Contents

Formaliz. Math. 20 (**3**)

FORMALIZED MATHEMATICS
Vol. 20, No. 3, Pages 193–197, 2012
DOI: 10.2478/v10037-012-0022-0

VERSITA
versita.com/fm/

Transition of Consistency and Satisfiability under Language Extensions[1]

Julian J. Schlöder
Mathematisches Institut
Rheinische Friedrich-Wilhelms-Universität Bonn
Endenicher Allee 60
D-53113 Bonn, Germany

Peter Koepke
Mathematisches Institut
Rheinische Friedrich-Wilhelms-Universität Bonn
Endenicher Allee 60
D-53113 Bonn, Germany

Summary. This article is the first in a series of two Mizar articles constituting a formal proof of the Gödel Completeness theorem [17] for uncountably large languages. We follow the proof given in [18]. The present article contains the techniques required to expand formal languages. We prove that consistent or satisfiable theories retain these properties under changes to the language they are formulated in.

MML identifier: `QC_TRANS`, version: `7.14.01 4.183.1153`

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

[1] This article is part of the first author's Bachelor thesis under the supervision of the second author.

ISSN 1426–2630(p), 1898-9934(e)

1. Language Extensions

For simplicity, we adopt the following rules: A_1 denotes an alphabet, P_1 denotes a consistent subset of CQC-WFF A_1, p, r denote elements of CQC-WFF A_1, A denotes a non empty set, J denotes an interpretation of A_1 and A, v denotes an element of the valuations in A_1 and A, k denotes a natural number, l denotes a CQC-variable list of k and A_1, P denotes a predicate symbol of k and A_1, and x, y denote bound variables of A_1.

Let us consider A_1 and let A_2 be an alphabet. We say that A_2 is A_1-expanding if and only if:

(Def. 1) $A_1 \subseteq A_2$.

Let us consider A_1. Note that there exists an alphabet which is A_1-expanding.

Let A_3, A_4 be countable alphabets. One can check that there exists an alphabet which is countable, A_3-expanding, and A_4-expanding.

Let A_1, A_4 be alphabets and let P be a subset of CQC-WFF A_1. We say that P is A_4-consistent if and only if:

(Def. 2) For every subset S of CQC-WFF A_4 such that $P = S$ holds S is consistent.

Let us consider A_1. One can check that there exists a subset of CQC-WFF A_1 which is non empty and consistent.

Let us consider A_1. One can check that every subset of CQC-WFF A_1 which is consistent is also A_1-consistent and every subset of CQC-WFF A_1 which is A_1-consistent is also consistent.

For simplicity, we follow the rules: A_4 is an A_1-expanding alphabet, J_2 is an interpretation of A_4 and A, J_1 is an interpretation of A_1 and A, v_2 is an element of the valuations in A_4 and A, and v_1 is an element of the valuations in A_1 and A.

Next we state several propositions:

(1) $\mathrm{Arity}(P) = \mathrm{len}\, l$.

(2) $\mathrm{Symb}\, A_1 \subseteq \mathrm{Symb}\, A_4$.

(3) The predicate symbols of $A_1 \subseteq$ the predicate symbols of A_4.

(4) The bound variables of $A_1 \subseteq$ the bound variables of A_4.

(5) For every k holds every l is a CQC-variable list of k and A_4.

(6) P is a predicate symbol of k and A_4.

(7) For every A_1-expanding alphabet A_4 holds every p is an element of CQC-WFF A_4.

Let us consider A_1, let A_4 be an A_1-expanding alphabet, and let p be an element of CQC-WFF A_1. The functor A_4-Cast p yields an element of CQC-WFF A_4 and is defined by:

(Def. 3) $A_4\text{-Cast}\, p = p$.

Let us consider A_1, let A_4 be an A_1-expanding alphabet, and let x be a bound variable of A_1. The functor A_4-Cast x yields a bound variable of A_4 and is defined as follows:

(Def. 4) $A_4\text{-Cast}\,x = x$.

Let us consider A_1, let A_4 be an A_1-expanding alphabet, let us consider k, and let P be a predicate symbol of k and A_1. The functor A_4-Cast P yielding a predicate symbol of k and A_4 is defined as follows:

(Def. 5) $A_4\text{-Cast}\,P = P$.

Let us consider A_1, let A_4 be an A_1-expanding alphabet, let us consider k, and let l be a CQC-variable list of k and A_1. The functor A_4-Cast l yielding a CQC-variable list of k and A_4 is defined as follows:

(Def. 6) $A_4\text{-Cast}\,l = l$.

Next we state the proposition

(8) Let given p, r, x, P, l and A_4 be an A_1-expanding alphabet. Then $A_4\text{-Cast}\,\mathrm{VERUM}\,A_1 = \mathrm{VERUM}\,A_4$ and $A_4\text{-Cast}\,P[l] = (A_4\text{-Cast}\,P)[A_4\text{-Cast}\,l]$ and $A_4\text{-Cast}\,\neg p = \neg(A_4\text{-Cast}\,p)$ and $A_4\text{-Cast}(p \wedge r) = (A_4\text{-Cast}\,p) \wedge (A_4\text{-Cast}\,r)$ and $A_4\text{-Cast}\,\forall_x p = \forall_{A_4\text{-Cast}\,x}(A_4\text{-Cast}\,p)$.

2. Downward Transfer of Consistency and Satisfiability

The following propositions are true:

(9) Suppose $J_1 = J_2\restriction$the predicate symbols of A_1 and $v_1 = v_2\restriction$the bound variables of A_1. Then $J_2 \models_{v_2} A_4\text{-Cast}\,r$ if and only if $J_1 \models_{v_1} r$.

(10) Let A_4 be an A_1-expanding alphabet and T_1 be a subset of CQC-WFF A_4. Suppose $P_1 \subseteq T_1$. Let A_2 be a non empty set, J_2 be an interpretation of A_4 and A_2, and v_2 be an element of the valuations in A_4 and A_2. If $J_2 \models_{v_2} T_1$, then there exist A, J, v such that $J \models_v P_1$.

(11) Let f be a finite sequence of elements of CQC-WFF A_4 and g be a finite sequence of elements of CQC-WFF A_1. If $f = g$, then $\mathrm{Ant}(f) = \mathrm{Ant}(g)$ and $\mathrm{Suc}(f) = \mathrm{Suc}(g)$.

(12) For every p holds the still not bound in p = the still not bound in $A_4\text{-Cast}\,p$.

(13) Let p_2 be an element of CQC-WFF A_4, S be a substitution of A_1, S_2 be a substitution of A_4, x_2 be a bound variable of A_4, and given x, p. If $p = p_2$ and $S = S_2$ and $x = x_2$, then $\mathrm{RestrictSub}(x, p, S) = \mathrm{RestrictSub}(x_2, p_2, S_2)$.

(14) Let p_2 be an element of CQC-WFF A_4, S be a finite substitution of A_1, S_2 be a finite substitution of A_4, and given p. If $S = S_2$ and $p = p_2$, then $\mathrm{upVar}(S, p) = \mathrm{upVar}(S_2, p_2)$.

(15) Let p_2 be an element of CQC-WFF A_4, S be a substitution of A_1, S_2 be a substitution of A_4, x_2 be a bound variable of A_4, and given x, p. If $p = p_2$ and $S = S_2$ and $x = x_2$, then $\mathrm{ExpandSub}(x, p, \mathrm{RestrictSub}(x, \forall_x p, S)) = \mathrm{ExpandSub}(x_2, p_2, \mathrm{RestrictSub}(x_2, \forall_{x_2} p_2, S_2))$.

(16) Let Z be an element of CQC-Sub-WFF A_1 and Z_2 be an element of CQC-Sub-WFF A_4. Suppose $Z_{\mathbf{1}}$ is universal and $(Z_2)_{\mathbf{1}}$ is universal and $\mathrm{Bound}(Z_{\mathbf{1}}) = \mathrm{Bound}((Z_2)_{\mathbf{1}})$ and $\mathrm{Scope}(Z_{\mathbf{1}}) = \mathrm{Scope}((Z_2)_{\mathbf{1}})$ and $Z = Z_2$. Then S-Bound($^{@} Z$) = S-Bound($^{@} Z_2$).

(17) Let p_2 be an element of CQC-WFF A_4, x_2, y_2 be bound variables of A_4, and given p, x, y. If $p = p_2$ and $x = x_2$ and $y = y_2$, then $p(x, y) = p_2(x_2, y_2)$.

(18) For every consistent subset P_1 of CQC-WFF A_4 such that P_1 is a subset of CQC-WFF A_1 holds P_1 is A_1-consistent.

3. Upward Transfer of Consistency and Satisfiability

Next we state two propositions:

(19) For every p there exists a countable alphabet A_3 such that p is an element of CQC-WFF A_3 and A_1 is A_3-expanding.

(20) Let P_1 be a finite subset of CQC-WFF A_1. Then there exists a countable alphabet A_3 such that P_1 is a finite subset of CQC-WFF A_3 and A_1 is A_3-expanding.

Let us consider A_1 and let P_1 be a finite subset of CQC-WFF A_1. Note that the still not bound in P_1 is finite.

Next we state three propositions:

(21) Let T_1 be a subset of CQC-WFF A_4. Suppose $P_1 = T_1$. Let given A, J, v. Suppose $J \models_v P_1$. Then there exists a non empty set A_2 and there exists an interpretation J_2 of A_4 and A_2 and there exists an element v_2 of the valuations in A_4 and A_2 such that $J_2 \models_{v_2} T_1$.

(22) For every subset C_1 of CQC-WFF A_1 such that $C_1 \subseteq P_1$ holds C_1 is consistent.

(23) P_1 is A_4-consistent.

References

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

[2] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

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

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

[5] Patrick Braselmann and Peter Koepke. Coincidence lemma and substitution lemma. *Formalized Mathematics*, 13(**1**):17–26, 2005.

[6] Patrick Braselmann and Peter Koepke. Equivalences of inconsistency and Henkin models. *Formalized Mathematics*, 13(**1**):45–48, 2005.

[7] Patrick Braselmann and Peter Koepke. Gödel's completeness theorem. *Formalized Mathematics*, 13(**1**):49–53, 2005.

[8] Patrick Braselmann and Peter Koepke. A sequent calculus for first-order logic. *Formalized Mathematics*, 13(**1**):33–39, 2005.

[9] Patrick Braselmann and Peter Koepke. Substitution in first-order formulas: Elementary properties. *Formalized Mathematics*, 13(**1**):5–15, 2005.

[10] Patrick Braselmann and Peter Koepke. Substitution in first-order formulas. Part II. The construction of first-order formulas. *Formalized Mathematics*, 13(**1**):27–32, 2005.

[11] Czesław Byliński. A classical first order language. *Formalized Mathematics*, 1(**4**):669–676, 1990.

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

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

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

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

[16] Agata Darmochwał. A first–order predicate calculus. *Formalized Mathematics*, 1(**4**):689–695, 1990.

[17] Kurt Gödel. *Die Vollständigkeit der Axiome des logischen Funktionenkalküls*. Monatshefte für Mathematik und Physik 37, 1930.

[18] W. Thomas H.-D. Ebbinghaus, J. Flum. *Einführung in die Mathematische Logik*. Springer-Verlag, Berlin Heidelberg, 2007.

[19] Piotr Rudnicki and Andrzej Trybulec. A first order language. *Formalized Mathematics*, 1(**2**):303–311, 1990.

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

[21] Edmund Woronowicz. Interpretation and satisfiability in the first order logic. *Formalized Mathematics*, 1(**4**):739–743, 1990.

[22] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

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

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

Received May 7, 2012

..

FORMALIZED MATHEMATICS
Vol. 20, No. 3, Pages 199–203, 2012
DOI: 10.2478/v10037-012-0023-z

VERSITA
versita.com/fm/

The Gödel Completeness Theorem for Uncountable Languages[1]

Julian J. Schlöder
Mathematisches Institut
Rheinische Friedrich-Wilhelms-Universität Bonn
Endenicher Allee 60
D-53113 Bonn, Germany

Peter Koepke
Mathematisches Institut
Rheinische Friedrich-Wilhelms-Universität Bonn
Endenicher Allee 60
D-53113 Bonn, Germany

Summary. This article is the second in a series of two Mizar articles constituting a formal proof of the Gödel Completeness theorem [15] for uncountably large languages. We follow the proof given in [16]. The present article contains the techniques required to expand a theory such that the expanded theory contains witnesses and is negation faithful. Then the completeness theorem follows immediately.

MML identifier: GOEDCPUC, version: 7.14.01 4.183.1153

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

[1] This article is part of the first author's Bachelor thesis under the supervision of the second author.

ISSN 1426–2630(p), 1898-9934(e)

1. Formula-Constant Extension

For simplicity, we use the following convention: A_1 denotes an alphabet, P_1 denotes a consistent subset of CQC-WFF A_1, P_2 denotes a subset of CQC-WFF A_1, p, q, r, s denote elements of CQC-WFF A_1, A denotes a non empty set, J denotes an interpretation of A_1 and A, v denotes an element of the valuations in A_1 and A, n, k denote elements of $\mathbb{N}$, x denotes a bound variable of A_1, and A_2 denotes an A_1-expanding alphabet.

Let us consider A_1 and let P_1 be a subset of CQC-WFF A_1. We say that P_1 is satisfiable if and only if:

(Def. 1) There exist A, J, v such that $J \models_v P_1$.

In the sequel J_2 is an interpretation of A_2 and A and J_1 is an interpretation of A_1 and A.

One can prove the following proposition

(1) There exists a set s such that for all p, x holds $\langle s, \langle x, p\rangle\rangle \notin \mathrm{Symb}\, A_1$.

Let us consider A_1. A set is called a free symbol of A_1 if:

(Def. 2) For all p, x holds $\langle \mathrm{it}, \langle x, p\rangle\rangle \notin \mathrm{Symb}\, A_1$.

Let us consider A_1. The functor FCEx A_1 yielding an A_1-expanding alphabet is defined as follows:

(Def. 3) $\mathrm{FCEx}\, A_1 = \mathbb{N} \times (\mathrm{Symb}\, A_1 \cup \{\langle \text{ the free symbol of } A_1,\ \langle x, p\rangle\rangle\})$.

Let us consider A_1, p, x. The example of p and x yielding a bound variable of FCEx A_1 is defined as follows:

(Def. 4) The example of p and $x = \langle 4, \langle \text{ the free symbol of } A_1,\ \langle x, p\rangle\rangle\rangle$.

Let us consider A_1, p, x. The example formula of p and x yielding an element of CQC-WFF FCEx A_1 is defined by:

(Def. 5) The example formula of p and $x = \neg\exists_{\mathrm{FCEx}\, A_1 \text{-Cast}\, x}(\mathrm{FCEx}\, A_1 \text{-Cast}\, p) \vee (\mathrm{FCEx}\, A_1 \text{-Cast}\, p)(\mathrm{FCEx}\, A_1 \text{-Cast}\, x, \text{the example of } p \text{ and } x)$.

Let us consider A_1. The example formulae of A_1 yields a subset of CQC-WFF FCEx A_1 and is defined as follows:

(Def. 6) The example formulae of $A_1 = \{$the example formula of p and $x\}$.

One can prove the following proposition

(2) Let k be an element of $\mathbb{N}$. Suppose $k > 0$. Then there exists a k-element finite sequence F such that

(i) for every natural number n such that $n \leq k$ and $1 \leq n$ holds $F(n)$ is an alphabet,

(ii) $F(1) = A_1$, and

(iii) for every natural number n such that $n < k$ and $1 \leq n$ there exists an alphabet A_2 such that $F(n) = A_2$ and $F(n+1) = \mathrm{FCEx}\, A_2$.

Let us consider A_1 and let k be a natural number. A $k+1$-element finite sequence is said to be a FCEx-sequence of A_1 and k if it satisfies the conditions (Def. 7).

(Def. 7)(i) For every natural number n such that $n \leq k+1$ and $1 \leq n$ holds it(n) is an alphabet,

(ii) it$(1) = A_1$, and

(iii) for every natural number n such that $n < k+1$ and $1 \leq n$ there exists an alphabet A_2 such that it$(n) = A_2$ and it$(n+1) = \mathrm{FCEx}\,A_2$.

The following propositions are true:

(3) For every natural number k and for every FCEx-sequence S of A_1 and k holds $S(k+1)$ is an alphabet.

(4) For every natural number k and for every FCEx-sequence S of A_1 and k holds $S(k+1)$ is an A_1-expanding alphabet.

Let us consider A_1 and let k be a natural number. The k-th FCEx of A_1 yielding an A_1-expanding alphabet is defined as follows:

(Def. 8) The k-th FCEx of $A_1 =$ the FCEx-sequence of A_1 and $k(k+1)$.

Let us consider A_1, P_1. A function is called an EF-sequence of A_1 and P_1 if it satisfies the conditions (Def. 9).

