text{SCM}}(\text{Chg}_{\text{SCM}}(s, x\,\text{const\_address}, x\,\text{const\_value}), \text{Next}(\mathbf{IC}_s)), \text{ if there} \\ \quad \text{exists an element } m_1 \text{ of Data-Loc}_{\text{SCM}} \text{ and there exists an element } r \\ \quad \text{of the carrier of } R \text{ such that } x = \langle 5, \langle m_1, r \rangle \rangle, \\ s, \text{ otherwise.} \end{cases}$$

Let S be a non empty 1-sorted structure, let f be a function from $\text{Instr}_{\text{SCM}}(S)$ into $(\prod \text{OK}_{\text{SCM}}(S))^{\prod \text{OK}_{\text{SCM}}(S)}$, and let x be an element of $\text{Instr}_{\text{SCM}}(S)$. One can check that $f(x)$ is function-like and relation-like.

Let R be a good ring. The functor $\text{Exec}_{\text{SCM}}(R)$ yielding a function from $\text{Instr}_{\text{SCM}}(R)$ into $(\prod \text{OK}_{\text{SCM}}(R))^{\prod \text{OK}_{\text{SCM}}(R)}$ is defined as follows:

(Def. 15) For every element x of $\text{Instr}_{\text{SCM}}(R)$ and for every **SCM**-state y over R holds $(\text{Exec}_{\text{SCM}}(R))(x)(y) = \text{Exec-Res}_{\text{SCM}}(x, y)$.

References

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

[2] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

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

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

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

[6] Yatsuka Nakamura and Andrzej Trybulec. On a mathematical model of programs. *Formalized Mathematics*, 3(**2**):241–250, 1992.

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

[8] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[9] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

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

[11] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

Received November 29, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

The Basic Properties of SCM over Ring

Artur Korniłowicz
University of Białystok

MML Identifier: SCMRING2.

The articles [6], [7], [12], [1], [8], [2], [3], [10], [4], [11], [9], and [5] provide the terminology and notation for this paper.

1. SCM over Ring

In this paper I is an element of $\mathbb{Z}_8$, S is a non empty 1-sorted structure, t is an element of the carrier of S, and x is a set.

Let R be a good ring. The functor $\mathbf{SCM}(R)$ yields a strict AMI over {the carrier of R} and is defined by the conditions (Def. 1).

(Def. 1)(i) The objects of $\mathbf{SCM}(R) = \mathbb{N}$,
(ii) the instruction counter of $\mathbf{SCM}(R) = 0$,
(iii) the instruction locations of $\mathbf{SCM}(R) = \text{Instr-Loc}_{\text{SCM}}$,
(iv) the instruction codes of $\mathbf{SCM}(R) = \mathbb{Z}_8$,
(v) the instructions of $\mathbf{SCM}(R) = \text{Instr}_{\text{SCM}}(R)$,
(vi) the object kind of $\mathbf{SCM}(R) = \text{OK}_{\text{SCM}}(R)$, and
(vii) the execution of $\mathbf{SCM}(R) = \text{Exec}_{\text{SCM}}(R)$.

Let R be a good ring, let s be a state of $\mathbf{SCM}(R)$, and let a be an element of $\text{Data-Loc}_{\text{SCM}}$. Then $s(a)$ is an element of R.

Let R be a good ring. An object of $\mathbf{SCM}(R)$ is called a Data-Location of R if:

(Def. 2) It $\in$ (the objects of $\mathbf{SCM}(R)) \setminus (\text{Instr-Loc}_{\text{SCM}} \cup \{0\})$.

For simplicity, we use the following convention: R is a good ring, r is an element of the carrier of R, a, b, c, d_1, d_2 are Data-Location of R, and i_1 is an instruction-location of $\mathbf{SCM}(R)$.

Next we state the proposition

ISSN 1426–2630

(1) x is a Data-Location of R iff $x \in \text{Data-Loc}_{\text{SCM}}$.

Let R be a good ring, let s be a state of $\mathbf{SCM}(R)$, and let a be a Data-Location of R. Then $s(a)$ is an element of R.

We now state several propositions:

(2) $\langle 0, \varepsilon \rangle \in \text{Instr}_{\text{SCM}}(S)$.

(3) $\langle 0, \varepsilon \rangle$ is an instruction of $\mathbf{SCM}(R)$.

(4) If $x \in \{1, 2, 3, 4\}$, then $\langle x, \langle d_1, d_2 \rangle \rangle \in \text{Instr}_{\text{SCM}}(S)$.

(5) $\langle 5, \langle d_1, t \rangle \rangle \in \text{Instr}_{\text{SCM}}(S)$.

(6) $\langle 6, \langle i_1 \rangle \rangle \in \text{Instr}_{\text{SCM}}(S)$.

(7) $\langle 7, \langle i_1, d_1 \rangle \rangle \in \text{Instr}_{\text{SCM}}(S)$.

Let R be a good ring and let a, b be Data-Location of R. The functor $a{:=}b$ yielding an instruction of $\mathbf{SCM}(R)$ is defined by:

(Def. 3) $a{:=}b = \langle 1, \langle a, b \rangle \rangle$.

The functor $\text{AddTo}(a, b)$ yielding an instruction of $\mathbf{SCM}(R)$ is defined by:

(Def. 4) $\text{AddTo}(a, b) = \langle 2, \langle a, b \rangle \rangle$.

The functor $\text{SubFrom}(a, b)$ yielding an instruction of $\mathbf{SCM}(R)$ is defined by:

(Def. 5) $\text{SubFrom}(a, b) = \langle 3, \langle a, b \rangle \rangle$.

The functor $\text{MultBy}(a, b)$ yielding an instruction of $\mathbf{SCM}(R)$ is defined as follows:

(Def. 6) $\text{MultBy}(a, b) = \langle 4, \langle a, b \rangle \rangle$.

Let R be a good ring, let a be a Data-Location of R, and let r be an element of the carrier of R. The functor $a{:=}r$ yields an instruction of $\mathbf{SCM}(R)$ and is defined by:

(Def. 7) $a{:=}r = \langle 5, \langle a, r \rangle \rangle$.

Let R be a good ring and let l be an instruction-location of $\mathbf{SCM}(R)$. The functor goto l yielding an instruction of $\mathbf{SCM}(R)$ is defined by:

(Def. 8) goto $l = \langle 6, \langle l \rangle \rangle$.

Let R be a good ring, let l be an instruction-location of $\mathbf{SCM}(R)$, and let a be a Data-Location of R. The functor **if** $a = 0$ **goto** l yielding an instruction of $\mathbf{SCM}(R)$ is defined as follows:

(Def. 9) **if** $a = 0$ **goto** $l = \langle 7, \langle l, a \rangle \rangle$.