(Def. 9)(i) $\mathrm{dom}\,\mathrm{it} = \mathbb{N}$,

(ii) it$(0) = P_1$, and

(iii) for every natural number n holds it$(n+1) =$ it$(n) \cup$ the example formulae of the n-th FCEx of A_1.

Next we state two propositions:

(5) For every natural number k holds FCEx (the k-th FCEx of A_1) $=$ the $(k+1)$-th FCEx of A_1.

(6) For all k, n such that $n \leq k$ holds the n-th FCEx of $A_1 \subseteq$ the k-th FCEx of A_1.

Let us consider A_1, P_1 and let k be a natural number. The k-th EF of A_1 and P_1 yields a subset of CQC-WFF (the k-th FCEx of A_1) and is defined as follows:

(Def. 10) The k-th EF of A_1 and $P_1 =$ the EF-sequence of A_1 and $P_1(k)$.

One can prove the following propositions:

(7) For all r, s, x holds A_2-Cast$(r \vee s) = A_2\text{-Cast}\,r \vee A_2\text{-Cast}\,s$ and $A_2\text{-Cast}\,\exists_x r = \exists_{A_2\text{-Cast}\,x}(A_2\text{-Cast}\,r)$.

(8) For all p, q, A, J, v holds $J \models_v p$ or $J \models_v q$ iff $J \models_v p \vee q$.

(9) $P_1 \cup$ the example formulae of A_1 is a consistent subset of CQC-WFF FCEx A_1.

2. The Completeness Theorem

We now state four propositions:

(10) There exists an A_1-expanding alphabet A_2 and there exists a consistent subset P_2 of CQC-WFF A_2 such that $P_1 \subseteq P_2$ and P_2 has examples.

(11) $P_1 \cup \{p\}$ is consistent or $P_1 \cup \{\neg p\}$ is consistent.

(12) Let P_2 be a consistent subset of CQC-WFF A_1. Then there exists a consistent subset T_1 of CQC-WFF A_1 such that T_1 is negation faithful and $P_2 \subseteq T_1$.

(13) For every consistent subset T_1 of CQC-WFF A_1 such that $P_1 \subseteq T_1$ and P_1 has examples holds T_1 has examples.

Let us consider A_1. One can check that every subset of CQC-WFF A_1 which is consistent is also satisfiable.

We now state the proposition

(14)[2] If $P_2 \models p$, then $P_2 \vdash p$.

References

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

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

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

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

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

[6] Patrick Braselmann and Peter Koepke. Equivalences of inconsistency and Henkin models. *Formalized Mathematics*, 13(**1**):45–48, 2005.

[7] Patrick Braselmann and Peter Koepke. Gödel's completeness theorem. *Formalized Mathematics*, 13(**1**):49–53, 2005.

[8] Patrick Braselmann and Peter Koepke. A sequent calculus for first-order logic. *Formalized Mathematics*, 13(**1**):33–39, 2005.

[9] Patrick Braselmann and Peter Koepke. Substitution in first-order formulas. Part II. The construction of first-order formulas. *Formalized Mathematics*, 13(**1**):27–32, 2005.

[10] Czesław Byliński. A classical first order language. *Formalized Mathematics*, 1(**4**):669–676, 1990.

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

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

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

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

[15] Kurt Gödel. *Die Vollständigkeit der Axiome des logischen Funktionenkalküls.* Monatshefte für Mathematik und Physik 37, 1930.

[16] W. Thomas H.-D. Ebbinghaus, J. Flum. *Einführung in die Mathematische Logik.* Springer-Verlag, Berlin Heidelberg, 2007.

[17] Piotr Rudnicki and Andrzej Trybulec. A first order language. *Formalized Mathematics*, 1(**2**):303–311, 1990.

[2] Completeness Theorem.

[18] Julian J. Schlöder and Peter Koepke. Transition of consistency and satisfiability under language extensions. *Formalized Mathematics*, 20(**3**):193–197, 2012, doi: 10.2478/v10037-012-0022-0.

[19] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

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

[21] Edmund Woronowicz. Interpretation and satisfiability in the first order logic. *Formalized Mathematics*, 1(**4**):739–743, 1990.

[22] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

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

Received May 7, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 3, Pages 205–214, 2012
DOI: 10.2478/v10037-012-0024-y

VERSITA
versita.com/fm/

Quotient Module of $\mathbb{Z}$-module[1]

Yuichi Futa
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article we formalize a quotient module of $\mathbb{Z}$-module and a vector space constructed by the quotient module. We formally prove that for a $\mathbb{Z}$-module V and a prime number p, a quotient module V/pV has the structure of a vector space over $\mathbb{F}_p$. $\mathbb{Z}$-module is necessary for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm and cryptographic systems with lattices [14]. Some theorems in this article are described by translating theorems in [20] and [19] into theorems of $\mathbb{Z}$-module.

MML identifier: ZMODUL02, version: 7.14.01 4.183.1153

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

1. Quotient Module of $\mathbb{Z}$-module and Vector Space

For simplicity, we follow the rules: x is a set, V is a $\mathbb{Z}$-module, u, v are vectors of V, F, G, H are finite sequences of elements of V, i is an element of $\mathbb{N}$, and f, g are sequences of V.

Let V be a $\mathbb{Z}$-module and let a be an integer number. The functor $a \cdot V$ yielding a non empty subset of V is defined by:

(Def. 1) $a \cdot V = \{a \cdot v : v$ ranges over elements of $V\}$.

Let V be a $\mathbb{Z}$-module and let a be an integer number. The functor $\mathrm{Zero}(a, V)$ yielding an element of $a \cdot V$ is defined as follows:

(Def. 2) $\mathrm{Zero}(a, V) = 0_V$.

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

Let V be a $\mathbb{Z}$-module and let a be an integer number. The functor $\mathrm{Add}(a, V)$ yielding a function from $(a \cdot V) \times (a \cdot V)$ into $a \cdot V$ is defined by:

(Def. 3) $\mathrm{Add}(a, V) = (\text{the addition of } V) \restriction ((a \cdot V) \times (a \cdot V))$.

Let V be a $\mathbb{Z}$-module and let a be an integer number. The functor $\mathrm{Mult}(a, V)$ yielding a function from $\mathbb{Z} \times (a \cdot V)$ into $a \cdot V$ is defined by:

(Def. 4) $\mathrm{Mult}(a, V) = (\text{the external multiplication of } V) \restriction (\mathbb{Z} \times (a \cdot V))$.

Let V be a $\mathbb{Z}$-module and let a be an integer number. The functor $a \circ V$ yields a submodule of V and is defined as follows:

(Def. 5) $a \circ V = \langle a \cdot V, \mathrm{Zero}(a, V), \mathrm{Add}(a, V), \mathrm{Mult}(a, V) \rangle$.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. The functor $\mathrm{CosetSet}(V, W)$ yields a non empty family of subsets of V and is defined as follows:

(Def. 6) $\mathrm{CosetSet}(V, W) = \{A : A \text{ ranges over cosets of } W\}$.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. The functor $\mathrm{addCoset}(V, W)$ yields a binary operation on $\mathrm{CosetSet}(V, W)$ and is defined as follows:

(Def. 7) For all elements A, B of $\mathrm{CosetSet}(V, W)$ and for all vectors a, b of V such that $A = a+W$ and $B = b+W$ holds $(\mathrm{addCoset}(V, W))(A, B) = a+b+W$.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. The functor $\mathrm{zeroCoset}(V, W)$ yielding an element of $\mathrm{CosetSet}(V, W)$ is defined by:

(Def. 8) $\mathrm{zeroCoset}(V, W) = \text{the carrier of } W$.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. The functor $\mathrm{lmultCoset}(V, W)$ yields a function from $\mathbb{Z} \times \mathrm{CosetSet}(V, W)$ into $\mathrm{CosetSet}(V, W)$ and is defined as follows:

(Def. 9) For every integer z and for every element A of $\mathrm{CosetSet}(V, W)$ and for every vector a of V such that $A = a+W$ holds $(\mathrm{lmultCoset}(V, W))(z, A) = z \cdot a + W$.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. The functor $\mathbb{Z}\text{-ModuleQuot}(V, W)$ yields a strict $\mathbb{Z}$-module and is defined by the conditions (Def. 10).

(Def. 10)(i) The carrier of $\mathbb{Z}\text{-ModuleQuot}(V, W) = \mathrm{CosetSet}(V, W)$,

(ii) the addition of $\mathbb{Z}\text{-ModuleQuot}(V, W) = \mathrm{addCoset}(V, W)$,

(iii) $0_{\mathbb{Z}\text{-ModuleQuot}(V,W)} = \mathrm{zeroCoset}(V, W)$, and

(iv) the external multiplication of $\mathbb{Z}\text{-ModuleQuot}(V, W) = \mathrm{lmultCoset}(V, W)$.

The following propositions are true:

(1) Let p be an integer, V be a $\mathbb{Z}$-module, W be a submodule of V, and x be a vector of $\mathbb{Z}\text{-ModuleQuot}(V, W)$. If $W = p \circ V$, then $p \cdot x = 0_{\mathbb{Z}\text{-ModuleQuot}(V,W)}$.

(2) Let p, i be integers, V be a $\mathbb{Z}$-module, W be a submodule of V, and x be a vector of $\mathbb{Z}$-ModuleQuot(V, W). If $p \neq 0$ and $W = p \circ V$, then $i \cdot x = (i \bmod p) \cdot x$.

(3) Let p, q be integers, V be a $\mathbb{Z}$-module, W be a submodule of V, and v be a vector of V. Suppose $W = p \circ V$ and $p > 1$ and $q > 1$ and p and q are relative prime. If $q \cdot v = 0_V$, then $v + W = 0_{\mathbb{Z}\text{-ModuleQuot}(V,W)}$.

Let p be a prime number and let V be a $\mathbb{Z}$-module. The functor MultModpV(V, p) yields a function from (the carrier of GF(p)) × (the carrier of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$) into the carrier of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$ and is defined by the condition (Def. 11).

(Def. 11) Let a be an element of GF(p), i be an integer, and x be an element of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$. If $a = i \bmod p$, then (MultModpV(V, p))$(a, x) = (i \bmod p) \cdot x$.

Let p be a prime number and let V be a $\mathbb{Z}$-module. The functor $\mathbb{Z}$-MQVectSp(V, p) yielding a non empty strict vector space structure over GF(p) is defined by:

(Def. 12) $\mathbb{Z}$-MQVectSp$(V, p) = \langle$the carrier of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$, the addition of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$, the zero of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$, MultModpV$(V, p)\rangle$.

Let p be a prime number and let V be a $\mathbb{Z}$-module. Observe that $\mathbb{Z}$-MQVectSp(V, p) is scalar distributive, vector distributive, scalar associative, scalar unital, add-associative, right zeroed, right complementable, and Abelian.

Let p be a prime number, let V be a $\mathbb{Z}$-module, and let v be a vector of V. The functor $\mathbb{Z}$-MtoMQV(V, p, v) yields a vector of $\mathbb{Z}$-MQVectSp(V, p) and is defined as follows:

(Def. 13) $\mathbb{Z}$-MtoMQV$(V, p, v) = v + p \circ V$.

Let X be a $\mathbb{Z}$-module. The functor MultINT∗ X yielding a function from (the carrier of $(\mathbb{Z}^{\rm R})$) × (the carrier of X) into the carrier of X is defined by:

(Def. 14) MultINT∗ X = the external multiplication of X.

Let X be a $\mathbb{Z}$-module. The functor PreNorms X yielding a non empty strict vector space structure over $\mathbb{Z}^{\rm R}$ is defined by:

(Def. 15) PreNorms $X = \langle$the carrier of X, the addition of X, the zero of X, MultINT∗ $X\rangle$.

Let X be a $\mathbb{Z}$-module. Observe that PreNorms X is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

Let X be a left module over $\mathbb{Z}^{\rm R}$. The functor MultINT∗ X yielding a function from $\mathbb{Z}$ × the carrier of X into the carrier of X is defined as follows:

(Def. 16) MultINT∗ X = the left multiplication of X.

Let X be a left module over $\mathbb{Z}^{\mathrm{R}}$. The functor PreNorms X yields a non empty strict $\mathbb{Z}$-module structure and is defined as follows:

(Def. 17) PreNorms $X = \langle$the carrier of X, the zero of X, the addition of X, MultINT$*$ $X\rangle$.

Let X be a left module over $\mathbb{Z}^{\mathrm{R}}$. Note that PreNorms X is Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, and scalar unital.

We now state four propositions:

(4) Let X be a $\mathbb{Z}$-module, v, w be elements of X, and v_1, w_1 be elements of PreNorms X. If $v = v_1$ and $w = w_1$, then $v + w = v_1 + w_1$ and $v - w = v_1 - w_1$.

(5) Let X be a $\mathbb{Z}$-module, v be an element of X, v_1 be an element of PreNorms X, a be an integer, and a_1 be an element of $\mathbb{Z}^{\mathrm{R}}$. If $v = v_1$ and $a = a_1$, then $a \cdot v = a_1 \cdot v_1$.

(6) Let X be a left module over $\mathbb{Z}^{\mathrm{R}}$, v, w be elements of X, and v_1, w_1 be elements of PreNorms X. If $v = v_1$ and $w = w_1$, then $v + w = v_1 + w_1$ and $v - w = v_1 - w_1$.

(7) Let X be a left module over $\mathbb{Z}^{\mathrm{R}}$, v be an element of X, v_1 be an element of PreNorms X, a be an element of $\mathbb{Z}^{\mathrm{R}}$, and a_1 be an integer. If $v = v_1$ and $a = a_1$, then $a \cdot v = a_1 \cdot v_1$.

2. Linear Combination of $\mathbb{Z}$-module

Let V be a non empty zero structure. An element of $\mathbb{Z}^{\text{the carrier of } V}$ is said to be a $\mathbb{Z}$-linear combination of V if:

(Def. 18) There exists a finite subset T of V such that for every element v of V such that $v \notin T$ holds $\mathrm{it}(v) = 0$.

In the sequel K, L, L_1, L_2, L_3 denote $\mathbb{Z}$-linear combinations of V.

Let V be a non empty additive loop structure and let L be a $\mathbb{Z}$-linear combination of V. The support of L yielding a finite subset of V is defined by:

(Def. 19) The support of $L = \{v \in V \colon L(v) \neq 0\}$.

Next we state the proposition

(8) Let V be a non empty additive loop structure, L be a $\mathbb{Z}$-linear combination of V, and v be an element of V. Then $L(v) = 0$ if and only if $v \notin$ the support of L.

Let V be a non empty additive loop structure. The functor $\mathbb{Z}$-ZeroLC V yields a $\mathbb{Z}$-linear combination of V and is defined by:

(Def. 20) The support of $\mathbb{Z}$-ZeroLC $V = \emptyset$.

One can prove the following proposition

(9) For every non empty additive loop structure V and for every element v of V holds $(\mathbb{Z}\text{-ZeroLC}\,V)(v) = 0$.

Let V be a non empty additive loop structure and let A be a subset of V. A $\mathbb{Z}$-linear combination of V is said to be a $\mathbb{Z}$-linear combination of A if:

(Def. 21) The support of it $\subseteq A$.

For simplicity, we adopt the following convention: a, b are integers, G, H_1, H_2, F, F_1, F_2, F_3 are finite sequences of elements of V, A, B are subsets of V, v_1, v_2, v_3, u_1, u_2, u_3 are vectors of V, f is a function from the carrier of V into $\mathbb{Z}$, i is an element of $\mathbb{N}$, and l, l_1, l_2 are $\mathbb{Z}$-linear combinations of A.

One can prove the following propositions:

(10) If $A \subseteq B$, then l is a $\mathbb{Z}$-linear combination of B.

(11) $\mathbb{Z}$-ZeroLC V is a $\mathbb{Z}$-linear combination of A.

(12) For every $\mathbb{Z}$-linear combination l of $\emptyset_{\text{the carrier of } V}$ holds $l = \mathbb{Z}\text{-ZeroLC}\,V$.

Let us consider V, F, f. The functor $f \cdot F$ yields a finite sequence of elements of V and is defined by:

(Def. 22) $\text{len}(f \cdot F) = \text{len}\,F$ and for every i such that $i \in \text{dom}(f \cdot F)$ holds $(f \cdot F)(i) = f(F_i) \cdot F_i$.

Next we state several propositions:

(13) If $i \in \text{dom}\,F$ and $v = F(i)$, then $(f \cdot F)(i) = f(v) \cdot v$.

(14) $f \cdot \varepsilon_{(\text{the carrier of } V)} = \varepsilon_{(\text{the carrier of } V)}$.

(15) $f \cdot \langle v \rangle = \langle f(v) \cdot v \rangle$.

(16) $f \cdot \langle v_1, v_2 \rangle = \langle f(v_1) \cdot v_1, f(v_2) \cdot v_2 \rangle$.

(17) $f \cdot \langle v_1, v_2, v_3 \rangle = \langle f(v_1) \cdot v_1, f(v_2) \cdot v_2, f(v_3) \cdot v_3 \rangle$.

Let us consider V, L. The functor $\sum L$ yielding an element of V is defined by:

(Def. 23) There exists F such that F is one-to-one and $\text{rng}\,F =$ the support of L and $\sum L = \sum(L \cdot F)$.

Next we state several propositions:

(18) $A \neq \emptyset$ and A is linearly closed iff for every l holds $\sum l \in A$.

(19) $\sum \mathbb{Z}\text{-ZeroLC}\,V = 0_V$.

(20) For every $\mathbb{Z}$-linear combination l of $\emptyset_{\text{the carrier of } V}$ holds $\sum l = 0_V$.

(21) For every $\mathbb{Z}$-linear combination l of $\{v\}$ holds $\sum l = l(v) \cdot v$.

(22) If $v_1 \neq v_2$, then for every $\mathbb{Z}$-linear combination l of $\{v_1, v_2\}$ holds $\sum l = l(v_1) \cdot v_1 + l(v_2) \cdot v_2$.

(23) If the support of $L = \emptyset$, then $\sum L = 0_V$.

(24) If the support of $L = \{v\}$, then $\sum L = L(v) \cdot v$.

(25) If the support of $L = \{v_1, v_2\}$ and $v_1 \neq v_2$, then $\sum L = L(v_1) \cdot v_1 + L(v_2) \cdot v_2$.

Let V be a non empty additive loop structure and let L_1, L_2 be $\mathbb{Z}$-linear combinations of V. Let us observe that $L_1 = L_2$ if and only if:

(Def. 24) For every element v of V holds $L_1(v) = L_2(v)$.

Let V be a non empty additive loop structure and let L_1, L_2 be $\mathbb{Z}$-linear combinations of V. Then $L_1 + L_2$ is a $\mathbb{Z}$-linear combination of V and it can be characterized by the condition:

(Def. 25) For every element v of V holds $(L_1 + L_2)(v) = L_1(v) + L_2(v)$.

Let us observe that the functor $L_1 + L_2$ is commutative.

The following propositions are true:

(26) The support of $L_1 + L_2 \subseteq$ (the support of L_1) $\cup$ (the support of L_2).

(27) Suppose L_1 is a $\mathbb{Z}$-linear combination of A and L_2 is a $\mathbb{Z}$-linear combination of A. Then $L_1 + L_2$ is a $\mathbb{Z}$-linear combination of A.

(28) $L_1 + (L_2 + L_3) = (L_1 + L_2) + L_3$.

Let us consider V, a, L. Note that $L + \mathbb{Z}$-ZeroLC V reduces to L.

The functor $a \cdot L$ yielding a $\mathbb{Z}$-linear combination of V is defined as follows:

(Def. 26) For every v holds $(a \cdot L)(v) = a \cdot L(v)$.

We now state several propositions:

(29) If $a \neq 0$, then the support of $a \cdot L =$ the support of L.

(30) $0 \cdot L = \mathbb{Z}$-ZeroLC V.

(31) If L is a $\mathbb{Z}$-linear combination of A, then $a \cdot L$ is a $\mathbb{Z}$-linear combination of A.

(32) $(a + b) \cdot L = a \cdot L + b \cdot L$.

(33) $a \cdot (L_1 + L_2) = a \cdot L_1 + a \cdot L_2$.

(34) $a \cdot (b \cdot L) = (a \cdot b) \cdot L$.

Let us consider V, L. One can check that $1 \cdot L$ reduces to L.

The functor $-L$ yielding a $\mathbb{Z}$-linear combination of V is defined as follows:

(Def. 27) $-L = (-1) \cdot L$.

Let us note that the functor $-L$ is involutive.

We now state four propositions:

(35) $(-L)(v) = -L(v)$.

(36) If $L_1 + L_2 = \mathbb{Z}$-ZeroLC V, then $L_2 = -L_1$.

(37) The support of $-L =$ the support of L.

(38) If L is a $\mathbb{Z}$-linear combination of A, then $-L$ is a $\mathbb{Z}$-linear combination of A.

Let us consider V, L_1, L_2. The functor $L_1 - L_2$ yields a $\mathbb{Z}$-linear combination of V and is defined as follows:

(Def. 28) $L_1 - L_2 = L_1 + -L_2$.

The following four propositions are true:

(39) $(L_1 - L_2)(v) = L_1(v) - L_2(v)$.

(40) The support of $L_1 - L_2 \subseteq$ (the support of L_1) $\cup$ (the support of L_2).

(41) Suppose L_1 is a $\mathbb{Z}$-linear combination of A and L_2 is a $\mathbb{Z}$-linear combination of A. Then $L_1 - L_2$ is a $\mathbb{Z}$-linear combination of A.

(42) $L - L = \mathbb{Z}\text{-ZeroLC}\, V$.

Let us consider V. The functor LC_V yielding a set is defined by:

(Def. 29) $x \in \mathrm{LC}_V$ iff x is a $\mathbb{Z}$-linear combination of V.

Let us consider V. One can verify that LC_V is non empty.

In the sequel e, e_1, e_2 denote elements of LC_V.

Let us consider V, e. The functor ${}^{@}e$ yielding a $\mathbb{Z}$-linear combination of V is defined by:

(Def. 30) ${}^{@}e = e$.

Let us consider V, L. The functor ${}^{@}L$ yielding an element of LC_V is defined by:

(Def. 31) ${}^{@}L = L$.

Let us consider V. The functor $+_{\mathrm{LC}_V}$ yields a binary operation on LC_V and is defined as follows:

(Def. 32) For all e_1, e_2 holds $+_{\mathrm{LC}_V}(e_1, e_2) = ({}^{@}e_1) + {}^{@}e_2$.

Let us consider V. The functor $\cdot_{\mathrm{LC}_V}$ yields a function from $\mathbb{Z} \times \mathrm{LC}_V$ into LC_V and is defined by:

(Def. 33) For all a, e holds $\cdot_{\mathrm{LC}_V}(\langle a, e\rangle) = a \cdot ({}^{@}e)$.

Let us consider V. The functor LC-$\mathbb{Z}$-Module V yielding a $\mathbb{Z}$-module structure is defined as follows:

(Def. 34) LC-$\mathbb{Z}$-Module $V = \langle \mathrm{LC}_V, {}^{@}\mathbb{Z}\text{-ZeroLC}\, V, +_{\mathrm{LC}_V}, \cdot_{\mathrm{LC}_V} \rangle$.

Let us consider V. One can check that LC-$\mathbb{Z}$-Module V is strict and non empty.

Let us consider V. Observe that LC-$\mathbb{Z}$-Module V is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

Next we state several propositions:

(43) The carrier of LC-$\mathbb{Z}$-Module $V = \mathrm{LC}_V$.

(44) $0_{\text{LC-}\mathbb{Z}\text{-Module}\, V} = \mathbb{Z}\text{-ZeroLC}\, V$.

(45) The addition of LC-$\mathbb{Z}$-Module $V = +_{\mathrm{LC}_V}$.

(46) The external multiplication of LC-$\mathbb{Z}$-Module $V = \cdot_{\mathrm{LC}_V}$.

(47) ${L_1}^{\text{LC-}\mathbb{Z}\text{-Module}\, V} + {L_2}^{\text{LC-}\mathbb{Z}\text{-Module}\, V} = L_1 + L_2$.

(48) $a \cdot L^{\text{LC-}\mathbb{Z}\text{-Module}\, V} = a \cdot L$.

(49) $-L^{\text{LC-}\mathbb{Z}\text{-Module}\, V} = -L$.

(50) ${L_1}^{\text{LC-}\mathbb{Z}\text{-Module}\, V} - {L_2}^{\text{LC-}\mathbb{Z}\text{-Module}\, V} = L_1 - L_2$.

Let us consider V, A. The functor LC-$\mathbb{Z}$-Module A yielding a strict submodule of LC-$\mathbb{Z}$-Module V is defined by:

(Def. 35) The carrier of LC-$\mathbb{Z}$-Module $A = \{l\}$.

3. Linearly Independent Subset of $\mathbb{Z}$-module

For simplicity, we use the following convention: W, W_1, W_2, W_3 are submodules of V, v, v_1 are vectors of V, C is a subset of V, T is a finite subset of V, L, L_1, L_2 are $\mathbb{Z}$-linear combinations of V, l is a $\mathbb{Z}$-linear combination of A, and G is a finite sequence of elements of the carrier of V.

One can prove the following propositions:

(51) $f \cdot (F ^\frown G) = (f \cdot F) ^\frown (f \cdot G)$.

(52) $\sum(L_1 + L_2) = \sum L_1 + \sum L_2$.

(53) $\sum(a \cdot L) = a \cdot \sum L$.

(54) $\sum(-L) = -\sum L$.

(55) $\sum(L_1 - L_2) = \sum L_1 - \sum L_2$.

Let us consider V, A. We say that A is linearly independent if and only if:

(Def. 36) For every l such that $\sum l = 0_V$ holds the support of $l = \emptyset$.

Let us consider V, A. We introduce A is linearly dependent as an antonym of A is linearly independent.

We now state three propositions:

(56) If $A \subseteq B$ and B is linearly independent, then A is linearly independent.

(57) If A is linearly independent, then $0_V \notin A$.

(58) $\emptyset_{\text{the carrier of } V}$ is linearly independent.

Let us consider V. Observe that there exists a subset of V which is linearly independent.

One can prove the following proposition

(59) If V inherits cancelable on multiplication, then $\{v\}$ is linearly independent iff $v \neq 0_V$.

Let us consider V. Note that $\{0_V\}$ is linearly dependent as a subset of V.

One can prove the following propositions:

(60) If $\{v_1, v_2\}$ is linearly independent, then $v_1 \neq 0_V$.

(61) $\{v, 0_V\}$ is linearly dependent.

(62) Suppose V inherits cancelable on multiplication. Then $v_1 \neq v_2$ and $\{v_1, v_2\}$ is linearly independent if and only if $v_2 \neq 0_V$ and for all a, b such that $b \neq 0$ holds $b \cdot v_1 \neq a \cdot v_2$.

(63) Suppose V inherits cancelable on multiplication. Then $v_1 \neq v_2$ and $\{v_1, v_2\}$ is linearly independent if and only if for all a, b such that $a \cdot v_1 + b \cdot v_2 = 0_V$ holds $a = 0$ and $b = 0$.

Let us consider V, A. The functor $\mathrm{Lin}(A)$ yielding a strict submodule of V is defined as follows:

(Def. 37) The carrier of $\mathrm{Lin}(A) = \{\sum l\}$.

The following propositions are true:

(64) $x \in \mathrm{Lin}(A)$ iff there exists l such that $x = \sum l$.

(65) If $x \in A$, then $x \in \mathrm{Lin}(A)$.

(66) $x \in \mathbf{0}_V$ iff $x = 0_V$.

(67) $\mathrm{Lin}(\emptyset_{\text{the carrier of } V}) = \mathbf{0}_V$.

(68) If $\mathrm{Lin}(A) = \mathbf{0}_V$, then $A = \emptyset$ or $A = \{0_V\}$.

(69) For every strict $\mathbb{Z}$-module V and for every subset A of V such that $A =$ the carrier of V holds $\mathrm{Lin}(A) = V$.

(70) If $A \subseteq B$, then $\mathrm{Lin}(A)$ is a submodule of $\mathrm{Lin}(B)$.

(71) For every strict $\mathbb{Z}$-module V and for all subsets A, B of V such that $\mathrm{Lin}(A) = V$ and $A \subseteq B$ holds $\mathrm{Lin}(B) = V$.

(72) $\mathrm{Lin}(A \cup B) = \mathrm{Lin}(A) + \mathrm{Lin}(B)$.

(73) $\mathrm{Lin}(A \cap B)$ is a submodule of $\mathrm{Lin}(A) \cap \mathrm{Lin}(B)$.

4. Theorems Related to Submodule

One can prove the following propositions:

(74) If W_1 is a submodule of W_3, then $W_1 \cap W_2$ is a submodule of W_3.

(75) If W_1 is a submodule of W_2 and a submodule of W_3, then W_1 is a submodule of $W_2 \cap W_3$.

(76) If W_1 is a submodule of W_3 and W_2 is a submodule of W_3, then $W_1 + W_2$ is a submodule of W_3.

(77) If W_1 is a submodule of W_2, then W_1 is a submodule of $W_2 + W_3$.

References

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

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

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

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

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

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

[7] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

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

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

[10] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012, doi: 10.2478/v10037-012-0007-z.

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

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

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

[14] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: A cryptographic perspective (the international series in engineering and computer science). 2002.

[15] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.

[16] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

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

[18] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[19] Wojciech A. Trybulec. Basis of real linear space. *Formalized Mathematics*, 1(**5**):847–850, 1990.

[20] Wojciech A. Trybulec. Linear combinations in real linear space. *Formalized Mathematics*, 1(**3**):581–588, 1990.

[21] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

[22] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

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

Received May 7, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 3, Pages 215–219, 2012
DOI: 10.2478/v10037-012-0025-x

VERSITA
versita.com/fm/

The Derivations of Temporal Logic Formulas[1]

Mariusz Giero[2]
Department of Logic, Informatics and Philosophy of Science
University of Białystok
Plac Uniwersytecki 1, 15-420 Białystok, Poland

Summary. This is a preliminary article to prove the completeness theorem of an extension of basic propositional temporal logic. We base it on the proof of completeness for basic propositional temporal logic given in [12]. We introduce n-ary connectives and prove their properties. We derive temporal logic formulas.

MML identifier: LTLAXIO2, version: 7.14.01 4.183.1153

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

1. Preliminaries

For simplicity, we adopt the following rules: A, B, p, q, r, s are elements of the LTLB-WFF, i, k, n are elements of $\mathbb{N}$, X is a subset of the LTLB-WFF, f, f_1 are finite sequences of elements of the LTLB-WFF, and g is a function from the LTLB-WFF into *Boolean*.

Let f be a finite sequence and let x be an empty set. One can check that $f(x)$ is empty.

We now state three propositions:

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

[2] I would like to thank Prof. Andrzej Trybulec, Dr. Artur Korniłowicz, Dr. Adam Naumowicz and Karol Pąk for their help in preparation of the article.

(1) For every finite sequence f such that $\operatorname{len} f > 0$ and $n > 0$ holds $\operatorname{len}(f \restriction n) > 0$.

(2) For every finite sequence f such that $\operatorname{len} f = 0$ holds $f_{\lfloor n} = f$.

(3) For all finite sequences f, g such that $\operatorname{rng} f = \operatorname{rng} g$ holds $\operatorname{len} f = 0$ iff $\operatorname{len} g = 0$.

Let us consider A, B. The functor $\mathrm{UN}(A, B)$ yields an element of the LTLB-WFF and is defined by:

(Def. 1) $\mathrm{UN}(A, B) = B \vee (A \,\&\&(A\, \mathcal{U}\, B))$.

One can prove the following proposition

(4) $\mathrm{VAL}_g(\top_t) = 1$.

Next we state the proposition

(5) $\mathrm{VAL}_g(p \vee q) = \mathrm{VAL}_g(p) \vee \mathrm{VAL}_g(q)$.

2. n-Argument Connectives and their Properties

Let us consider f. The functor conjunction f yielding a finite sequence of elements of the LTLB-WFF is defined as follows:

(Def. 2)(i) len conjunction f = $\operatorname{len} f$ and $(\text{conjunction } f)(1) = f(1)$ and for every i such that $1 \leq i < \operatorname{len} f$ holds $(\text{conjunction } f)(i + 1) = (\text{conjunction } f)_i \,\&\&\, f_{i+1}$ if $\operatorname{len} f > 0$,

(ii) conjunction $f = \langle \top_t \rangle$, otherwise.

Let us consider f, A. The functor implication(f, A) yielding a finite sequence of elements of the LTLB-WFF is defined as follows:

(Def. 3)(i) len implication$(f, A) = \operatorname{len} f$ and $(\text{implication}(f, A))(1) = \mathcal{G}(f_1) \Rightarrow A$ and for every i such that $1 \leq i < \operatorname{len} f$ holds $(\text{implication}(f, A))(i+1) = \mathcal{G}(f_{i+1}) \Rightarrow (\text{implication}(f, A))_i$ if $\operatorname{len} f > 0$,

(ii) implication$(f, A) = \varepsilon_{(\text{the LTLB-WFF})}$, otherwise.

Let us consider f. The functor negation f yields a finite sequence of elements of the LTLB-WFF and is defined by:

(Def. 4) len negation f = $\operatorname{len} f$ and for every i such that $1 \leq i \leq \operatorname{len} f$ holds $(\text{negation } f)(i) = \neg(f_i)$.