One can prove the following proposition

(8) Let I be a set. Then I is an instruction of $\mathbf{SCM}(R)$ if and only if one of the following conditions is satisfied:

(i) $I = \langle 0, \varepsilon \rangle$, or

(ii) there exist a, b such that $I = a{:=}b$, or

(iii) there exist a, b such that $I = \text{AddTo}(a, b)$, or

(iv) there exist a, b such that $I = \text{SubFrom}(a, b)$, or

(v) there exist a, b such that $I = \mathrm{MultBy}(a, b)$, or
(vi) there exists i_1 such that $I = \mathrm{goto}\ i_1$, or
(vii) there exist a, i_1 such that $I = \mathbf{if}\ a = 0\ \mathbf{goto}\ i_1$, or
(viii) there exist a, r such that $I = a{:=}r$.

In the sequel s denotes a state of $\mathbf{SCM}(R)$.

Let us consider R. Observe that $\mathbf{SCM}(R)$ is von Neumann.

The following two propositions are true:

(9) $\mathbf{IC}_{\mathbf{SCM}(R)} = 0$.

(10) For every **SCM**-state S over R such that $S = s$ holds $\mathbf{IC}_s = \mathbf{IC}_S$.

Let R be a good ring and let i_1 be an instruction-location of $\mathbf{SCM}(R)$. The functor $\mathrm{Next}(i_1)$ yields an instruction-location of $\mathbf{SCM}(R)$ and is defined by:

(Def. 10) There exists an element m_1 of $\mathrm{Instr\text{-}Loc}_{\mathrm{SCM}}$ such that $m_1 = i_1$ and $\mathrm{Next}(i_1) = \mathrm{Next}(m_1)$.

The following propositions are true:

(11) For every instruction-location i_1 of $\mathbf{SCM}(R)$ and for every element m_1 of $\mathrm{Instr\text{-}Loc}_{\mathrm{SCM}}$ such that $m_1 = i_1$ holds $\mathrm{Next}(m_1) = \mathrm{Next}(i_1)$.

(12) Let I be an instruction of $\mathbf{SCM}(R)$ and i be an element of $\mathrm{Instr}_{\mathrm{SCM}}(R)$. If $i = I$, then for every **SCM**-state S over R such that $S = s$ holds $\mathrm{Exec}(I, s) = \mathrm{Exec\text{-}Res}_{\mathrm{SCM}}(i, S)$.

2. Users Guide

Next we state several propositions:

(13) $(\mathrm{Exec}(a{:=}b, s))(\mathbf{IC}_{\mathbf{SCM}(R)}) = \mathrm{Next}(\mathbf{IC}_s)$ and $(\mathrm{Exec}(a{:=}b, s))(a) = s(b)$ and for every c such that $c \neq a$ holds $(\mathrm{Exec}(a{:=}b, s))(c) = s(c)$.

(14) $(\mathrm{Exec}(\mathrm{AddTo}(a, b), s))(\mathbf{IC}_{\mathbf{SCM}(R)}) = \mathrm{Next}(\mathbf{IC}_s)$ and $(\mathrm{Exec}(\mathrm{AddTo}(a, b), s))(a) = s(a) + s(b)$ and for every c such that $c \neq a$ holds $(\mathrm{Exec}(\mathrm{AddTo}(a, b), s))(c) = s(c)$.

(15) $(\mathrm{Exec}(\mathrm{SubFrom}(a, b), s))(\mathbf{IC}_{\mathbf{SCM}(R)}) = \mathrm{Next}(\mathbf{IC}_s)$ and $(\mathrm{Exec}(\mathrm{SubFrom}(a, b), s))(a) = s(a) - s(b)$ and for every c such that $c \neq a$ holds $(\mathrm{Exec}(\mathrm{SubFrom}(a, b), s))(c) = s(c)$.

(16) $(\mathrm{Exec}(\mathrm{MultBy}(a, b), s))(\mathbf{IC}_{\mathbf{SCM}(R)}) = \mathrm{Next}(\mathbf{IC}_s)$ and $(\mathrm{Exec}(\mathrm{MultBy}(a, b), s))(a) = s(a) \cdot s(b)$ and for every c such that $c \neq a$ holds $(\mathrm{Exec}(\mathrm{MultBy}(a, b), s))(c) = s(c)$.

(17) $(\mathrm{Exec}(\mathrm{goto}\ i_1, s))(\mathbf{IC}_{\mathbf{SCM}(R)}) = i_1$ and $(\mathrm{Exec}(\mathrm{goto}\ i_1, s))(c) = s(c)$.

(18) If $s(a) = 0_R$, then $(\mathrm{Exec}(\mathbf{if}\ a = 0\ \mathbf{goto}\ i_1, s))(\mathbf{IC}_{\mathbf{SCM}(R)}) = i_1$ and if $s(a) \neq 0_R$, then $(\mathrm{Exec}(\mathbf{if}\ a = 0\ \mathbf{goto}\ i_1, s))(\mathbf{IC}_{\mathbf{SCM}(R)}) = \mathrm{Next}(\mathbf{IC}_s)$ and $(\mathrm{Exec}(\mathbf{if}\ a = 0\ \mathbf{goto}\ i_1, s))(c) = s(c)$.

(19) $(\mathrm{Exec}(a{:=}r, s))(\mathbf{IC}_{\mathbf{SCM}(R)}) = \mathrm{Next}(\mathbf{IC}_s)$ and $(\mathrm{Exec}(a{:=}r, s))(a) = r$ and for every c such that $c \neq a$ holds $(\mathrm{Exec}(a{:=}r, s))(c) = s(c)$.

3. Halt Instruction

The following two propositions are true:

(20) For every instruction I of $\mathbf{SCM}(R)$ such that there exists s such that $(\mathrm{Exec}(I, s))(\mathbf{IC}_{\mathbf{SCM}(R)}) = \mathrm{Next}(\mathbf{IC}_s)$ holds I is non halting.

(21) For every instruction I of $\mathbf{SCM}(R)$ such that $I = \langle 0, \varepsilon \rangle$ holds I is halting.

Let us consider R, a, b. One can check the following observations:

* $a{:=}b$ is non halting,
* $\mathrm{AddTo}(a, b)$ is non halting,
* $\mathrm{SubFrom}(a, b)$ is non halting, and
* $\mathrm{MultBy}(a, b)$ is non halting.

Let us consider R, i_1. Observe that goto i_1 is non halting.

Let us consider R, a, i_1. Observe that **if** $a = 0$ **goto** i_1 is non halting.

Let us consider R, a, r. Note that $a{:=}r$ is non halting.

Let us consider R. One can check that $\mathbf{SCM}(R)$ is halting definite data-oriented steady-programmed and realistic.

One can prove the following propositions:

(29)[1] For every instruction I of $\mathbf{SCM}(R)$ such that I is halting holds $I = \mathbf{halt}_{\mathbf{SCM}(R)}$.