Let us consider f. The functor next f yields a finite sequence of elements of the LTLB-WFF and is defined by:

(Def. 5) len next f = $\operatorname{len} f$ and for every i such that $1 \leq i \leq \operatorname{len} f$ holds $(\text{next } f)(i) = \mathcal{X}(f_i)$.

We now state a number of propositions:

(6) If $\operatorname{len} f > 0$, then $(\text{conjunction } f)_1 = f_1$.

(7) For every natural number i such that $1 \leq i < \operatorname{len} f$ holds $(\text{conjunction } f)_{i+1} = (\text{conjunction } f)_i \,\&\&\, f_{i+1}$.

(8) For every natural number i such that $i \in \operatorname{dom} f$ holds $(\text{negation}\, f)_i = \neg(f_i)$.

(9) For every natural number i such that $i \in \operatorname{dom} f$ holds $(\text{next}\, f)_i = \mathcal{X}(f_i)$.

(10) $(\text{conjunction}(\varepsilon_{(\text{the LTLB-WFF})}))_{\text{len}\,\text{conjunction}(\varepsilon_{(\text{the LTLB-WFF})})} = \top_t$.

(11) $(\text{conjunction}\langle A\rangle)_{\text{len}\,\text{conjunction}\langle A\rangle} = A$.

(12) For every k such that $n \leq k$ holds $(\text{conjunction}\, f)(n) = (\text{conjunction}(f{\restriction}k))(n)$.

(13) For every k such that $n \leq k$ and $1 \leq n \leq \text{len}\, f$ holds $(\text{conjunction}\, f)_n = (\text{conjunction}(f{\restriction}k))_n$.

(14) $\text{negation}\langle A\rangle = \langle\neg A\rangle$.

(15) $\text{negation}(f \frown \langle A\rangle) = (\text{negation}\, f) \frown \langle\neg A\rangle$.

(16) $\text{negation}(f \frown f_1) = (\text{negation}\, f) \frown \text{negation}\, f_1$.

(17) $\text{VAL}_g((\text{conjunction}(f \frown f_1))_{\text{len}\,\text{conjunction}(f \frown f_1)}) = \text{VAL}_g((\text{conjunction}\, f)_{\text{len}\,\text{conjunction}\, f}) \wedge \text{VAL}_g((\text{conjunction}\, f_1)_{\text{len}\,\text{conjunction}\, f_1})$.

(18) If $n \in \operatorname{dom} f$, then $\text{VAL}_g((\text{conjunction}\, f)_{\text{len}\,\text{conjunction}\, f}) = \text{VAL}_g((\text{conjunction}(f{\restriction}(n -' 1)))_{\text{len}\,\text{conjunction}(f{\restriction}(n-'1))}) \wedge \text{VAL}_g(f_n) \wedge \text{VAL}_g((\text{conjunction}(f_{\downharpoonleft n}))_{\text{len}\,\text{conjunction}(f_{\downharpoonleft n})})$.

(19) $\text{VAL}_g((\text{conjunction}\, f)_{\text{len}\,\text{conjunction}\, f}) = 1$ iff for every natural number i such that $i \in \operatorname{dom} f$ holds $\text{VAL}_g(f_i) = 1$.

(20) $\text{VAL}_g(\neg((\text{conjunction}\,\text{negation}\, f)_{\text{len}\,\text{conjunction}\,\text{negation}\, f})) = 0$ iff for every natural number i such that $i \in \operatorname{dom} f$ holds $\text{VAL}_g(f_i) = 0$.

(21) If $\operatorname{rng} f = \operatorname{rng} f_1$, then $\text{VAL}_g((\text{conjunction}\, f)_{\text{len}\,\text{conjunction}\, f}) = \text{VAL}_g((\text{conjunction}\, f_1)_{\text{len}\,\text{conjunction}\, f_1})$.

3. Classical Tautologies of Temporal Language

Next we state a number of propositions:

(22) $p \Rightarrow \top_t$ is tautologically valid.

(23) $\neg\top_t \Rightarrow p$ is tautologically valid.

(24) $p \Rightarrow p$ is tautologically valid.

(25) $\neg\neg p \Rightarrow p$ is tautologically valid.

(26) $p \Rightarrow \neg\neg p$ is tautologically valid.

(27) $p \,\&\&\, q \Rightarrow p$ is tautologically valid.

(28) $p \,\&\&\, q \Rightarrow q$ is tautologically valid.

(29) For every natural number k such that $k \in \operatorname{dom} f$ holds $f_k \Rightarrow \neg((\text{conjunction}\,\text{negation}\, f)_{\text{len}\,\text{conjunction}\,\text{negation}\, f})$ is tautologically valid.

(30) If $\operatorname{rng} f \subseteq \operatorname{rng} f_1$, then $\neg((\text{conjunction}\,\text{negation}\, f)_{\text{len}\,\text{conjunction}\,\text{negation}\, f}) \Rightarrow \neg((\text{conjunction}\,\text{negation}\, f_1)_{\text{len}\,\text{conjunction}\,\text{negation}\, f_1})$ is tautologically valid.

(31) $\neg(p \Rightarrow q) \Rightarrow p$ is tautologically valid.

(32) $\neg(p \Rightarrow q) \Rightarrow \neg q$ is tautologically valid.

(33) $p \Rightarrow (q \Rightarrow p)$ is tautologically valid.

(34) $p \Rightarrow (q \Rightarrow (p \Rightarrow q))$ is tautologically valid.

(35) $\neg(p \mathbin{\&\&} q) \Rightarrow \neg p \vee \neg q$ is tautologically valid.

(36) $\neg(p \vee q) \Rightarrow \neg p \mathbin{\&\&} \neg q$ is tautologically valid.

(37) $\neg(p \mathbin{\&\&} q) \Rightarrow (p \Rightarrow \neg q)$ is tautologically valid.

(38) $\neg(\top_t \mathbin{\&\&} \neg A) \Rightarrow A$ is tautologically valid.

(39) $\neg(s \mathbin{\&\&} q) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow \neg s))$ is tautologically valid.

(40) $(p \Rightarrow r) \Rightarrow ((p \Rightarrow s) \Rightarrow (p \Rightarrow r \mathbin{\&\&} s))$ is tautologically valid.

(41) $\neg(p \mathbin{\&\&} s) \Rightarrow \neg(r \mathbin{\&\&} s \mathbin{\&\&}(p \mathbin{\&\&} q))$ is tautologically valid.

(42) $\neg(p \mathbin{\&\&} s) \Rightarrow \neg(p \mathbin{\&\&} q \mathbin{\&\&}(r \mathbin{\&\&} s))$ is tautologically valid.

(43) $(p \Rightarrow q \mathbin{\&\&} \neg q) \Rightarrow \neg p$ is tautologically valid.

(44) $(q \Rightarrow p \mathbin{\&\&} r) \Rightarrow ((p \Rightarrow s) \Rightarrow (q \Rightarrow s \mathbin{\&\&} r))$ is tautologically valid.

(45) $(p \Rightarrow q) \Rightarrow ((r \Rightarrow s) \Rightarrow (p \mathbin{\&\&} r \Rightarrow q \mathbin{\&\&} s))$ is tautologically valid.

(46) $(p \Rightarrow q) \Rightarrow ((p \Rightarrow r) \Rightarrow ((r \Rightarrow p) \Rightarrow (r \Rightarrow q)))$ is tautologically valid.

(47) $(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg r) \Rightarrow (p \Rightarrow \neg(q \Rightarrow r)))$ is tautologically valid.

(48) $(p \Rightarrow q \vee r) \Rightarrow ((r \Rightarrow s) \Rightarrow (p \Rightarrow q \vee s))$ is tautologically valid.

(49) $(p \Rightarrow r) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \vee q \Rightarrow r))$ is tautologically valid.

(50) $(r \Rightarrow \mathrm{UN}(p, q)) \Rightarrow ((r \Rightarrow \neg p \mathbin{\&\&} \neg q) \Rightarrow \neg r)$ is tautologically valid.

(51) $(r \Rightarrow \mathrm{UN}(p, q)) \Rightarrow ((r \Rightarrow \neg q \mathbin{\&\&} \neg(p \,\mathcal{U}\, q)) \Rightarrow \neg r)$ is tautologically valid.

4. The Derivations of Temporal Logic Formulas within Classical Logic

One can prove the following propositions:

(52) If $X \vdash p \Rightarrow q$ and $X \vdash p \Rightarrow r$, then $X \vdash p \Rightarrow q \mathbin{\&\&} r$.

(53) If $X \vdash p \Rightarrow q$ and $X \vdash r \Rightarrow s$, then $X \vdash p \mathbin{\&\&} r \Rightarrow q \mathbin{\&\&} s$.

(54) If $X \vdash p \Rightarrow q$ and $X \vdash p \Rightarrow r$ and $X \vdash r \Rightarrow p$, then $X \vdash r \Rightarrow q$.

(55) If $X \vdash p \Rightarrow q \mathbin{\&\&} \neg q$, then $X \vdash \neg p$.

(56) If for every natural number i such that $i \in \mathrm{dom}\, f$ holds
$\emptyset_{\text{the LTLB-WFF}} \vdash p \Rightarrow f_i$, then
$\emptyset_{\text{the LTLB-WFF}} \vdash p \Rightarrow (\text{conjunction}\, f)_{\text{len conjunction}\, f}$.

(57) If for every natural number i such that $i \in \mathrm{dom}\, f$ holds
$\emptyset_{\text{the LTLB-WFF}} \vdash f_i \Rightarrow p$, then
$\emptyset_{\text{the LTLB-WFF}} \vdash \neg((\text{conjunction negation}\, f)_{\text{len conjunction negation}\, f}) \Rightarrow p$.

5. The Derivations of Temporal Logic Formulas

Next we state several propositions:

(58) $X \vdash (\mathcal{X}\, p \Rightarrow \mathcal{X}\, q) \Rightarrow \mathcal{X}(p \Rightarrow q)$.

(59) $X \vdash \mathcal{X}(p \,\&\&\, q) \Rightarrow \mathcal{X}\, p \,\&\&\, \mathcal{X}\, q$.

(60) $\emptyset_{\text{the LTLB-WFF}} \vdash (\text{conjunction}\,\text{next}\, f)_{\text{len}\,\text{conjunction}\,\text{next}\, f} \Rightarrow \mathcal{X}((\text{conjunction}\, f)_{\text{len}\,\text{conjunction}\, f})$.

(61) $X \vdash \mathcal{X}\, p \vee \mathcal{X}\, q \Rightarrow \mathcal{X}(p \vee q)$.

(62) $X \vdash \mathcal{X}(p \vee q) \Rightarrow \mathcal{X}\, p \vee \mathcal{X}\, q$.

(63) $X \vdash \neg(A\, \mathcal{U}\, B) \Rightarrow \mathcal{X} \neg\, \text{UN}(A, B)$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[9] Mariusz Giero. The axiomatization of propositional linear time temporal logic. *Formalized Mathematics*, 19(**2**):113–119, 2011, doi: 10.2478/v10037-011-0018-1.
[10] Adam Grabowski. Hilbert positive propositional calculus. *Formalized Mathematics*, 8(**1**):69–72, 1999.
[11] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.
[12] Fred Kröger and Stephan Merz. *Temporal Logic and State Systems.* Springer-Verlag, 2008.
[13] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[14] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[15] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 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.

Received May 7, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 3, Pages 221–226, 2012
DOI: 10.2478/v10037-012-0026-9

VERSITA
versita.com/fm/

The Properties of Sets of Temporal Logic Subformulas[1]

Mariusz Giero[2]
Department of Logic, Informatics and Philosophy of Science
University of Białystok
Plac Uniwersytecki 1, 15-420 Białystok, Poland

Summary. This is a second preliminary article to prove the completeness theorem of an extension of basic propositional temporal logic. We base it on the proof of completeness for basic propositional temporal logic given in [17]. We introduce two modified definitions of a subformula. In the former one we treat until-formula as indivisible. In the latter one, we extend the set of subformulas of until-formulas by a special disjunctive formula. This is needed to construct a temporal model. We also define an ordered positive-negative pair of finite sequences of formulas (PNP). PNPs represent states of a temporal model.

MML identifier: `LTLAXIO3`, version: `7.14.01 4.183.1153`

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

1. Preliminaries

For simplicity, we adopt the following convention: A, B, p, q, r are elements of the LTLB-WFF, n is an element of $\mathbb{N}$, X is a subset of the LTLB-WFF, g is a function from the LTLB-WFF into *Boolean*, and x is a set.

Next we state two propositions:

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

[2] I would like to thank Prof. Andrzej Trybulec, Dr. Artur Korniłowicz, Dr. Adam Naumowicz and Karol Pąk for their help in preparation of the article.

ISSN 1426–2630(p), 1898-9934(e)

(1) Let X be a non empty set, t be a finite sequence of elements of X, and k be a natural number. If $k+1 \leq \operatorname{len} t$, then $t_{\restriction k} = \langle t(k+1)\rangle \frown (t_{\restriction k+1})$.

(2) $\mathbb{N} \longmapsto \emptyset$ is a LTL Model.

Let us consider X. We say that X is without implication if and only if:

(Def. 1) For every p such that $p \in X$ holds p is not conditional.

Let D be a set. The functor D^{*}_{1-1} yielding a set is defined by:

(Def. 2) For every x holds $x \in D^{*}_{1-1}$ iff x is a one-to-one finite sequence of elements of D.

Let D be a set. One can verify that D^{*}_{1-1} is non empty.

Let D be a finite set. Observe that D^{*}_{1-1} is finite.

We now state the proposition

(3) For all sets D_1, D_2 such that $D_1 \subseteq D_2$ holds $D_{1}{}^{*}_{1-1} \subseteq D_{2}{}^{*}_{1-1}$.

Let a_1 be a set and let a_2 be a subset of a_1. Then $a_{2}{}^{*}_{1-1}$ is a non empty subset of $a_{1}{}^{*}_{1-1}$.

Next we state the proposition

(4) For all one-to-one finite sequences F, G such that $\operatorname{rng} F$ misses $\operatorname{rng} G$ holds $F \frown G$ is one-to-one.

Let X be a set and let f, g be one-to-one finite sequences of elements of X. Let us assume that $\operatorname{rng} f$ misses $\operatorname{rng} g$. The functor $f \frown g$ yielding a one-to-one finite sequence of elements of X is defined as follows:

(Def. 3) $f \frown g = f \frown g$.

2. Set of Subformulas where an Until-formula is treated as Indivisible and its Properties

The function $\dot{\tau}$ from the LTLB-WFF into $2^{\text{the LTLB-WFF}}$ is defined as follows:

(Def. 4) $\dot{\tau}(\bot_t) = \{\bot_t\}$ and $\dot{\tau}(\operatorname{prop} n) = \{\operatorname{prop} n\}$ and $\dot{\tau}(A \Rightarrow B) = \{A \Rightarrow B\} \cup \dot{\tau}(A) \cup \dot{\tau}(B)$ and $\dot{\tau}(A\,\mathcal{U}\,B) = \{A\,\mathcal{U}\,B\}$.

One can prove the following propositions:

(5) If A is not conditional, then $\dot{\tau}(A) = \{A\}$.

(6) $p \in \dot{\tau}(p)$.

Let us consider p. Observe that $\dot{\tau}(p)$ is non empty and finite.

One can prove the following propositions:

(7) If $p \Rightarrow q \in \dot{\tau}(r)$, then $p, q \in \dot{\tau}(r)$.

(8) If $p \in \dot{\tau}(q)$, then $\dot{\tau}(p) \subseteq \dot{\tau}(q)$.

(9) If $p\,\mathcal{U}\,q \in \dot{\tau}(\neg A)$, then $p\,\mathcal{U}\,q \in \dot{\tau}(A)$.

(10) If $p\,\mathcal{U}\,q \in \dot{\tau}(A \,\&\&\, B)$, then $p\,\mathcal{U}\,q \in \dot{\tau}(A)$ or $p\,\mathcal{U}\,q \in \dot{\tau}(B)$.

(11) If $p \in \dot{\tau}(q)$ and $p \neq q$, then $\operatorname{len} p < \operatorname{len} q$.

(12) $\dot{\tau}(p) \subseteq \dot{\tau}(\neg p)$.

(13) $\dot{\tau}(q) \subseteq \dot{\tau}(p \mathbin{\&\&} q)$.

(14) $\dot{\tau}(q) \subseteq \dot{\tau}(p \vee q)$.

Let us consider X. The functor $\tau(X)$ yields a subset of the LTLB-WFF and is defined as follows:

(Def. 5) $x \in \tau(X)$ iff there exists A such that $A \in X$ and $x \in \dot{\tau}(A)$.

We now state two propositions:

(15) $\tau(X) = \bigcup\{\dot{\tau}(p); p$ ranges over elements of the LTLB-WFF: $p \in X\}$.

(16) $X \subseteq \tau(X)$.

Let X be an empty subset of the LTLB-WFF. One can check that $\tau(X)$ is empty.

Let X be a finite subset of the LTLB-WFF. Note that $\tau(X)$ is finite.

Let X be a non empty subset of the LTLB-WFF. One can verify that $\tau(X)$ is non empty.

The following propositions are true:

(17) $\tau(\tau(X)) = \tau(X)$.

(18) If X is without implication, then $\tau(X) = X$.

(19) If $p \Rightarrow q \in \tau(X)$, then p, $q \in \tau(X)$.

(20) If $p \mathbin{\&\&} q \in \tau(X)$, then p, $q \in \tau(X)$.

(21) If $p \vee q \in \tau(X)$, then p, $q \in \tau(X)$.

(22) If $\mathrm{UN}(p, q) \in \tau(X)$, then p, q, $p \,\mathcal{U}\, q \in \tau(X)$.

(23) If $p \in \tau(X)$, then $\dot{\tau}(p) \subseteq \tau(X)$.

3. Extended Set of Subformulas and its Properties

The function $\dot{\sigma}$ from the LTLB-WFF into $2^{\text{the LTLB-WFF}}$ is defined by:

(Def. 6) $\dot{\sigma}(\bot_t) = \{\bot_t\}$ and $\dot{\sigma}(\mathrm{prop}\, n) = \{\mathrm{prop}\, n\}$ and $\dot{\sigma}(A \Rightarrow B) = \{A \Rightarrow B\} \cup \dot{\sigma}(A) \cup \dot{\sigma}(B)$ and $\dot{\sigma}(A \,\mathcal{U}\, B) = \dot{\tau}(\mathrm{UN}(A, B)) \cup \dot{\sigma}(A) \cup \dot{\sigma}(B)$.

One can prove the following propositions:

(24) $p \,\mathcal{U}\, q \in \dot{\sigma}(p \,\mathcal{U}\, q)$.

(25) $\dot{\tau}(p) \subseteq \dot{\sigma}(p)$.

Let us consider p. Note that $\dot{\sigma}(p)$ is non empty and finite.

The following proposition is true

(26) If $p \in \dot{\sigma}(A \,\mathcal{U}\, B)$, then if $A \,\mathcal{U}\, B \in \dot{\sigma}(q)$, then $p \in \dot{\sigma}(q)$.

Let us consider X. The functor $\sigma(X)$ yielding a subset of $2^{\text{the LTLB-WFF}}$ is defined as follows:

(Def. 7) $\sigma(X) = \{\dot{\sigma}(A); A$ ranges over elements of the LTLB-WFF: $A \in X\}$.

Let X be a finite subset of the LTLB-WFF. Note that $\sigma(X)$ is finite and finite-membered.

4. An Ordered Pair of Finite Sequences of Formulas. PNP-formula, Consistent PNP and Complete PNP

A positive-negative pair is an element of
(the LTLB-WFF)$^*_{1-1}$ × (the LTLB-WFF)$^*_{1-1}$.

In the sequel P, Q, P_1, R are positive-negative pairs.

Let us consider P. Then $P_{\mathbf{1}}$ is a one-to-one finite sequence of elements of the LTLB-WFF. Then $P_{\mathbf{2}}$ is a one-to-one finite sequence of elements of the LTLB-WFF.

Let us consider P. The functor $\operatorname{rng} P$ yielding a finite subset of the LTLB-WFF is defined by:

(Def. 8) $\operatorname{rng} P = \operatorname{rng}(P_{\mathbf{1}}) \cup \operatorname{rng}(P_{\mathbf{2}})$.

Let f_1, f_2 be one-to-one finite sequences of elements of the LTLB-WFF. Then $\langle f_1, f_2 \rangle$ is a positive-negative pair.

Let us consider P. The functor $\widehat{P}$ yielding an element of the LTLB-WFF is defined by:

(Def. 9) $\widehat{P} = (\text{conjunction}(P_{\mathbf{1}}))_{\text{len conjunction}(P_{\mathbf{1}})}$
$\&\&(\text{conjunction negation}(P_{\mathbf{2}}))_{\text{len conjunction negation}(P_{\mathbf{2}})}$.

We now state three propositions:

(27) $\widehat{F} = \top_t \,\&\&\, \top_t$, where $F = \langle \varepsilon_{(\text{the LTLB-WFF})}, \varepsilon_{(\text{the LTLB-WFF})} \rangle$.

(28) If $A \in \operatorname{rng}(P_{\mathbf{1}})$, then $\emptyset_{\text{the LTLB-WFF}} \vdash \widehat{P} \Rightarrow A$.

(29) If $A \in \operatorname{rng}(P_{\mathbf{2}})$, then $\emptyset_{\text{the LTLB-WFF}} \vdash \widehat{P} \Rightarrow \neg A$.

Let us consider P. We say that P is inconsistent if and only if:

(Def. 10) $\emptyset_{\text{the LTLB-WFF}} \vdash \neg\widehat{P}$.

Let us consider P. We introduce P is consistent as an antonym of P is inconsistent.

We say that P is complete if and only if:

(Def. 11) $\tau(\operatorname{rng} P) = \operatorname{rng} P$.

One can check that $\langle \varepsilon_{(\text{the LTLB-WFF})}, \varepsilon_{(\text{the LTLB-WFF})} \rangle$ is consistent as a positive-negative pair.

Let us observe that $\langle \varepsilon_{(\text{the LTLB-WFF})}, \varepsilon_{(\text{the LTLB-WFF})} \rangle$ is complete as a positive-negative pair.

One can check that there exists a positive-negative pair which is consistent and complete.

Let P be a consistent positive-negative pair. Observe that $\langle P_{\mathbf{1}}, P_{\mathbf{2}} \rangle$ is consistent as a positive-negative pair.

5. The Properties of Consistent PNPs

One can prove the following propositions:

(30) For every consistent positive-negative pair P holds $\operatorname{rng}(P_{\mathbf{1}})$ misses $\operatorname{rng}(P_{\mathbf{2}})$.

(31) Let P be a consistent positive-negative pair. If $A \notin \operatorname{rng} P$, then $\langle (P_{\mathbf{1}}) ^\frown \langle A \rangle, P_{\mathbf{2}} \rangle$ is consistent or $\langle P_{\mathbf{1}}, (P_{\mathbf{2}}) ^\frown \langle A \rangle \rangle$ is consistent.

(32) For every consistent positive-negative pair P holds $\perp_t \notin \operatorname{rng}(P_{\mathbf{1}})$.

(33) Let P be a consistent positive-negative pair. Suppose A, B, $A \Rightarrow B \in \operatorname{rng} P$. Then $A \Rightarrow B \in \operatorname{rng}(P_{\mathbf{1}})$ if and only if $A \in \operatorname{rng}(P_{\mathbf{2}})$ or $B \in \operatorname{rng}(P_{\mathbf{1}})$.

(34) Let P be a consistent positive-negative pair. Then there exists a consistent positive-negative pair P_1 such that $\operatorname{rng}(P_{\mathbf{1}}) \subseteq \operatorname{rng}((P_1)_{\mathbf{1}})$ and $\operatorname{rng}(P_{\mathbf{2}}) \subseteq \operatorname{rng}((P_1)_{\mathbf{2}})$ and $\tau(\operatorname{rng} P) = \operatorname{rng} P_1$.

References

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

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

[3] Grzegorz Bancerek. Introduction to trees. *Formalized Mathematics*, 1(**2**):421–427, 1990.

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

[5] Grzegorz Bancerek. König's lemma. *Formalized Mathematics*, 2(**3**):397–402, 1991.

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

[7] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

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

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

[10] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

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

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

[13] Mariusz Giero. The axiomatization of propositional linear time temporal logic. *Formalized Mathematics*, 19(**2**):113–119, 2011, doi: 10.2478/v10037-011-0018-1.

[14] Mariusz Giero. The derivations of temporal logic formulas. *Formalized Mathematics*, 20(**3**):215–219, 2012, doi: 10.2478/v10037-012-0025-x.

[15] Adam Grabowski. Hilbert positive propositional calculus. *Formalized Mathematics*, 8(**1**):69–72, 1999.

[16] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.

[17] Fred Kröger and Stephan Merz. *Temporal Logic and State Systems*. Springer-Verlag, 2008.

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

[19] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[20] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

[21] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

[22] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

[23] Andrzej Trybulec. Defining by structural induction in the positive propositional language. *Formalized Mathematics*, 8(**1**):133–137, 1999.

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

[25] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

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

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

Received May 7, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 3, Pages 227–234, 2012
DOI: 10.2478/v10037-012-0027-8

VERSITA
versita.com/fm/

Weak Completeness Theorem for Propositional Linear Time Temporal Logic[1]

Mariusz Giero[2]
Department of Logic, Informatics and Philosophy of Science
University of Białystok
Plac Uniwersytecki 1, 15-420 Białystok, Poland

Summary. We prove weak (finite set of premises) completeness theorem for extended propositional linear time temporal logic with irreflexive version of until-operator. We base it on the proof of completeness for basic propositional linear time temporal logic given in [20] which roughly follows the idea of the Henkin-Hasenjaeger method for classical logic. We show that a temporal model exists for every formula which negation is not derivable (Satisfiability Theorem). The contrapositive of that theorem leads to derivability of every valid formula. We build a tree of consistent and complete PNPs which is used to construct the model.

MML identifier: `LTLAXIO4`, version: `7.14.01 4.183.1153`

The papers [25], [14], [28], [21], [4], [1], [30], [11], [26], [31], [13], [24], [2], [3], [5], [6], [7], [12], [15], [9], [23], [8], [10], [19], [27], [29], [22], [16], [17], and [18] provide the notation and terminology for this paper.

[1] The author is the winner of the Mizar Prize for Young Researchers in 2012 for this article. This work has been supported by the Polish Ministry of Science and Higher Education project "Managing a Large Repository of Computer-verified Mathematical Knowledge" (N N519 385136).

[2] I would like to thank Prof. Dr. Stephan Merz for valuable hints which helped me to prove the theorem. I would particularly like to thank Dr. Artur Korniłowicz who patiently answered a lot of my questions regarding writing this article. I would like to thank Dr. Josef Urban for discussions and encouragement to write the article. I would like to thank Prof. Andrzej Trybulec, Dr. Adam Naumowicz, Dr. Grzegorz Bancerek and Karol Pąk for their help in preparation of the article.

ISSN 1426–2630(p), 1898-9934(e)

1. Preliminaries

For simplicity, we use the following convention: A, B, p, q denote elements of the LTLB-WFF, M denotes a LTL Model, j, k, n denote elements of $\mathbb{N}$, i denotes a natural number, X denotes a subset of the LTLB-WFF, F denotes a finite subset of the LTLB-WFF, f denotes a finite sequence of elements of the LTLB-WFF, and P, Q, R denote positive-negative pairs.

Let X be a finite set. We see that the enumeration of X is a one-to-one finite sequence of elements of X.

Let E be a set and let F be a finite subset of E. We see that the enumeration of F is a one-to-one finite sequence of elements of E.

Let D be a set. One can verify that there exists a set of finite sequences of D which is non empty and finite.

We now state the proposition

(1) Let X be a set and G be a non empty finite set of finite sequences of X. Then there exists a finite sequence A such that $A \in G$ and for every finite sequence B such that $B \in G$ holds $\operatorname{len} B \leq \operatorname{len} A$.

Let T be a decorated tree, let us consider n, and let t be a node of T. Then $t{\restriction}n$ is a node of T.

We now state the proposition

(2) p is a finite sequence of elements of $\mathbb{N}$.

Let us consider A. We introduce A is s-until as a synonym of A is conjunctive.

Let us consider A. Let us assume that A is s-until. The right argument of A yields an element of the LTLB-WFF and is defined by:

(Def. 1) There exists p such that $p\,\mathcal{U}$ the right argument of $A = A$.

Let us consider A. We say that A is satisfiable if and only if:

(Def. 2) There exist M, n such that $\mathrm{SAT}_M(\langle n, A\rangle) = 1$.

We now state four propositions:

(3) $\emptyset_{\text{the LTLB-WFF}} \models A$ iff $\neg A$ is not satisfiable.

(4) If $\top_t \mathbin{\&\&} A$ is satisfiable, then A is satisfiable.

(5) Let i be an element of $\mathbb{N}$. Then $\mathrm{SAT}_M(\langle i, p\,\mathcal{U}\,q\rangle) = 1$ if and only if there exists j such that $j > i$ and $\mathrm{SAT}_M(\langle j, q\rangle) = 1$ and for every k such that $i < k < j$ holds $\mathrm{SAT}_M(\langle k, p\rangle) = 1$.

(6) $\mathrm{SAT}_M(\langle n, (\text{conjunction}\, f)_{\text{len conjunction}\, f}\rangle) = 1$ iff for every i such that $i \in \operatorname{dom} f$ holds $\mathrm{SAT}_M(\langle n, f_i\rangle) = 1$.

One can prove the following three propositions:

(7) $\widehat{W} = \top_t \mathbin{\&\&} \neg A$, where $W = \langle \varepsilon_{(\text{the LTLB-WFF})}, \langle A\rangle\rangle$.

(8) For every complete positive-negative pair P such that $\mathrm{UN}(A, B) \in \operatorname{rng} P$ holds A, B, $A\,\mathcal{U}\,B \in \operatorname{rng} P$.

(9) $\operatorname{rng} P \subseteq \bigcup \sigma(\operatorname{rng} P)$.

2. Set of PNP-formulas. Completions of Formulas and PNPs

In the sequel P is an element of (the LTLB-WFF)$^*_{1-1}\times$(the LTLB-WFF)$^*_{1-1}$.

Let F be a subset of (the LTLB-WFF)$^*_{1-1}\times$(the LTLB-WFF)$^*_{1-1}$. The functor $\widehat{F}$ yields a subset of the LTLB-WFF and is defined by:

(Def. 3) $\widehat{F} = \{\widehat{P} : P \in F\}$.

Let F be a non empty subset of (the LTLB-WFF)$^*_{1-1}\times$(the LTLB-WFF)$^*_{1-1}$. Note that $\widehat{F}$ is non empty.

Let F be a finite subset of (the LTLB-WFF)$^*_{1-1}$ $\times$ (the LTLB-WFF)$^*_{1-1}$. Observe that $\widehat{F}$ is finite.

We now state the proposition

(10) For all subsets F, G of (the LTLB-WFF)$^*_{1-1}$ $\times$ (the LTLB-WFF)$^*_{1-1}$ holds $\widehat{F \cup G} = \widehat{F} \cup \widehat{G}$.

One can prove the following proposition

(11) $\widehat{W} = \{\top_t \,\&\&\, \top_t\}$, where $W = \{\langle \varepsilon_{(\text{the LTLB-WFF})}, \varepsilon_{(\text{the LTLB-WFF})}\rangle\}$.

In the sequel Q denotes a positive-negative pair.

Let F be a finite subset of the LTLB-WFF. The functor comp F yielding a non empty finite subset of (the LTLB-WFF)$^*_{1-1}$ $\times$ (the LTLB-WFF)$^*_{1-1}$ is defined as follows:

(Def. 4) $\operatorname{comp} F = \{Q : \operatorname{rng} Q = \tau(F) \ \wedge\ \operatorname{rng}(Q_{\mathbf{1}}) \text{ misses } \operatorname{rng}(Q_{\mathbf{2}})\}$.

Let F be a finite subset of the LTLB-WFF. Note that every element of comp F is complete.

One can prove the following proposition

(12) $\operatorname{comp}(\emptyset_{\text{the LTLB-WFF}}) = \{\langle \varepsilon_{(\text{the LTLB-WFF})}, \varepsilon_{(\text{the LTLB-WFF})}\rangle\}$.

Let us consider P, Q. We say that Q is completion of P if and only if:

(Def. 5) $\operatorname{rng}(P_{\mathbf{1}}) \subseteq \operatorname{rng}(Q_{\mathbf{1}})$ and $\operatorname{rng}(P_{\mathbf{2}}) \subseteq \operatorname{rng}(Q_{\mathbf{2}})$ and $\tau(\operatorname{rng} P) = \operatorname{rng} Q$.

We now state the proposition

(13) If Q is completion of P, then Q is complete.

In the sequel Q is a consistent positive-negative pair.

Let us consider P. The functor comp P yields a finite subset of (the LTLB-WFF)$^*_{1-1}$ $\times$ (the LTLB-WFF)$^*_{1-1}$ and is defined by:

(Def. 6) $\operatorname{comp} P = \{Q : Q \text{ is completion of } P\}$.

Let P be a consistent positive-negative pair. One can check that comp P is non empty. Observe that every element of comp P is consistent.

In the sequel P denotes an element of (the LTLB-WFF)$^*_{1-1}$ $\times$ (the LTLB-WFF)$^*_{1-1}$.