(30) $\mathbf{halt}_{\mathbf{SCM}(R)} = \langle 0, \varepsilon \rangle$.

References

[1] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.
[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[4] Artur Korniłowicz. The construction of **SCM** over ring. *Formalized Mathematics*, 7(**2**):295–300, 1998.
[5] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[6] Yatsuka Nakamura and Andrzej Trybulec. A mathematical model of CPU. *Formalized Mathematics*, 3(**2**):151–160, 1992.
[7] Yatsuka Nakamura and Andrzej Trybulec. On a mathematical model of programs. *Formalized Mathematics*, 3(**2**):241–250, 1992.
[8] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

[1]The propositions (22)–(28) have been removed.

[9] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[10] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[11] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[12] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

Received November 29, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

A Theory of Boolean Valued Functions and Quantifiers with Respect to Partitions

Shunichi Kobayashi
Shinshu University
Nagano

Yatsuka Nakamura
Shinshu University
Nagano

Summary. In this paper, we define the coordinate of partitions. We also introduce the universal quantifier and the existential quantifier of Boolean valued functions with respect to partitions. Some predicate calculus formulae containing such quantifiers are proved. Such a theory gives a discussion of semantics to usual predicate logic.

MML Identifier: BVFUNC_2.

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

1. Preliminaries

In this paper Y denotes a non empty set and G denotes a subset of PARTITIONS(Y).

Let X be a set. Then PARTITIONS(X) is a partition family of X.

Let X be a set and let F be a non empty partition family of X. We see that the element of F is a partition of X.

The following proposition is true

(1) Let y be an element of Y. Then there exists a subset X of Y such that

(i) $y \in X$, and

(ii) there exists a function h and there exists a family F of subsets of Y such that $\operatorname{dom} h = G$ and $\operatorname{rng} h = F$ and for every set d such that $d \in G$ holds $h(d) \in d$ and $X = \text{Intersect}(F)$ and $X \neq \emptyset$.

ISSN 1426–2630

Let us consider Y and let G be a subset of PARTITIONS(Y). The functor $\bigwedge G$ yielding a partition of Y is defined by the condition (Def. 1).

(Def. 1) Let x be a set. Then $x \in \bigwedge G$ if and only if there exists a function h and there exists a family F of subsets of Y such that $\operatorname{dom} h = G$ and $\operatorname{rng} h = F$ and for every set d such that $d \in G$ holds $h(d) \in d$ and $x = \operatorname{Intersect}(F)$ and $x \neq \emptyset$.

Let us consider Y, let G be a subset of PARTITIONS(Y), and let b be a set. We say that b is upper min depend of G if and only if the conditions (Def. 2) are satisfied.

(Def. 2)(i) For every partition d of Y such that $d \in G$ holds b is a dependent set of d, and

(ii) for every set e such that $e \subseteq b$ and for every partition d of Y such that $d \in G$ holds e is a dependent set of d holds $e = b$.

One can prove the following proposition

(2) For every element y of Y such that $G \neq \emptyset$ there exists a subset X of Y such that $y \in X$ and X is upper min depend of G.

Let us consider Y and let G be a subset of PARTITIONS(Y). The functor $\bigvee G$ yielding a partition of Y is defined by:

(Def. 3)(i) For every set x holds $x \in \bigvee G$ iff x is upper min depend of G if $G \neq \emptyset$,

(ii) $\bigvee G = \mathcal{I}(Y)$, otherwise.

The following propositions are true:

(3) For every subset G of PARTITIONS(Y) and for every partition P_1 of Y such that $P_1 \in G$ holds $P_1 \Supset \bigwedge G$.

(4) For every subset G of PARTITIONS(Y) and for every partition P_1 of Y such that $P_1 \in G$ holds $P_1 \Subset \bigvee G$.

2. Coordinate and Quantifiers

Let us consider Y and let G be a subset of PARTITIONS(Y). We say that G is a generating family of partitions if and only if:

(Def. 4) $\bigwedge G = \mathcal{I}(Y)$.

Let us consider Y and let G be a subset of PARTITIONS(Y). We say that G is an independent family of partitions if and only if the condition (Def. 5) is satisfied.

(Def. 5) Let h be a function and F be a family of subsets of Y. Suppose $\operatorname{dom} h = G$ and $\operatorname{rng} h = F$ and for every set d such that $d \in G$ holds $h(d) \in d$. Then $\operatorname{Intersect}(F) \neq \emptyset$.

Let us consider Y and let G be a subset of PARTITIONS(Y). We say that G is a coordinate if and only if the conditions (Def. 6) are satisfied.

(Def. 6)(i) G is an independent family of partitions ,

(ii) G is a generating family of partitions, and

(iii) for all partitions d_1, d_2 of Y such that $d_1 \in G$ and $d_2 \in G$ and $d_1 \neq d_2$ holds $d_1 \vee d_2 = \mathcal{O}(Y)$.

Let us consider Y and let P_1 be a partition of Y. Then $\{P_1\}$ is a subset of PARTITIONS(Y).

Let us consider Y, let P_1 be a partition of Y, and let G be a subset of PARTITIONS(Y). The functor CompF(P_1, G) yielding a partition of Y is defined by:

(Def. 7) $\mathrm{CompF}(P_1, G) = \bigwedge G \setminus \{P_1\}$.

Let us consider Y, let a be an element of BVF(Y), let G be a subset of PARTITIONS(Y), and let P_1 be a partition of Y. We say that a is independent of P_1, G if and only if:

(Def. 8) a is dependent of CompF(P_1, G).

Let us consider Y, let a be an element of BVF(Y), let G be a subset of PARTITIONS(Y), and let P_1 be a partition of Y. The functor $\forall_{a,P_1} G$ yielding an element of BVF(Y) is defined by:

(Def. 9) $\forall_{a,P_1} G = \mathrm{INF}(a, \mathrm{CompF}(P_1, G))$.

Let us consider Y, let a be an element of BVF(Y), let G be a subset of PARTITIONS(Y), and let P_1 be a partition of Y. The functor $\exists_{a,P_1} G$ yielding an element of BVF(Y) is defined as follows:

(Def. 10) $\exists_{a,P_1} G = \mathrm{SUP}(a, \mathrm{CompF}(P_1, G))$.

One can prove the following propositions:

(5) Let a be an element of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\forall_{a,P_1} G$ is dependent of CompF(P_1, G).

(6) Let a be an element of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\exists_{a,P_1} G$ is dependent of CompF(P_1, G).

(7) Let a be an element of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\forall_{true(Y),P_1} G = true(Y)$.

(8) Let a be an element of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\exists_{true(Y),P_1} G = true(Y)$.

(9) Let a be an element of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\forall_{false(Y),P_1} G = false(Y)$.