Let X be a subset of (the LTLB-WFF)$^*_{1-1}\times$(the LTLB-WFF)$^*_{1-1}$. The functor comp X yields a subset of (the LTLB-WFF)$^*_{1-1}$ $\times$ (the LTLB-WFF)$^*_{1-1}$ and is defined by:

(Def. 7) $\operatorname{comp} X = \bigcup\{\operatorname{comp} P : P \in X\}$.

Let X be a finite subset of (the LTLB-WFF)$^*_{1-1}$ × (the LTLB-WFF)$^*_{1-1}$. One can check that $\operatorname{comp} X$ is finite.

We now state four propositions:

(14) For every non empty subset X of (the LTLB-WFF)$^*_{1-1}$ × (the LTLB-WFF)$^*_{1-1}$ such that $Q \in X$ holds $\operatorname{comp} Q \subseteq \operatorname{comp} X$.

(15) For every non empty finite subset F of the LTLB-WFF there exists p such that $p \in \tau(F)$ and $\tau(\tau(F) \setminus \{p\}) = \tau(F) \setminus \{p\}$.

(16) Let F be a finite subset of the LTLB-WFF and f be a finite sequence of elements of the LTLB-WFF. If $\operatorname{rng} f = \widehat{\operatorname{comp} F}$, then $\emptyset_{\text{the LTLB-WFF}} \vdash \neg((\text{conjunction negation}\, f)_{\text{len conjunction negation}\, f})$.

(17) Let P be a consistent positive-negative pair and f be a finite sequence of elements of the LTLB-WFF. If $\operatorname{rng} f = \widehat{\operatorname{comp} P}$, then $\emptyset_{\text{the LTLB-WFF}} \vdash \widehat{P} \Rightarrow \neg((\text{conjunction negation}\, f)_{\text{len conjunction negation}\, f})$.

3. Set of Possible Next-State PNPs

In the sequel A, B denote elements of the LTLB-WFF.

Let us consider X. The functor $\mathrm{UN}(X)$ yields a subset of the LTLB-WFF and is defined as follows:

(Def. 8) $\mathrm{UN}(X) = \{\mathrm{UN}(A, B) : A\, \mathcal{U}\, B \in X\}$.

Let X be a finite subset of the LTLB-WFF. One can check that $\mathrm{UN}(X)$ is finite.

Let us consider P. The functor $\mathrm{UN}(P)$ yielding a non empty finite subset of (the LTLB-WFF)$^*_{1-1}$ × (the LTLB-WFF)$^*_{1-1}$ is defined by:

(Def. 9) $\mathrm{UN}(P) = \{Q; Q$ ranges over positive-negative pairs: $\operatorname{rng}(Q_{\mathbf{1}}) = \mathrm{UN}(\operatorname{rng}(P_{\mathbf{1}})) \wedge \operatorname{rng}(Q_{\mathbf{2}}) = \mathrm{UN}(\operatorname{rng}(P_{\mathbf{2}}))\}$.

One can prove the following proposition

(18) For every element Q of $\mathrm{UN}(P)$ holds $\emptyset_{\text{the LTLB-WFF}} \vdash \widehat{P} \Rightarrow \mathcal{X}\, \widehat{Q}$.

Let P be a consistent positive-negative pair. Note that every element of $\mathrm{UN}(P)$ is consistent. In the sequel Q denotes an element of (the LTLB-WFF)$^*_{1-1}$ × (the LTLB-WFF)$^*_{1-1}$.

Let us consider P. The next completion of P yielding a finite subset of (the LTLB-WFF)$^*_{1-1}$ × (the LTLB-WFF)$^*_{1-1}$ is defined by:

(Def. 10) The next completion of $P = \{Q : Q \in \operatorname{comp} \mathrm{UN}(P)\}$.

Let P be a consistent positive-negative pair. One can verify that the next completion of P is non empty.

Let P be a consistent positive-negative pair. One can check that every element of the next completion of P is consistent.

Next we state two propositions:

(19) If $Q \in$ the next completion of P and $R \in \mathrm{UN}(P)$, then Q is completion of R.

(20) If $Q \in$ the next completion of P, then Q is complete.

Let P be a consistent positive-negative pair. One can verify that every element of the next completion of P is complete.

Next we state several propositions:

(21) If $A\,\mathcal{U}\,B \in \mathrm{rng}(P_{\mathbf{2}})$ and $Q \in$ the next completion of P, then $\mathrm{UN}(A, B) \in \mathrm{rng}(Q_{\mathbf{2}})$.

(22) If $A\,\mathcal{U}\,B \in \mathrm{rng}(P_{\mathbf{1}})$ and $Q \in$ the next completion of P, then $\mathrm{UN}(A, B) \in \mathrm{rng}(Q_{\mathbf{1}})$.

(23) If $R \in$ the next completion of Q and $\mathrm{rng}\,Q \subseteq \bigcup\sigma(\mathrm{rng}\,P)$, then $\mathrm{rng}\,R \subseteq \bigcup\sigma(\mathrm{rng}\,P)$.

(24) Let P be a consistent complete positive-negative pair and Q be an element of the next completion of P. If $A\,\mathcal{U}\,B \in \mathrm{rng}(P_{\mathbf{2}})$, then $B \in \mathrm{rng}(Q_{\mathbf{2}})$ but $A \in \mathrm{rng}(Q_{\mathbf{2}})$ or $A\,\mathcal{U}\,B \in \mathrm{rng}(Q_{\mathbf{2}})$.

(25) Let P be a consistent complete positive-negative pair and Q be an element of the next completion of P. If $A\,\mathcal{U}\,B \in \mathrm{rng}(P_{\mathbf{1}})$, then $B \in \mathrm{rng}(Q_{\mathbf{1}})$ or A, $A\,\mathcal{U}\,B \in \mathrm{rng}(Q_{\mathbf{1}})$.

4. A PNP-Tree and its Properties

Let us consider P. A finite-branching tree decorated with elements of (the LTLB-WFF)$^*_{1-1}$ × (the LTLB-WFF)$^*_{1-1}$ is said to be a tree of positive-negative pairs of P if it satisfies the conditions (Def. 11).

(Def. 11)(i) $\mathrm{It}(\emptyset) = P$, and

(ii) for every element t of $\mathrm{dom}\,\mathrm{it}$ and for every element w of (the LTLB-WFF)$^*_{1-1}$ × (the LTLB-WFF)$^*_{1-1}$ such that $w = \mathrm{it}(t)$ holds $\mathrm{succ}(\mathrm{it}, t) =$ the enumeration of the next completion of w.

In the sequel T is a tree of positive-negative pairs of P and t is a node of T.

Let us consider P, T, t. Then $T{\restriction}t$ is a tree of positive-negative pairs of $T(t)$.

Next we state two propositions:

(26) For every natural number n such that $t \mathbin{^\frown} \langle n \rangle \in \mathrm{dom}\,T$ holds $T(t \mathbin{^\frown} \langle n \rangle) \in$ the next completion of $T(t)$.

(27) If $Q \in \mathrm{rng}\,T$, then $\mathrm{rng}\,Q \subseteq \bigcup\sigma(\mathrm{rng}\,P)$.

Let us consider P, T. One can check that $\mathrm{rng}\,T$ is non empty and finite.

Let P be a consistent positive-negative pair and let T be a tree of positive-negative pairs of P. One can check that every element of $\mathrm{rng}\,T$ is consistent.

Let P be a consistent complete positive-negative pair and let T be a tree of positive-negative pairs of P. One can verify that every element of $\operatorname{rng} T$ is complete.

Let P be a consistent complete positive-negative pair, let T be a tree of positive-negative pairs of P, and let t be a node of T. Observe that $T(t)$ is consistent and complete as a positive-negative pair.

Let P be a consistent positive-negative pair, let T be a tree of positive-negative pairs of P, and let t be an element of $\operatorname{dom} T$. Observe that $\operatorname{succ} t$ is non empty.

Let us consider P, T. The range of T except the root node yields a finite subset of $(\text{the LTLB-WFF})^{*}_{1-1} \times (\text{the LTLB-WFF})^{*}_{1-1}$ and is defined as follows:

(Def. 12) The range of T except the root node $= \{T(t); t$ ranges over nodes of T: $t \neq \emptyset\}$.

Let P be a consistent positive-negative pair and let T be a tree of positive-negative pairs of P. One can verify that the range of T except the root node is non empty.

One can prove the following proposition

(28) If $R \in \operatorname{rng} T$ and $Q \in \mathrm{UN}(R)$, then $\operatorname{comp} Q \subseteq$ the range of T except the root node.

One can prove the following proposition

(29) Let P be a consistent complete positive-negative pair, T be a tree of positive-negative pairs of P, and f be a finite sequence of elements of the LTLB-WFF. If $\operatorname{rng} f = \widehat{J}$, then $\emptyset_{\text{the LTLB-WFF}} \vdash \neg((\text{conjunction negation } f)_{\text{len conjunction negation } f}) \Rightarrow \mathcal{X} \neg((\text{conjunction negation } f)_{\text{len conjunction negation } f})$, where $J =$ the range of T except the root node.

5. A Path in PNP-Tree and its Properties. Existence of Temporal Model for a Consistent PNP. Weak Completeness Theorem

Let P be a consistent positive-negative pair and let T be a tree of positive-negative pairs of P. A sequence of $\operatorname{dom} T$ is called a path of T if:

(Def. 13) $\mathrm{It}(0) = \emptyset$ and for every natural number k holds $\mathrm{it}(k+1) \in \operatorname{succ} \mathrm{it}(k)$.

Let P be a consistent complete positive-negative pair, let T be a tree of positive-negative pairs of P, let t be a path of T, and let us consider i. Then $t(i)$ is a node of T.

Next we state three propositions:

(30) Let P be a consistent complete positive-negative pair, T be a tree of positive-negative pairs of P, and t be a path of T. Suppose $A \,\mathcal{U}\, B \in \operatorname{rng}(T(t(i))_{\mathbf{2}})$. Let given j. If $j > i$, then $B \in \operatorname{rng}(T(t(j))_{\mathbf{2}})$ or there exists k such that $i < k < j$ and $A \in \operatorname{rng}(T(t(k))_{\mathbf{2}})$.

(31) Let P be a consistent complete positive-negative pair and T be a tree of positive-negative pairs of P. Suppose $A \,\mathcal{U}\, B \in \mathrm{rng}(P_{\mathbf{1}})$ and for every element Q of the range of T except the root node holds $B \notin \mathrm{rng}(Q_{\mathbf{1}})$. Let Q be an element of the range of T except the root node. Then $B \in \mathrm{rng}(Q_{\mathbf{2}})$ and $A \,\mathcal{U}\, B \in \mathrm{rng}(Q_{\mathbf{1}})$.

(32) Let P be a consistent complete positive-negative pair and T be a tree of positive-negative pairs of P. Suppose $A \,\mathcal{U}\, B \in \mathrm{rng}(P_{\mathbf{1}})$. Then there exists an element R of the range of T except the root node such that $B \in \mathrm{rng}(R_{\mathbf{1}})$.

Let P be a consistent positive-negative pair, let T be a tree of positive-negative pairs of P, and let t be a path of T. We say that t is complete if and only if the condition (Def. 14) is satisfied.

(Def. 14) Let given i. Suppose $A \,\mathcal{U}\, B \in \mathrm{rng}(T(t(i))_{\mathbf{1}})$. Then there exists j such that $j > i$ and $B \in \mathrm{rng}(T(t(j))_{\mathbf{1}})$ and for every k such that $i < k < j$ holds $A \in \mathrm{rng}(T(t(k))_{\mathbf{1}})$.

Let P be a consistent complete positive-negative pair and let T be a tree of positive-negative pairs of P. Note that there exists a path of T which is complete.

Let P be a consistent positive-negative pair. Observe that $\widehat{P}$ is satisfiable.

One can prove the following proposition

(33)[3] If $F \models A$, then $F \vdash A$.

References

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

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

[3] Grzegorz Bancerek. Introduction to trees. *Formalized Mathematics*, 1(**2**):421–427, 1990.

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

[5] Grzegorz Bancerek. König's lemma. *Formalized Mathematics*, 2(**3**):397–402, 1991.

[6] Grzegorz Bancerek. Joining of decorated trees. *Formalized Mathematics*, 4(**1**):77–82, 1993.

[7] Grzegorz Bancerek. Subtrees. *Formalized Mathematics*, 5(**2**):185–190, 1996.

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

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

[10] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

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

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

[13] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

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

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

[3] Weak completeness theorem of basic propositional linear temporal logic extended with $\mathcal{U}$ operator (LTLB).

[16] Mariusz Giero. The axiomatization of propositional linear time temporal logic. *Formalized Mathematics*, 19(**2**):113–119, 2011, doi: 10.2478/v10037-011-0018-1.

[17] Mariusz Giero. The derivations of temporal logic formulas. *Formalized Mathematics*, 20(**3**):215–219, 2012, doi: 10.2478/v10037-012-0025-x.

[18] Mariusz Giero. The properties of sets of temporal logic subformulas. *Formalized Mathematics*, 20(**3**):221–226, 2012, doi: 10.2478/v10037-012-0026-9.

[19] Adam Grabowski. Hilbert positive propositional calculus. *Formalized Mathematics*, 8(**1**):69–72, 1999.

[20] Fred Kröger and Stephan Merz. *Temporal Logic and State Systems*. Springer-Verlag, 2008.

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

[22] Karol Pąk. Continuity of barycentric coordinates in Euclidean topological spaces. *Formalized Mathematics*, 19(**3**):139–144, 2011, doi: 10.2478/v10037-011-0022-5.

[23] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[24] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

[25] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

[26] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

[27] Andrzej Trybulec. Defining by structural induction in the positive propositional language. *Formalized Mathematics*, 8(**1**):133–137, 1999.

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

[29] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

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

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

Received May 7, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 3, Pages 235–237, 2012
DOI: 10.2478/v10037-012-0028-7

VERSITA
versita.com/fm/

The Friendship Theorem[1]

Karol Pąk
Institute of Informatics
University of Białystok
Poland

Summary. In this article we prove the friendship theorem according to the article [1], which states that if a group of people has the property that any pair of persons have exactly one common friend, then there is a universal friend, i.e. a person who is a friend of every other person in the group.

MML identifier: FRIENDS1, version: 7.15.01 4.184.1155

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

1. Preliminaries

For simplicity, we adopt the following rules: x, y, z are sets, i, k, n are natural numbers, R is a binary relation, P is a finite binary relation, and p, q are finite sequences.

Let us consider P, x. Observe that $P^{\circ}x$ is finite.

We now state several propositions:

(1) $\overline{\overline{R}} = \overline{\overline{R^{\smile}}}$.

(2) If R is symmetric, then $R^{\circ}x = R^{-1}(x)$.

(3) If $(p_{\lfloor k}) ^\frown (p{\upharpoonright}k) = (q_{\lfloor n}) ^\frown (q{\upharpoonright}n)$ and $k \leq n \leq \operatorname{len} p$, then $p = (q_{\lfloor n -' k}) ^\frown (q{\upharpoonright}(n -' k))$.

(4) If $n \in \operatorname{dom} q$ and $p = (q_{\lfloor n}) ^\frown (q{\upharpoonright}n)$, then $q = (p_{\lfloor \operatorname{len} p -' n}) ^\frown (p{\upharpoonright}(\operatorname{len} p -' n))$.

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

(5) If $(p_{\lfloor k}) \frown (p \restriction k) = (q_{\lfloor n}) \frown (q \restriction n)$, then there exists i such that $p = (q_{\lfloor i}) \frown (q \restriction i)$.

The scheme *Sch* deals with a non empty set $\mathcal{A}$, a non zero natural number $\mathcal{B}$, and a unary predicate $\mathcal{P}$, and states that:

There exists a cardinal number C such that $\mathcal{B} \cdot C = \overline{\overline{\{F \in \mathcal{A}^{\mathcal{B}}\colon \mathcal{P}[F]\}}}$

provided the following requirements are met:

- For all finite sequences p, q of elements of $\mathcal{A}$ such that $p \frown q$ is $\mathcal{B}$-element and $\mathcal{P}[p \frown q]$ holds $\mathcal{P}[q \frown p]$, and
- For every element p of $\mathcal{A}^{\mathcal{B}}$ such that $\mathcal{P}[p]$ and for every natural number i such that $i < \mathcal{B}$ and $p = (p_{\lfloor i}) \frown (p \restriction i)$ holds $i = 0$.

One can prove the following propositions:

(6) Let X be a non empty set, A be a non empty finite subset of X, and P be a function from X into 2^X. Suppose that for every x such that $x \in X$ holds $\overline{\overline{P(x)}} = n$. Then $\overline{\overline{\{F \in X^{k+1}\colon F(1) \in A \ \wedge\ \bigwedge_i \ (i \in \operatorname{Seg} k \ \Rightarrow\ F(i+1) \in P(F(i)))\}}} = \overline{\overline{A}} \cdot n^k$.