(10) Let a be an element of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\exists_{false(Y),P_1} G =$

false(Y).

(11) Let a be an element of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\forall_{a,P_1}G \Subset a$.

(12) Let a be an element of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $a \Subset \exists_{a,P_1}G$.

(13) Let a, b be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\forall_{a \wedge b,P_1}G = \forall_{a,P_1}G \wedge \forall_{b,P_1}G$.

(14) Let a, b be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\forall_{a,P_1}G \vee \forall_{b,P_1}G \Subset \forall_{a \vee b,P_1}G$.

(15) Let a, b be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\forall_{a \Rightarrow b,P_1}G \Subset \forall_{a,P_1}G \Rightarrow \forall_{b,P_1}G$.

(16) Let a, b be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\exists_{a \vee b,P_1}G = \exists_{a,P_1}G \vee \exists_{b,P_1}G$.

(17) Let a, b be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\exists_{a \wedge b,P_1}G \Subset \exists_{a,P_1}G \wedge \exists_{b,P_1}G$.

(18) Let a, b be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\exists_{a,P_1}G \oplus \exists_{b,P_1}G \Subset \exists_{a \oplus b,P_1}G$.

(19) Let a, b be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\exists_{a,P_1}G \Rightarrow \exists_{b,P_1}G \Subset \exists_{a \Rightarrow b,P_1}G$.

(20) Let a be an element of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\neg\forall_{a,P_1}G = \exists_{\neg a,P_1}G$.

(21) Let a be an element of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. If G is a coordinate and $P_1 \in G$, then $\neg\exists_{a,P_1}G = \forall_{\neg a,P_1}G$.

(22) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\forall_{u \Rightarrow a,P_1}G = u \Rightarrow \forall_{a,P_1}G$.

(23) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\forall_{a \Rightarrow u,P_1}G = \exists_{a,P_1}G \Rightarrow u$.

(24) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u

is independent of P_1, G. Then $\forall_{u \vee a, P_1} G = u \vee \forall_{a,P_1} G$.

(25) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\forall_{a \vee u, P_1} G = \forall_{a,P_1} G \vee u$.

(26) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\forall_{a \vee u, P_1} G \Subset \exists_{a,P_1} G \vee u$.

(27) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\forall_{u \wedge a, P_1} G = u \wedge \forall_{a,P_1} G$.

(28) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\forall_{a \wedge u, P_1} G = \forall_{a,P_1} G \wedge u$.

(29) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\forall_{a \wedge u, P_1} G \Subset \exists_{a,P_1} G \wedge u$.

(30) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\forall_{u \oplus a, P_1} G \Subset u \oplus \forall_{a,P_1} G$.

(31) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\forall_{a \oplus u, P_1} G \Subset \forall_{a,P_1} G \oplus u$.

(32) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\forall_{u \Leftrightarrow a, P_1} G \Subset u \Leftrightarrow \forall_{a,P_1} G$.

(33) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\forall_{a \Leftrightarrow u, P_1} G \Subset \forall_{a,P_1} G \Leftrightarrow u$.

(34) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\exists_{u \vee a, P_1} G = u \vee \exists_{a,P_1} G$.

(35) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\exists_{a \vee u, P_1} G = \exists_{a,P_1} G \vee u$.

(36) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\exists_{u \wedge a, P_1} G = u \wedge \exists_{a,P_1} G$.

(37) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\exists_{a \wedge u, P_1} G = \exists_{a,P_1} G \wedge u$.

(38) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $u \Rightarrow \exists_{a,P_1} G \Subset \exists_{u \Rightarrow a,P_1} G$.

(39) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\exists_{a,P_1} G \Rightarrow u \Subset \exists_{a \Rightarrow u,P_1} G$.

(40) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $u \oplus \exists_{a,P_1} G \Subset \exists_{u \oplus a,P_1} G$.

(41) Let a, u be elements of BVF(Y), G be a subset of PARTITIONS(Y), and P_1 be a partition of Y. Suppose G is a coordinate and $P_1 \in G$ and u is independent of P_1, G. Then $\exists_{a,P_1} G \oplus u \Subset \exists_{a \oplus u,P_1} G$.

References

[1] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[2] Shunichi Kobayashi and Kui Jia. A theory of Boolean valued functions and partitions. *Formalized Mathematics*, 7(**2**):249–254, 1998.
[3] Shunichi Kobayashi and Kui Jia. A theory of partitions. Part I. *Formalized Mathematics*, 7(**2**):243–247, 1998.
[4] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[5] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.
[6] Alexander Yu. Shibakov and Andrzej Trybulec. The Cantor set. *Formalized Mathematics*, 5(**2**):233–236, 1996.
[7] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[8] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[9] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received December 21, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Predicate Calculus for Boolean Valued Functions. Part I

Shunichi Kobayashi
Shinshu University
Nagano

Yatsuka Nakamura
Shinshu University
Nagano

Summary. In this paper, we have proved some elementary predicate calculus formulae containing the quantifiers of Boolean valued functions with respect to partitions. Such a theory is an analogy of usual predicate logic.

MML Identifier: BVFUNC_3.

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

For simplicity, we adopt the following convention: Y denotes a non empty set, G denotes a subset of PARTITIONS(Y), a, b, c, u denote elements of BVF(Y), and P_1 denotes a partition of Y.

The following propositions are true:

(1) $a \Rightarrow b \Subset \forall_{a,P_1} G \Rightarrow \exists_{b,P_1} G$.

(2) $\forall_{a,P_1} G \wedge \forall_{b,P_1} G \Subset a \wedge b$.

(3) $a \wedge b \Subset \exists_{a,P_1} G \wedge \exists_{b,P_1} G$.

(4) $\neg(\forall_{a,P_1} G \wedge \forall_{b,P_1} G) = \exists_{\neg a,P_1} G \vee \exists_{\neg b,P_1} G$.

(5) $\neg(\exists_{a,P_1} G \wedge \exists_{b,P_1} G) = \forall_{\neg a,P_1} G \vee \forall_{\neg b,P_1} G$.

(6) $\forall_{a,P_1} G \vee \forall_{b,P_1} G \Subset a \vee b$.

(7) $a \vee b \Subset \exists_{a,P_1} G \vee \exists_{b,P_1} G$.

(8) $a \oplus b \Subset \neg(\exists_{\neg a,P_1} G \oplus \exists_{b,P_1} G) \vee \neg(\exists_{a,P_1} G \oplus \exists_{\neg b,P_1} G)$.

(9) $\forall_{a \vee b,P_1} G \Subset \forall_{a,P_1} G \vee \exists_{b,P_1} G$.

(10) $\forall_{a \vee b,P_1} G \Subset \exists_{a,P_1} G \vee \forall_{b,P_1} G$.

(11) $\forall_{a \vee b,P_1} G \Subset \exists_{a,P_1} G \vee \exists_{b,P_1} G$.

(12) $\exists_{a,P_1} G \wedge \forall_{b,P_1} G \Subset \exists_{a \wedge b,P_1} G$.

ISSN 1426–2630

(13) $\forall_{a,P_1}G \wedge \exists_{b,P_1}G \Subset \exists_{a\wedge b,P_1}G$.

(14) $\forall_{a\Rightarrow b,P_1}G \Subset \forall_{a,P_1}G \Rightarrow \exists_{b,P_1}G$.

(15) $\forall_{a\Rightarrow b,P_1}G \Subset \exists_{a,P_1}G \Rightarrow \exists_{b,P_1}G$.

(16) $\exists_{a,P_1}G \Rightarrow \forall_{b,P_1}G \Subset \forall_{a\Rightarrow b,P_1}G$.

(17) $a \Rightarrow b \Subset a \Rightarrow \exists_{b,P_1}G$.

(18) $a \Rightarrow b \Subset \forall_{a,P_1}G \Rightarrow b$.

(19) $\exists_{a\Rightarrow b,P_1}G \Subset \forall_{a,P_1}G \Rightarrow \exists_{b,P_1}G$.

(20) $\forall_{a,P_1}G \Subset \exists_{b,P_1}G \Rightarrow \exists_{a\wedge b,P_1}G$.

(21) If u is independent of P_1, G, then $\exists_{u\Rightarrow a,P_1}G \Subset u \Rightarrow \exists_{a,P_1}G$.

(22) If u is independent of P_1, G, then $\exists_{a\Rightarrow u,P_1}G \Subset \forall_{a,P_1}G \Rightarrow u$.

(23) $\forall_{a,P_1}G \Rightarrow \exists_{b,P_1}G = \exists_{a\Rightarrow b,P_1}G$.

(24) $\forall_{a,P_1}G \Rightarrow \forall_{b,P_1}G \Subset \forall_{a,P_1}G \Rightarrow \exists_{b,P_1}G$.

(25) $\exists_{a,P_1}G \Rightarrow \exists_{b,P_1}G \Subset \forall_{a,P_1}G \Rightarrow \exists_{b,P_1}G$.

(26) $\forall_{a\Rightarrow b,P_1}G = \forall_{\neg a\vee b,P_1}G$.

(27) If G is a coordinate and $P_1 \in G$, then $\forall_{a\Rightarrow b,P_1}G = \neg\exists_{a\wedge\neg b,P_1}G$.

(28) $\exists_{a,P_1}G \Subset \neg(\forall_{a\Rightarrow b,P_1}G \wedge \forall_{a\Rightarrow\neg b,P_1}G)$.

(29) $\exists_{a,P_1}G \Subset \neg(\neg\exists_{a\wedge b,P_1}G \wedge \neg\exists_{a\wedge\neg b,P_1}G)$.

(30) $\exists_{a,P_1}G \wedge \forall_{a\Rightarrow b,P_1}G \Subset \exists_{a\wedge b,P_1}G$.

(31) $\exists_{a,P_1}G \wedge \neg\exists_{a\wedge b,P_1}G \Subset \neg\forall_{a\Rightarrow b,P_1}G$.

(32) $\forall_{a\Rightarrow c,P_1}G \wedge \forall_{c\Rightarrow b,P_1}G \Subset \forall_{a\Rightarrow b,P_1}G$.

(33) $\forall_{c\Rightarrow b,P_1}G \wedge \exists_{a\wedge c,P_1}G \Subset \exists_{a\wedge b,P_1}G$.

(34) $\forall_{b\Rightarrow\neg c,P_1}G \wedge \forall_{a\Rightarrow c,P_1}G \Subset \forall_{a\Rightarrow\neg b,P_1}G$.

(35) $\forall_{b\Rightarrow c,P_1}G \wedge \forall_{a\Rightarrow\neg c,P_1}G \Subset \forall_{a\Rightarrow\neg b,P_1}G$.

(36) $\forall_{b\Rightarrow\neg c,P_1}G \wedge \exists_{a\wedge c,P_1}G \Subset \exists_{a\wedge\neg b,P_1}G$.

(37) $\forall_{b\Rightarrow c,P_1}G \wedge \exists_{a\wedge\neg c,P_1}G \Subset \exists_{a\wedge\neg b,P_1}G$.

(38) $\exists_{c,P_1}G \wedge \forall_{c\Rightarrow b,P_1}G \wedge \forall_{c\Rightarrow a,P_1}G \Subset \exists_{a\wedge b,P_1}G$.

(39) $\forall_{b\Rightarrow c,P_1}G \wedge \forall_{c\Rightarrow\neg a,P_1}G \Subset \forall_{a\Rightarrow\neg b,P_1}G$.

(40) $\exists_{b,P_1}G \wedge \forall_{b\Rightarrow c,P_1}G \wedge \forall_{c\Rightarrow a,P_1}G \Subset \exists_{a\wedge b,P_1}G$.

(41) $\exists_{c,P_1}G \wedge \forall_{b\Rightarrow\neg c,P_1}G \wedge \forall_{c\Rightarrow a,P_1}G \Subset \exists_{a\wedge\neg b,P_1}G$.

References

[1] Shunichi Kobayashi and Kui Jia. A theory of Boolean valued functions and partitions. *Formalized Mathematics*, 7(**2**):249–254, 1998.

[2] Shunichi Kobayashi and Yatsuka Nakamura. A theory of Boolean valued functions and quantifiers with respect to partitions. *Formalized Mathematics*, 7(**2**):307–312, 1998.

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

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

Received December 21, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Public-Key Cryptography and Pepin's Test for the Primality of Fermat Numbers

Yoshinori Fujisawa
Shinshu University
Nagano

Yasushi Fuwa
Shinshu University
Nagano

Hidetaka Shimizu
Information Technology Research Institute
of Nagano Prefecture

Summary. In this article, we have proved the correctness of the Public-Key Cryptography and the Pepin's Test for the Primality of Fermat Numbers ($F(n) = 2^{2^n} + 1$). It is a very important result in the IDEA Cryptography that F(4) is a prime number. At first, we prepared some useful theorems. Then, we proved the correctness of the Public-Key Cryptography. Next, we defined the Order's function and proved some properties. This function is very important in the proof of the Pepin's Test. Next, we proved some theorems about the Fermat Number. And finally, we proved the Pepin's Test using some properties of the Order's Function. And using the obtained result we have proved that F(1), F(2), F(3) and F(4) are prime number.

MML Identifier: `PEPIN`.

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

1. Some Useful Theorems

We adopt the following convention: d, i, j, k, m, n, p, q, k_1, k_2 are natural numbers and a, b, c, i_1, i_2, i_3, i_4, i_5 are integers.

One can prove the following four propositions:

ISSN 1426–2630

(1) For every i holds i and $i+1$ are relative prime.