(7) If $\operatorname{len} p$ is prime and there exists i such that $0 < i < \operatorname{len} p$ and $p = (p_{\lfloor i}) \frown (p \restriction i)$, then $\operatorname{rng} p \subseteq \{p(1)\}$.

2. The Friendship Graph

Let us consider R and let x be an element of field R. We say that x is universal friend if and only if:

(Def. 1) For every y such that $y \in \operatorname{field} R \setminus \{x\}$ holds $\langle x, y \rangle \in R$.

Let R be a binary relation. We say that R has universal friend if and only if:

(Def. 2) There exists an element of field R which is universal friend.

Let R be a binary relation. We introduce R is without universal friend as an antonym of R has universal friend.

Let R be a binary relation. We say that R is friendship graph like if and only if:

(Def. 3) For all x, y such that $x, y \in \operatorname{field} R$ and $x \neq y$ there exists z such that $R^{\circ}x \cap \operatorname{Coim}(R, y) = \{z\}$.

Let us observe that there exists a binary relation which is finite, symmetric, irreflexive, and friendship graph like.

A friendship graph is a finite symmetric irreflexive friendship graph like binary relation.

In the sequel F_1 is a friendship graph.

The following propositions are true:

(8) $2 \mid \overline{\overline{F_1{}^\circ x}}$.

(9) If $x,\ y \in \operatorname{field} F_1$ and $\langle x,\ y \rangle \notin F_1$, then $\overline{\overline{F_1{}^\circ x}} = \overline{\overline{F_1{}^\circ y}}$.

(10) If F_1 is without universal friend and $x \in \operatorname{field} F_1$, then $\overline{\overline{F_1{}^\circ x}} > 2$.

(11) If F_1 is without universal friend and $x,\ y \in \operatorname{field} F_1$, then $\overline{\overline{F_1{}^\circ x}} = \overline{\overline{F_1{}^\circ y}}$.

(12) If F_1 is without universal friend and $x \in \operatorname{field} F_1$, then $\overline{\overline{\operatorname{field} F_1}} = 1 + \overline{\overline{F_1{}^\circ x}} \cdot (\overline{\overline{F_1{}^\circ x}} - 1)$.

(13) For all elements x, y of field F_1 such that x is universal friend and $x \neq y$ there exists z such that $F_1{}^\circ y = \{x, z\}$ and $F_1{}^\circ z = \{x, y\}$.

3. The Friendship Theorem

Next we state the proposition

(14) If F_1 is non empty, then F_1 has universal friend.

References

[1] Michael Albert. Notes on the friendship theorem, `http://www.math.auckland.ac.nz/~olympiad/training/2006/friendship.pdf`.

[2] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.

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

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

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

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

[7] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

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

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

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

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

[12] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.

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

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

[15] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

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

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

[18] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Received May 15, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 3, Pages 239–256, 2012
DOI: 10.2478/v10037-012-0029-6

VERSITA
versita.com/fm/

Free Term Algebras[1]

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

Summary. We interoduce a new characterization of algebras of normal forms of term rewriting systems [35] as algerbras of term free in itself (any function from free generators into the algebra generates endomorphism of the algebra). Introduced algebras are free in classes of algebras satisfying some sets of equalities. Their universes are subsets of all terms and the denotations of operation symbols are partially identical with the operations of construction of terms. These algebras are compiler algebras requiring some equalities of terms, e.g., associativity of addition.

MML identifier: `MSAFREE4`, version: `7.15.01 4.184.1155`

The terminology and notation used in this paper have been introduced in the following papers: [1], [3], [13], [18], [17], [27], [15], [25], [36], [21], [22], [5], [19], [14], [41], [34], [39], [16], [11], [38], [20], [28], [29], [12], [4], [23], [37], [31], [32], [26], [42], [43], [9], [30], [33], [40], [2], [6], [7], [8], [10], and [24].

1. Preliminaries

In this paper Σ is a non empty non void many sorted signature and X is a non-empty many sorted set indexed by Σ.

We now state the proposition

(1) For every set I and for all many sorted sets f_1, f_2 indexed by I such that $f_1 \subseteq f_2$ holds $\bigcup f_1 \subseteq \bigcup f_2$.

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

In the sequel x, y denote sets and i denotes a natural number.

Let I be a set, let X be a non-empty many sorted set indexed by I, and let A be a component of X. We see that the element of A is an element of $\bigcup X$.

Let I be a set, let X be a many sorted set indexed by I, and let i be an element of I. Then $X(i)$ is a component of X.

Let I be a set, let X, Y be many sorted sets indexed by I, let f be a many sorted function from X into Y, and let x be a set. Then $f(x)$ is a function from $X(x)$ into $Y(x)$.

In this article we present several logical schemes. The scheme *Sch1* deals with a set $\mathcal{A}$, a non-empty many sorted set $\mathcal{B}$ indexed by $\mathcal{A}$, and a binary functor $\mathcal{F}$ yielding a set, and states that:

> There exists a many sorted function f indexed by $\mathcal{A}$ such that for every x if $x \in \mathcal{A}$, then $\operatorname{dom} f(x) = \mathcal{B}(x)$ and for every element y of $\mathcal{B}(x)$ holds $f(x)(y) = \mathcal{F}(x, y)$

for all values of the parameters.

The scheme *Sch2* deals with a non empty set $\mathcal{A}$, non-empty many sorted sets $\mathcal{B}$, $\mathcal{C}$ indexed by $\mathcal{A}$, and a binary functor $\mathcal{F}$ yielding a set, and states that:

> There exists a many sorted function f from $\mathcal{B}$ into $\mathcal{C}$ such that for every element i of $\mathcal{A}$ and for every element a of $\mathcal{B}(i)$ holds $f(i)(a) = \mathcal{F}(i, a)$

provided the following condition is satisfied:

- For every element i of $\mathcal{A}$ and for every element a of $\mathcal{B}(i)$ holds $\mathcal{F}(i, a) \in \mathcal{C}(i)$.

Let X be a non empty set, let O be a set, let f be a function from O into X, and let g be a many sorted set indexed by X. Then $g \cdot f$ is a many sorted set indexed by O.

Let us consider Σ, X, let F be a many sorted set indexed by Σ-Terms(X), let o be an operation symbol of Σ, and let p be an argument sequence of $\mathrm{Sym}(o, X)$. One can check that $F \cdot p$ is finite sequence-like.

The following proposition is true

(2) Subtrees(the root tree of x) = {the root tree of x}.

Let f be a decorated tree yielding function. Observe that $\operatorname{rng} f$ is constituted of decorated trees.

The following three propositions are true:

(3) For every non empty decorated tree yielding finite sequence p holds Subtrees(x-tree(p)) = {x-tree(p)} ∪ Subtrees($\operatorname{rng} p$).

(4) Subtrees(x-tree($\emptyset$)) = {x-tree($\emptyset$)}.

(5) x-tree($\emptyset$) = the root tree of x.

Let us observe that there exists a finite sequence which is finite-yielding, decorated tree yielding, and non empty and there exists a finite sequence which is finite-yielding, tree yielding, and non empty.

Let f be a finite-yielding function. One can check that $\operatorname{dom}_\kappa f(\kappa)$ is finite-yielding.

Let p be a finite-yielding tree yielding finite sequence. Observe that $\overbrace{p}$ is finite.

Let τ be a finite decorated tree. Observe that $\mathrm{Subtrees}(\tau)$ is finite-membered.

Let p be a finite-yielding decorated tree yielding finite sequence and let us consider x. Note that x-tree(p) is finite.

One can prove the following propositions:

(6) For all finite decorated trees τ_1, τ_2 such that $\tau_1 \in \mathrm{Subtrees}(\tau_2)$ holds $\mathrm{height}\,\mathrm{dom}\,\tau_1 \leq \mathrm{height}\,\mathrm{dom}\,\tau_2$.

(7) Let p be a decorated tree yielding finite sequence. Suppose p is finite-yielding. Let τ be a decorated tree. If $x \in \mathrm{Subtrees}(\tau)$ and $\tau \in \mathrm{rng}\,p$, then $x \neq y$-tree(p).

Let us consider Σ and let X be a many sorted set indexed by Σ. Note that every Σ-Terms(X)-valued function is finite-yielding.

Next we state several propositions:

(8) For every non empty constituted of decorated trees set X and for every decorated tree τ such that $\tau \in X$ holds $\mathrm{Subtrees}(\tau) \subseteq \mathrm{Subtrees}(X)$.

(9) For every non empty constituted of decorated trees set X holds $X \subseteq \mathrm{Subtrees}(X)$.

(10) For every term τ of Σ over X and for every x such that $x \in \mathrm{Subtrees}(\tau)$ holds x is a term of Σ over X.

(11) For every decorated tree yielding finite sequence p holds $\mathrm{rng}\,p \subseteq \mathrm{Subtrees}(x\text{-tree}(p))$.

(12) For all decorated trees τ_1, τ_2 such that $\tau_1 \in \mathrm{Subtrees}(\tau_2)$ holds $\mathrm{Subtrees}(\tau_1) \subseteq \mathrm{Subtrees}(\tau_2)$.

(13) Let X be a many sorted set indexed by Σ, o be an operation symbol of Σ, and p be a finite sequence. If $p \in \mathrm{Args}(o, \mathrm{Free}_\Sigma(X))$, then $(\mathrm{Den}(o, \mathrm{Free}_\Sigma(X)))(p) = \langle o, \text{the carrier of } \Sigma\rangle$-tree$(p)$.

Let I be a set, let A, B be non-empty many sorted sets indexed by I, and let f be a many sorted function from A into B. Observe that $\mathrm{rng}_\kappa f(\kappa)$ is non-empty.

Let us consider Σ. One can check that every element of $\mathrm{T}_\Sigma(\mathbb{N})$ is relation-like and function-like.

Let I be a set, let A be a many sorted set indexed by I, and let f be a finite sequence of elements of I. Observe that $A \cdot f$ is $\mathrm{dom}\,f$-defined.

Let I be a set, let A be a many sorted set indexed by I, and let f be a finite sequence of elements of I. One can verify that $A \cdot f$ is total as a $\mathrm{dom}\,f$-defined binary relation.

The following propositions are true:

(14) Let I be a non empty set, J be a set, and A, B be many sorted sets indexed by I. Suppose $A \subseteq B$. Let f be a function from J into I. Then $A \cdot f \subseteq B \cdot f$ **qua** many sorted set indexed by J.

(15) Let I be a set and A, B be many sorted sets indexed by I. Suppose $A \subseteq B$. Let f be a finite sequence of elements of I. Then $A \cdot f \subseteq B \cdot f$ **qua** many sorted set indexed by $\operatorname{dom} f$.

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

(17) Let R be a weakly-normalizing binary relation with unique normal form property. If x is a normal form w.r.t. R, then $\mathrm{nf}_R(x) = x$.

(18) For every weakly-normalizing binary relation R with unique normal form property holds $\mathrm{nf}_R(\mathrm{nf}_R(x)) = \mathrm{nf}_R(x)$.

Let us consider Σ, X, let A be a subset of $\mathrm{Free}(X)$, and let us consider x. One can verify that every element of $A(x)$ is relation-like and function-like.

Let I be a set and let A be a many sorted set indexed by I. We say that A is countable if and only if:

(Def. 1) For every x such that $x \in I$ holds $A(x)$ is countable.

Let I be a set and let X be a countable set. Note that $I \longmapsto X$ is countable as a many sorted set indexed by I. Note that there exists a many sorted set indexed by I which is non-empty and countable.

Let X be a countable many sorted set indexed by I, and let x be a set. Note that $X(x)$ is countable.

Let A be a countable set. Observe that there exists a function from A into $\mathbb{N}$ which is one-to-one.

Let I be a set and let X_0 be a countable many sorted set indexed by I. One can check that there exists a many sorted function from X_0 into $I \longmapsto \mathbb{N}$ which is "1-1".

We now state a number of propositions:

(19) Let Σ be a set, X be a many sorted set indexed by Σ, Y be a non-empty many sorted set indexed by Σ, and w be a many sorted function from X into Y. Then $\mathrm{rng}_\kappa\, w(\kappa)$ is a many sorted subset of Y.

(20) Let Σ be a set and X be a countable many sorted set indexed by Σ. Then there exists a many sorted subset Y of $\Sigma \longmapsto \mathbb{N}$ and there exists a many sorted function w from X into $\Sigma \longmapsto \mathbb{N}$ such that w is "1-1" and $Y = \mathrm{rng}_\kappa\, w(\kappa)$ and for every x such that $x \in \Sigma$ holds $w(x)$ is an enumeration of $X(x)$ and $Y(x) = \overline{\overline{X(x)}}$.

(21) Let I be a set, A be a many sorted set indexed by I, and B be a non-empty many sorted set indexed by I. Then A is transformable to B.

(22) Let I be a set, A, B, C be non-empty many sorted sets indexed by I, and f be a many sorted function from A into B. Suppose B is a many

sorted subset of C. Then f is a many sorted function from A into C.

(23) Let I be a set and A, B be many sorted sets indexed by I. Suppose A is transformable to B. Let f be a many sorted function from A into B. Suppose f is onto. Then there exists a many sorted function g from B into A such that $f \circ g = \mathrm{id}_B$.

(24) Let $\mathfrak{A}_1$, $\mathfrak{A}_2$ be algebras over Σ. Suppose the algebra of $\mathfrak{A}_1 =$ the algebra of $\mathfrak{A}_2$. Let B_1 be a subset of $\mathfrak{A}_1$ and B_2 be a subset of $\mathfrak{A}_2$. Suppose $B_1 = B_2$. Let o be an operation symbol of Σ. If B_1 is closed on o, then B_2 is closed on o.

(25) Let $\mathfrak{A}_1$, $\mathfrak{A}_2$ be algebras over Σ. Suppose the algebra of $\mathfrak{A}_1 =$ the algebra of $\mathfrak{A}_2$. Let B_1 be a subset of $\mathfrak{A}_1$ and B_2 be a subset of $\mathfrak{A}_2$. Suppose $B_1 = B_2$. Let o be an operation symbol of Σ. If B_1 is closed on o, then $o_{B_2} = o_{B_1}$.

(26) Let $\mathfrak{A}_1$, $\mathfrak{A}_2$ be algebras over Σ. Suppose the algebra of $\mathfrak{A}_1 =$ the algebra of $\mathfrak{A}_2$. Let B_1 be a subset of $\mathfrak{A}_1$ and B_2 be a subset of $\mathfrak{A}_2$. If $B_1 = B_2$ and B_1 is operations closed, then $\mathrm{Opers}(\mathfrak{A}_2, B_2) = \mathrm{Opers}(\mathfrak{A}_1, B_1)$.

(27) Let $\mathfrak{A}_1$, $\mathfrak{A}_2$ be algebras over Σ. Suppose the algebra of $\mathfrak{A}_1 =$ the algebra of $\mathfrak{A}_2$. Let B_1 be a subset of $\mathfrak{A}_1$ and B_2 be a subset of $\mathfrak{A}_2$. If $B_1 = B_2$ and B_1 is operations closed, then B_2 is operations closed.

(28) Let $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{B}$ be algebras over Σ. Suppose the algebra of $\mathfrak{A}_1 =$ the algebra of $\mathfrak{A}_2$. Let $\mathfrak{B}_1$ be a subalgebra of $\mathfrak{A}_1$. Suppose the algebra of $\mathfrak{B} =$ the algebra of $\mathfrak{B}_1$. Then $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}_2$.

(29) For all algebras $\mathfrak{A}_1$, $\mathfrak{A}_2$ over Σ such that $\mathfrak{A}_2$ is empty holds every many sorted function from $\mathfrak{A}_1$ into $\mathfrak{A}_2$ is a homomorphism of $\mathfrak{A}_1$ into $\mathfrak{A}_2$.

(30) Let $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{B}_1$ be algebras over Σ and $\mathfrak{B}_2$ be a non-empty algebra over Σ. Suppose the algebra of $\mathfrak{A}_1 =$ the algebra of $\mathfrak{A}_2$ and the algebra of $\mathfrak{B}_1 =$ the algebra of $\mathfrak{B}_2$. Let h_1 be a many sorted function from $\mathfrak{A}_1$ into $\mathfrak{B}_1$ and h_2 be a many sorted function from $\mathfrak{A}_2$ into $\mathfrak{B}_2$. Suppose $h_1 = h_2$ and h_1 is a homomorphism of $\mathfrak{A}_1$ into $\mathfrak{B}_1$. Then h_2 is a homomorphism of $\mathfrak{A}_2$ into $\mathfrak{B}_2$.

2. Trivial Algebras

Let I be a set and let X be a many sorted set indexed by I. Let us observe that X is trivial-yielding if and only if:

(Def. 2) For every x such that $x \in I$ holds $X(x)$ is trivial.

Let I be a set. Note that there exists a many sorted set indexed by I which is non-empty and trivial-yielding.