(2) For every p such that p is prime holds m and p are relative prime or $\gcd(m,p)=p$.

(3) If $k \mid n \cdot m$ and n and k are relative prime, then $k \mid m$.

(4) If $n \mid m$ and $k \mid m$ and n and k are relative prime, then $n \cdot k \mid m$.

Let n be a natural number. Then $n^{\mathbf{2}}$ is a natural number.

We now state a number of propositions:

(5) If $c > 1$, then $1 \bmod c = 1$.

(6) For every i such that $i \neq 0$ holds $i \mid n$ iff $n \bmod i = 0$.

(7) If $m \neq 0$ and $m \mid n \bmod m$, then $m \mid n$.

(8) If $0 < n$ and $m \bmod n = k$, then $n \mid m - k$.

(9) If $i \cdot p \neq 0$ and p is prime and $k \bmod i \cdot p < p$, then $k \bmod i \cdot p = k \bmod p$.

(10) If $p \neq 0$, then $(a \cdot p + 1) \bmod p = 1 \bmod p$.

(11) If $1 < m$ and $n \cdot k \bmod m = k \bmod m$ and k and m are relative prime, then $n \bmod m = 1$.

(12) If $m \neq 0$, then $(p_{\mathbb{N}}^{k}) \bmod m = ((p \bmod m)_{\mathbb{N}}^{k}) \bmod m$.

(13) If $i \neq 0$, then $i^{\mathbf{2}} \bmod (i+1) = 1$.

(14) If $j \neq 0$ and $k^{\mathbf{2}} < j$ and $i \bmod j = k$, then $i^{\mathbf{2}} \bmod j = k^{\mathbf{2}}$.

(15) If p is prime and $i \bmod p = -1$, then $i^{\mathbf{2}} \bmod p = 1$.

(16) If n is even, then $n+1$ is odd.

(17) If $p > 2$ and p is prime, then p is odd.

(18) If $n > 0$, then the n-th power of 2 is even.

(19) If i is odd and j is odd, then $i \cdot j$ is odd.

(20) For every k such that i is odd holds $i_{\mathbb{N}}^{k}$ is odd.

(21) If $k > 0$ and i is even, then $i_{\mathbb{N}}^{k}$ is even.

(22) $2 \mid n$ iff n is even.

(23) If $m \cdot n$ is even, then m is even or n is even.

(24) $n_{\mathbb{N}}^{2} = n^{\mathbf{2}}$.

(25) $2_{\mathbb{N}}^{k} =$ the k-th power of 2.

(26) If $m > 1$ and $n > 0$, then $m_{\mathbb{N}}^{n} > 1$.

(27) If $n \neq 0$ and $p \neq 0$, then $n_{\mathbb{N}}^{p} = n \cdot n_{\mathbb{N}}^{p -' 1}$.

(28) For all n, m such that $m \bmod 2 = 0$ holds $(n_{\mathbb{N}}^{m \div 2})^{\mathbf{2}} = n_{\mathbb{N}}^{m}$.

(29) If $n \neq 0$ and $1 \leqslant k$, then $(n_{\mathbb{N}}^{k}) \div n = n_{\mathbb{N}}^{k -' 1}$.

(30) $2_{\mathbb{N}}^{n+1} = (2_{\mathbb{N}}^{n}) + 2_{\mathbb{N}}^{n}$.

(31) If $k > 1$ and $k_{\mathbb{N}}^{n} = k_{\mathbb{N}}^{m}$, then $n = m$.

(32) $m \leqslant n$ iff $2_{\mathbb{N}}^{m} \mid 2_{\mathbb{N}}^{n}$.

(33) If p is prime and $i \mid p_{\mathbb{N}}^{n}$, then $i = 1$ or there exists a natural number k such that $i = p \cdot k$.

(34) For every n such that $n \neq 0$ and p is prime and $n < p_{\mathbb{N}}^{k+1}$ holds $n \mid p_{\mathbb{N}}^{k+1}$ iff $n \mid p_{\mathbb{N}}^{k}$.

(35) For every k such that p is prime and $d \mid p_{\mathbb{N}}^{k}$ and $d \neq 0$ there exists a natural number t such that $d = p_{\mathbb{N}}^{t}$ and $t \leqslant k$.

(36) If $p > 1$ and $i \bmod p = 1$, then $(i_{\mathbb{N}}^{n}) \bmod p = 1$.

(37) If $m > 0$ and $n > 0$, then $(n_{\mathbb{N}}^{m}) \bmod n = 0$.

(38) If p is prime and n and p are relative prime, then $(n_{\mathbb{N}}^{p-'1}) \bmod p = 1$.

(39) If p is prime and $d > 1$ and $d \mid p_{\mathbb{N}}^{k}$ and $d \nmid (p_{\mathbb{N}}^{k}) \div p$, then $d = p_{\mathbb{N}}^{k}$.

Let a be an integer. Then $a^{\mathbf{2}}$ is a natural number.

We now state several propositions:

(40) For every n such that $n > 1$ holds $m \bmod n = 1$ iff $m \equiv 1 (\bmod n)$.

(41) If $a \equiv b (\bmod c)$, then $a^{\mathbf{2}} \equiv b^{\mathbf{2}} (\bmod c)$.

(42) If $i_5 = i_3 \cdot i_4$ and $i_1 \equiv i_2 (\bmod i_5)$, then $i_1 \equiv i_2 (\bmod i_3)$ and $i_1 \equiv i_2 (\bmod i_4)$.

(43) If $i_1 \equiv i_2 (\bmod i_5)$ and $i_1 \equiv i_3 (\bmod i_5)$, then $i_2 \equiv i_3 (\bmod i_5)$.

(44) 3 is prime.

(45) If $n \neq 0$, then $\mathrm{Euler}\, n \neq 0$.

(46) If $n \neq 0$, then $-n < n$.

(47) For all m, n such that $n > 0$ and $n > m$ holds $m \div n = 0$.

(48) If $n \neq 0$, then $n \div n = 1$.

2. Public-Key Cryptography

Let us consider k, m, n. The functor $\mathrm{Crypto}(m, n, k)$ yielding a natural number is defined as follows:

(Def. 1) $\mathrm{Crypto}(m, n, k) = (m_{\mathbb{N}}^{k}) \bmod n$.

One can prove the following proposition

(49) Suppose p is prime and q is prime and $p \neq q$ and $n = p \cdot q$ and k_1 and $\mathrm{Euler}\, n$ are relative prime and $k_1 \cdot k_2 \bmod \mathrm{Euler}\, n = 1$. Let m be a natural number. If $m < n$, then $\mathrm{Crypto}(\mathrm{Crypto}(m, n, k_1), n, k_2) = m$.

3. Order's Function

Let us consider i, p. Let us assume that $p > 1$ and i and p are relative prime. The functor $\mathrm{order}(i,p)$ yields a natural number and is defined as follows:

(Def. 2) $\mathrm{order}(i,p) > 0$ and $(i_{\mathbb{N}}^{\mathrm{order}(i,p)}) \bmod p = 1$ and for every k such that $k > 0$ and $(i_{\mathbb{N}}^{k}) \bmod p = 1$ holds $0 < \mathrm{order}(i,p)$ and $\mathrm{order}(i,p) \leqslant k$.

One can prove the following propositions:

(50) If $p > 1$, then $\mathrm{order}(1,p) = 1$.

(51) If $p > 1$ and i and p are relative prime, then $\mathrm{order}(i,p) \neq 0$.

(52) If $p > 1$ and $n > 0$ and $(i_{\mathbb{N}}^{n}) \bmod p = 1$ and i and p are relative prime, then $\mathrm{order}(i,p) \mid n$.

(53) If $p > 1$ and i and p are relative prime and $\mathrm{order}(i,p) \mid n$, then $(i_{\mathbb{N}}^{n}) \bmod p = 1$.

(54) If p is prime and i and p are relative prime, then $\mathrm{order}(i,p) \mid p -' 1$.

4. Fermat Number

Let n be a natural number. The functor $\mathrm{Fermat}\, n$ yielding a natural number is defined as follows:

(Def. 3) $\mathrm{Fermat}\, n = (2_{\mathbb{N}}^{2_{\mathbb{N}}^{n}}) + 1$.

Next we state several propositions:

(55) $\mathrm{Fermat}\, 0 = 3$.

(56) $\mathrm{Fermat}\, 1 = 5$.

(57) $\mathrm{Fermat}\, 2 = 17$.

(58) $\mathrm{Fermat}\, 3 = 257$.

(59) $\mathrm{Fermat}\, 4 = 256 \cdot 256 + 1$.

(60) $\mathrm{Fermat}\, n > 2$.

(61) If p is prime and $p > 2$ and $p \mid \mathrm{Fermat}\, n$, then there exists a natural number k such that $p = k \cdot 2_{\mathbb{N}}^{n+1} + 1$.

(62) If $n \neq 0$, then 3 and $\mathrm{Fermat}\, n$ are relative prime.

5. Pepin's Test

We now state several propositions:

(63) If $n > 0$ and $3_{\mathbb{N}}^{(\mathrm{Fermat}\,n -' 1) \div 2} \equiv -1 (\mathrm{mod}\,\mathrm{Fermat}\,n)$, then $\mathrm{Fermat}\,n$ is prime.

(64) 5 is prime.

(65) 17 is prime.

(66) 257 is prime.

(67) $256 \cdot 256 + 1$ is prime.

References

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

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

[3] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Formalized Mathematics*, 7(**1**):123–126, 1998.

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

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

[6] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[7] Konrad Raczkowski and Andrzej Nędzusiak. Serieses. *Formalized Mathematics*, 2(**4**):449–452, 1991.

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

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

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

Received December 21, 1998

FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University of Białystok

Lattice of Substitutions is a Heyting Algebra

Adam Grabowski
University of Białystok

MML Identifier: HEYTING2.

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

1. Preliminaries

We adopt the following convention: V, C, x are sets and A, B are elements of SubstitutionSet(V,C).

Let a, b be sets. Note that $\{\langle a, b\rangle\}$ is function-like and relation-like.

Let A, B be sets. Observe that $A \dot{\rightarrow} B$ is functional.

Next we state several propositions:

(1) For all non empty sets V, C there exists an element f of $V \dot{\rightarrow} C$ such that $f \neq \emptyset$.

(2) For all sets a, b such that $b \in$ SubstitutionSet(V,C) and $a \in b$ holds a is a finite function.

(3) For every element f of $V \dot{\rightarrow} C$ and for every set g such that $g \subseteq f$ holds $g \in V \dot{\rightarrow} C$.

(4) $V \dot{\rightarrow} C \subseteq 2^{[: V, C :]}$.

(5) If V is finite and C is finite, then $V \dot{\rightarrow} C$ is finite.

One can check that there exists a set which is functional, finite, and non empty.

ISSN 1426–2630

2. Some Properties of Sets of Substitutions

One can prove the following four propositions:

(6) For every finite element a of $V \dot{\to} C$ holds $\{a\} \in \mathrm{SubstitutionSet}(V, C)$.

(7) If $A \frown B = A$, then for every set a such that $a \in A$ there exists a set b such that $b \in B$ and $b \subseteq a$.

(8) If $\mu(A \frown B) = A$, then for every set a such that $a \in A$ there exists a set b such that $b \in B$ and $b \subseteq a$.

(9) If for every set a such that $a \in A$ there exists a set b such that $b \in B$ and $b \subseteq a$, then $\mu(A \frown B) = A$.

Let V be a set, let C be a finite set, and let A be an element of $\mathrm{Fin}(V \dot{\to} C)$. The functor $\mathrm{Involved}\, A$ is defined by:

(Def. 1) $x \in \mathrm{Involved}\, A$ iff there exists a finite function f such that $f \in A$ and $x \in \mathrm{dom}\, f$.

In the sequel C denotes a finite set.

The following propositions are true:

(10) For every set V and for every finite set C and for every element A of $\mathrm{Fin}(V \dot{\to} C)$ holds $\mathrm{Involved}\, A \subseteq V$.

(11) For every set V and for every finite set C and for every element A of $\mathrm{Fin}(V \dot{\to} C)$ such that $A = \emptyset$ holds $\mathrm{Involved}\, A = \emptyset$.

(12) For every set V and for every finite set C and for every element A of $\mathrm{Fin}(V \dot{\to} C)$ holds $\mathrm{Involved}\, A$ is finite.

(13) For every finite set C and for every element A of $\mathrm{Fin}(\emptyset \dot{\to} C)$ holds $\mathrm{Involved}\, A = \emptyset$.

Let V be a set, let C be a finite set, and let A be an element of $\mathrm{Fin}(V \dot{\to} C)$. The functor $-A$ yielding an element of $\mathrm{Fin}(V \dot{\to} C)$ is defined as follows:

(Def. 2) $-A = \{f;\, f$ ranges over elements of $\mathrm{Involved}\, A \dot{\to} C : \bigwedge_{g\,:\,\text{element of } V \dot{\to} C} (g \in A \Rightarrow f \not\approx g)\}$.

One can prove the following propositions:

(14) $A \frown -A = \emptyset$.

(15) If $A = \emptyset$, then $-A = \{\emptyset\}$.

(16) If $A = \{\emptyset\}$, then $-A = \emptyset$.

(17) For every set V and for every finite set C and for every element A of $\mathrm{SubstitutionSet}(V, C)$ holds $\mu(A \frown -A) = \bot_{\mathrm{SubstLatt}(V,C)}$.

(18) For every non empty set V and for every finite non empty set C and for every element A of $\mathrm{SubstitutionSet}(V, C)$ such that $A = \emptyset$ holds $\mu(-A) = \top_{\mathrm{SubstLatt}(V,C)}$.

(19) Let V be a set, C be a finite set, A be an element of SubstitutionSet(V, C), a be an element of $V \dot{\rightarrow} C$, and B be an element of SubstitutionSet(V, C). Suppose $B = \{a\}$. If $A \frown B = \emptyset$, then there exists a finite set b such that $b \in -A$ and $b \subseteq a$.

Let V be a set, let C be a finite set, and let A, B be elements of Fin$(V \dot{\rightarrow} C)$. The functor $A \rightarrowtail B$ yielding an element of Fin$(V \dot{\rightarrow} C)$ is defined as follows:

(Def. 3) $A \rightarrowtail B = (V \dot{\rightarrow} C) \cap \{\bigcup\{f(i) \setminus i; i$ ranges over elements of $V \dot{\rightarrow} C$: $i \in A\}; f$ ranges over elements of $A \dot{\rightarrow} B$: $\mathrm{dom}\, f = A\}$.

Next we state two propositions:

(20) Let A, B be elements of Fin$(V \dot{\rightarrow} C)$ and s be a set. Suppose $s \in A \rightarrowtail B$. Then there exists a partial function f from A to B such that $s = \bigcup\{f(i) \setminus i; i$ ranges over elements of $V \dot{\rightarrow} C : i \in A\}$ and $\mathrm{dom}\, f = A$.

(21) For every set V and for every finite set C and for every element A of Fin$(V \dot{\rightarrow} C)$ such that $A = \emptyset$ holds $A \rightarrowtail A = \{\emptyset\}$.

We adopt the following convention: u, v are elements of the carrier of SubstLatt(V, C), a is an element of $V \dot{\rightarrow} C$, and K, L are elements of SubstitutionSet(V, C).

The following proposition is true

(22) For every set X such that $X \subseteq u$ holds X is an element of the carrier of SubstLatt(V, C).

3. Lattice of Substitutions is Implicative

Let us consider V, C. The functor pseudo_compl(V, C) yielding a unary operation on the carrier of SubstLatt(V, C) is defined as follows:

(Def. 4) For every element u' of SubstitutionSet(V, C) such that $u' = u$ holds $(\text{pseudo\_compl}(V, C))(u) = \mu(-u')$.

The functor StrongImpl(V, C) yielding a binary operation on the carrier of SubstLatt(V, C) is defined by:

(Def. 5) For all elements u', v' of SubstitutionSet(V, C) such that $u' = u$ and $v' = v$ holds $(\text{StrongImpl}(V, C))(u, v) = \mu(u' \rightarrowtail v')$.

Let us consider u. The functor 2^u yielding an element of Fin (the carrier of SubstLatt(V, C)) is defined by:

(Def. 6) $2^u = 2^u$.

The functor $\square \setminus_u \square$ yielding a unary operation on the carrier of SubstLatt(V, C) is defined by:

(Def. 7) $(\square \setminus_u \square)(v) = u \setminus v$.

Let us consider V, C. The functor $\mathrm{Atom}(V, C)$ yielding a function from $V \dot{\rightarrow} C$ into the carrier of $\mathrm{SubstLatt}(V, C)$ is defined as follows:

(Def. 8) For every element a of $V \dot{\rightarrow} C$ holds $(\mathrm{Atom}(V, C))(a) = \mu\{a\}$.

Next we state a number of propositions:

(23) $\bigsqcup^{\mathrm{f}}_{K} \mathrm{Atom}(V, C) = \mathrm{FinUnion}(K, \mathrm{singleton}_{V \dot{\rightarrow} C})$.

(24) For every element u of $\mathrm{SubstitutionSet}(V, C)$ holds $u = \bigsqcup^{\mathrm{f}}_{u} \mathrm{Atom}(V, C)$.

(25) $(\square \setminus_{u} \square)(v) \sqsubseteq u$.

(26) For every element a of $V \dot{\rightarrow} C$ such that a is finite and for every set c such that $c \in (\mathrm{Atom}(V, C))(a)$ holds $c = a$.

(27) For every element a of $V \dot{\rightarrow} C$ such that $K = \{a\}$ and $L = u$ and $L \frown K = \emptyset$ holds $(\mathrm{Atom}(V, C))(a) \sqsubseteq (\mathrm{pseudo\_compl}(V, C))(u)$.

(28) For every finite element a of $V \dot{\rightarrow} C$ holds $a \in (\mathrm{Atom}(V, C))(a)$.

(29) Let u, v be elements of $\mathrm{SubstitutionSet}(V, C)$. Suppose that for every set c such that $c \in u$ there exists a set b such that $b \in v$ and $b \subseteq c \cup a$. Then there exists a set b such that $b \in u \rightarrowtail v$ and $b \subseteq a$.

(30) Let a be a finite element of $V \dot{\rightarrow} C$. Suppose for every element b of $V \dot{\rightarrow} C$ such that $b \in u$ holds $b \approx a$ and $u \sqcap (\mathrm{Atom}(V, C))(a) \sqsubseteq v$. Then $(\mathrm{Atom}(V, C))(a) \sqsubseteq (\mathrm{StrongImpl}(V, C))(u, v)$.

(31) $u \sqcap (\mathrm{pseudo\_compl}(V, C))(u) = \bot_{\mathrm{SubstLatt}(V, C)}$.

(32) $u \sqcap (\mathrm{StrongImpl}(V, C))(u, v) \sqsubseteq v$.

Let us consider V, C. Observe that $\mathrm{SubstLatt}(V, C)$ is implicative.

One can prove the following proposition

(33) $u \Rightarrow v = \bigsqcup^{\mathrm{f}}_{2^{u}}((\text{the meet operation of } \mathrm{SubstLatt}(V, C))^{\circ}(\mathrm{pseudo\_compl}(V, C), (\mathrm{StrongImpl}(V, C))^{\circ}(\square \setminus_{u} \square, v)))$.

References

[1] Grzegorz Bancerek. Filters - part I. *Formalized Mathematics*, 1(**5**):813–819, 1990.
[2] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[4] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[5] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[6] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[7] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[8] Adam Grabowski. Lattice of substitutions. *Formalized Mathematics*, 6(**3**):359–361, 1997.
[9] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[10] Andrzej Trybulec. Finite join and finite meet and dual lattices. *Formalized Mathematics*, 1(**5**):983–988, 1990.
[11] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.
[12] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[13] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.
[14] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[15] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[16] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[17] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[18] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

Received December 31, 1998

Index of MML Identifiers

Contents

Formaliz. Math. 7 (**2**)

Continued on inside back cover