Let I be a set, let Σ be a trivial-yielding many sorted set indexed by I, and let us consider x. One can check that $\Sigma(x)$ is trivial.

Let us consider Σ and let $\mathfrak{A}$ be an algebra over Σ. We say that $\mathfrak{A}$ is trivial if and only if:

(Def. 3) The sorts of $\mathfrak{A}$ are trivial-yielding.

Let us consider Σ. One can verify that there exists a strict algebra over Σ which is trivial, disjoint valued, and non-empty.

Let us consider Σ and let $\mathfrak{A}$ be a trivial algebra over Σ. One can verify that the sorts of $\mathfrak{A}$ is trivial-yielding.

Next we state four propositions:

(31) Let $\mathfrak{A}$ be a trivial non-empty algebra over Σ, s be a sort symbol of Σ, and e be an element of (the equations of Σ)(s). Then $\mathfrak{A} \models e$.

(32) For every trivial non-empty algebra $\mathfrak{A}$ over Σ and for every set T of equations of Σ holds $\mathfrak{A} \models T$.

(33) Let $\mathfrak{A}$ be a non-empty algebra over Σ and T be a non-empty trivial algebra over Σ. Then every many sorted function from $\mathfrak{A}$ into T is a homomorphism of $\mathfrak{A}$ into T.

(34) Let $\mathfrak{T}$ be a non-empty trivial algebra over Σ and $\mathfrak{A}$ be a non-empty subalgebra of $\mathfrak{T}$. Then the algebra of $\mathfrak{A}$ = the algebra of $\mathfrak{T}$.

3. Image

Let us consider Σ, let $\mathfrak{A}$ be a non-empty algebra over Σ, and let $\mathfrak{C}$ be an algebra over Σ. We say that $\mathfrak{C}$ is $\mathfrak{A}$-image if and only if the condition (Def. 4) is satisfied.

(Def. 4) There exists a non-empty algebra $\mathfrak{B}$ over Σ and there exists a many sorted function h from $\mathfrak{A}$ into $\mathfrak{B}$ such that h is a homomorphism of $\mathfrak{A}$ into $\mathfrak{B}$ and the algebra of $\mathfrak{C} = \operatorname{Im} h$.

Let us consider Σ and let $\mathfrak{A}$ be a non-empty algebra over Σ. Observe that every algebra over Σ which is $\mathfrak{A}$-image is also non-empty and there exists a non-empty strict algebra over Σ which is $\mathfrak{A}$-image.

Let us consider Σ, let $\mathfrak{A}$ be a non-empty algebra over Σ, and let $\mathfrak{C}$ be a non-empty algebra over Σ. Let us observe that $\mathfrak{C}$ is $\mathfrak{A}$-image if and only if:

(Def. 5) There exists a many sorted function from $\mathfrak{A}$ into $\mathfrak{C}$ which is an epimorphism of $\mathfrak{A}$ onto $\mathfrak{C}$.

Let us consider Σ and let $\mathfrak{A}$ be a non-empty algebra over Σ. An image of $\mathfrak{A}$ is an $\mathfrak{A}$-image non-empty algebra over Σ.

Let us consider Σ and let $\mathfrak{A}$ be a non-empty algebra over Σ. Observe that there exists an image of $\mathfrak{A}$ which is disjoint valued and trivial.

One can prove the following propositions:

(35) Let $\mathfrak{A}$ be a non-empty algebra over Σ, $\mathfrak{B}$ be an $\mathfrak{A}$-image algebra over Σ, s be a sort symbol of Σ, and e be an element of (the equations of Σ)(s). If $\mathfrak{A} \models e$, then $\mathfrak{B} \models e$.

(36) Let $\mathfrak{A}$ be a non-empty algebra over Σ, $\mathfrak{B}$ be an $\mathfrak{A}$-image algebra over Σ, and T be a set of equations of Σ. If $\mathfrak{A} \models T$, then $\mathfrak{B} \models T$.

4. Term Algebras

Let us consider Σ, X and let $\mathfrak{A}$ be an algebra over Σ. We say that $\mathfrak{A}$ is including Σ-terms over X if and only if:

(Def. 6) The sorts of $\mathfrak{A}$ are a many sorted subset of the sorts of $\mathrm{Free}_{\Sigma}(X)$.

Let us consider Σ, X. Note that $\mathrm{Free}_{\Sigma}(X)$ is including Σ-terms over X.

Let us consider Σ, X. One can check that $\mathrm{Free}_{\Sigma}(X)$ is non-empty and disjoint valued.

Let us consider Σ, X. One can check that there exists a strict algebra over Σ which is including Σ-terms over X and non-empty and there exists an algebra over Σ which is including Σ-terms over X and non-empty.

Let us consider Σ, X and let $\mathfrak{A}$ be an including Σ-terms over X algebra over Σ. We say that $\mathfrak{A}$ has all variables if and only if:

(Def. 7) FreeGenerator(X) is a many sorted subset of the sorts of $\mathfrak{A}$.

We say that $\mathfrak{A}$ inherits operations if and only if the condition (Def. 8) is satisfied.

(Def. 8) Let o be an operation symbol of Σ and p be a finite sequence. Suppose $p \in \mathrm{Args}(o, \mathrm{Free}_{\Sigma}(X))$ and $(\mathrm{Den}(o, \mathrm{Free}_{\Sigma}(X)))(p) \in$ (the sorts of $\mathfrak{A}$)(the result sort of o). Then $p \in \mathrm{Args}(o, \mathfrak{A})$ and $(\mathrm{Den}(o, \mathfrak{A}))(p) = (\mathrm{Den}(o, \mathrm{Free}_{\Sigma}(X)))(p)$.

We say that $\mathfrak{A}$ is free in itself if and only if the condition (Def. 9) is satisfied.

(Def. 9) Let f be a many sorted function from FreeGenerator(X) into the sorts of $\mathfrak{A}$ and G be a many sorted subset of the sorts of $\mathfrak{A}$. Suppose $G =$ FreeGenerator(X). Then there exists a many sorted function h from $\mathfrak{A}$ into $\mathfrak{A}$ such that h is a homomorphism of $\mathfrak{A}$ into $\mathfrak{A}$ and $f = h \restriction G$.

We now state two propositions:

(37) Let $\mathfrak{A}$, $\mathfrak{B}$ be non-empty algebras over Σ. Suppose the algebra of $\mathfrak{A} =$ the algebra of $\mathfrak{B}$. Suppose $\mathfrak{A}$ is including Σ-terms over X. Then $\mathfrak{B}$ is including Σ-terms over X.

(38) Let $\mathfrak{A}$, $\mathfrak{B}$ be including Σ-terms over X non-empty algebras over Σ such that the algebra of $\mathfrak{A} =$ the algebra of $\mathfrak{B}$. Then

(i) if $\mathfrak{A}$ has all variables, then $\mathfrak{B}$ has all variables,

(ii) if $\mathfrak{A}$ inherits operations, then $\mathfrak{B}$ inherits operations, and

(iii) if $\mathfrak{A}$ is free in itself, then $\mathfrak{B}$ is free in itself.

Let J be a non empty non void many sorted signature and let $\mathfrak{T}$ be a non-empty algebra over J. Observe that there exists a generator set of $\mathfrak{T}$ which is non-empty.

Let us consider Σ, X. Observe that $\mathrm{Free}_{\Sigma}(X)$ is free in itself, has all variables, and inherits operations.

Let us consider Σ, X. Note that every including Σ-terms over X algebra over Σ which has all variables is also non-empty and there exists an including Σ-terms over X strict algebra over Σ which is free in itself, has all variables, and inherits operations.

In the sequel $\mathfrak{A}_0$ denotes an including Σ-terms over X non-empty algebra over Σ, $\mathfrak{A}_1$ denotes an including Σ-terms over X algebra over Σ with all variables, $\mathfrak{A}_2$ denotes an including Σ-terms over X algebra over Σ with all variables and inheriting operations, and $\mathfrak{A}$ denotes a free in itself including Σ-terms over X algebra over Σ with all variables and inheriting operations.

Next we state three propositions:

(39) Every element of $\mathfrak{A}_0$ is an element of $\mathrm{Free}_{\Sigma}(X)$ and for every sort symbol s of Σ holds every element of $\mathfrak{A}_0$ from s is an element of $\mathrm{Free}_{\Sigma}(X)$ from s.

(40) Let s be a sort symbol of Σ and x be an element of $X(s)$. Then the root tree of $\langle x, s\rangle$ is an element of $\mathfrak{A}_1$ from s.

(41) For every operation symbol o of Σ holds $\mathrm{Args}(o, \mathfrak{A}_1) \subseteq \mathrm{Args}(o, \mathrm{Free}_{\Sigma}(X))$.

Let Σ be a set. Observe that there exists a many sorted set indexed by Σ which is disjoint valued and non-empty.

Let Σ be a set and let T be a disjoint valued non-empty many sorted set indexed by Σ. One can check that every many sorted subset of T is disjoint valued.

Let us consider Σ, X. Observe that there exists an algebra over Σ which is including Σ-terms over X and strict.

Let us consider Σ, X, $\mathfrak{A}_1$. The canonical homomorphism of $\mathfrak{A}_1$ yields a many sorted function from $\mathrm{Free}_{\Sigma}(X)$ into $\mathfrak{A}_1$ and is defined by the conditions (Def. 10).

(Def. 10)(i) The canonical homomorphism of $\mathfrak{A}_1$ is a homomorphism of $\mathrm{Free}_{\Sigma}(X)$ into $\mathfrak{A}_1$, and

(ii) for every generator set G of $\mathrm{Free}_{\Sigma}(X)$ such that $G = \mathrm{FreeGenerator}(X)$ holds $\mathrm{id}_G =$ (the canonical homomorphism of $\mathfrak{A}_1$) $\restriction G$.

Let us consider Σ, X, $\mathfrak{A}_0$. One can check that every element of $\mathfrak{A}_0$ is function-like and relation-like. Let s be a sort symbol of Σ. One can verify that every element of $\mathfrak{A}_0$ from s is function-like and relation-like.

Let us consider Σ, X, $\mathfrak{A}_0$. One can verify that every element of $\mathfrak{A}_0$ is decorated tree-like. Let s be a sort symbol of Σ. Note that every element of $\mathfrak{A}_0$ from s is decorated tree-like.

Let us consider Σ, X. Note that every algebra over Σ which is including Σ-terms over X is also disjoint valued.

The following propositions are true:

(42) Every element of $\mathfrak{A}_0$ is a term of Σ over X.

(43) Let τ be an element of $\mathfrak{A}_0$ and s be a sort symbol of Σ. If $\tau \in$ (the sorts of $\mathrm{Free}_\Sigma(X))(s)$, then $\tau \in$ (the sorts of $\mathfrak{A}_0)(s)$.

(44) For every element τ of $\mathfrak{A}_2$ and for every element p of $\mathrm{dom}\,\tau$ holds $\tau{\restriction}p$ is an element of $\mathfrak{A}_2$.

(45) FreeGenerator(X) is a generator set of $\mathfrak{A}_2$.

(46) Let T be a free in itself non-empty including Σ-terms over X algebra over Σ, $\mathfrak{A}$ be an image of T, and G be a generator set of T. Suppose $G =$ FreeGenerator(X). Let f be a many sorted function from G into the sorts of $\mathfrak{A}$. Then there exists a many sorted function h from T into $\mathfrak{A}$ such that h is a homomorphism of T into $\mathfrak{A}$ and $f = h \restriction G$.

(47)(i) The canonical homomorphism of $\mathfrak{A}_2$ is an epimorphism of $\mathrm{Free}_\Sigma(X)$ onto $\mathfrak{A}_2$, and

(ii) for every sort symbol s of Σ and for every element τ of $\mathfrak{A}_2$ from s holds (the canonical homomorphism of $\mathfrak{A}_2)(s)(\tau) = \tau$.

(48) (The canonical homomorphism of $\mathfrak{A}_2) \circ$ (the canonical homomorphism of $\mathfrak{A}_2) =$ the canonical homomorphism of $\mathfrak{A}_2$.

(49) $\mathfrak{A}$ is $\mathrm{Free}_\Sigma(X)$-image.

5. Satisfiability

The following four propositions are true:

(50) Let $\mathfrak{A}$ be a non-empty algebra over Σ, s be a sort symbol of Σ, and τ be an element of $\mathrm{T}_\Sigma(\mathbb{N})$ from s. Then $\mathfrak{A} \models \tau{=}\tau$.

(51) Let A be a non-empty algebra over Σ, s be a sort symbol of Σ, and τ_1, τ_2 be elements of $\mathrm{T}_\Sigma(\mathbb{N})$ from s. If $A \models \tau_1{=}\tau_2$, then $A \models \tau_2{=}\tau_1$.

(52) Let $\mathfrak{A}$ be a non-empty algebra over Σ, s be a sort symbol of Σ, and τ_1, τ_2, τ_3 be elements of $\mathrm{T}_\Sigma(\mathbb{N})$ from s. If $\mathfrak{A} \models \tau_1{=}\ \tau_2$ and $\mathfrak{A} \models \tau_2{=}\tau_3$, then $\mathfrak{A} \models \tau_1{=}\tau_3$.

(53) Let $\mathfrak{A}$ be a non-empty algebra over Σ, o be an operation symbol of Σ, and a_1, a_2 be finite sequences. Suppose that

(i) $a_1 \in \mathrm{Args}(o, \mathrm{T}_\Sigma(\mathbb{N}))$,

(ii) $a_2 \in \mathrm{Args}(o, \mathrm{T}_\Sigma(\mathbb{N}))$, and

(iii) for every natural number i such that $i \in \mathrm{dom}\,\mathrm{Arity}(o)$ and for every sort symbol s of Σ such that $s = \mathrm{Arity}(o)(i)$ and for all elements τ_1, τ_2 of $\mathrm{T}_\Sigma(\mathbb{N})$ from s such that $\tau_1 = a_1(i)$ and $\tau_2 = a_2(i)$ holds $\mathfrak{A} \models \tau_1{=}\tau_2$.

Let τ_1, τ_2 be elements of $\mathrm{T}_\Sigma(\mathbb{N})$ from the result sort of o. Suppose $\tau_1 = \langle o$, the carrier of $\Sigma\rangle$-tree(a_1) and $\tau_2 = \langle o$, the carrier of $\Sigma\rangle$-tree(a_2). Then $\mathfrak{A} \models \tau_1{=}\tau_2$.

Let us consider Σ, let T be a set of equations of Σ, and let $\mathfrak{A}$ be an algebra over Σ. We say that $\mathfrak{A}$ satisfies T if and only if:

(Def. 11) $\mathfrak{A} \models T$.

Let us consider Σ and let T be a set of equations of Σ. Observe that there exists an algebra over Σ which is non-empty and trivial and satisfies T .

Let us consider Σ, let T be a set of equations of Σ, and let $\mathfrak{A}$ be a non-empty algebra over Σ satisfying T . One can verify that every non-empty algebra over Σ which is $\mathfrak{A}$-image also satisfies T .

Let us consider Σ, let $\mathfrak{A}$ be an algebra over Σ, let T be a set of equations of Σ, and let G be a generator set of $\mathfrak{A}$. We say that G is T-free if and only if the condition (Def. 12) is satisfied.

(Def. 12) Let $\mathfrak{B}$ be a non-empty algebra over Σ satisfying T and f be a many sorted function from G into the sorts of $\mathfrak{B}$. Then there exists a many sorted function h from $\mathfrak{A}$ into $\mathfrak{B}$ such that h is a homomorphism of $\mathfrak{A}$ into $\mathfrak{B}$ and $h \restriction G = f$.

Let us consider Σ, let T be a set of equations of Σ, and let $\mathfrak{A}$ be an algebra over Σ. We say that $\mathfrak{A}$ is T-free if and only if:

(Def. 13) There exists a generator set of $\mathfrak{A}$ which is T-free.

Let us consider Σ and let $\mathfrak{A}$ be an algebra over Σ. The functor $\mathrm{Equations}(\Sigma, \mathfrak{A})$ yields a set of equations of Σ and is defined as follows:

(Def. 14) For every sort symbol s of Σ holds $(\mathrm{Equations}(\Sigma, \mathfrak{A}))(s) = \{e; e$ ranges over elements of (the equations of $\Sigma)(s)$: $\mathfrak{A} \models e\}$.

We now state the proposition

(54) For every algebra $\mathfrak{A}$ over Σ holds $\mathfrak{A} \models \mathrm{Equations}(\Sigma, \mathfrak{A})$.

Let us consider Σ and let $\mathfrak{A}$ be a non-empty algebra over Σ. One can verify that every $\mathfrak{A}$-image algebra over Σ satisfies $\mathrm{Equations}(\Sigma, \mathfrak{A})$.

6. Term Correspondence

Now we present two schemes. The scheme *TermDefEx* deals with a non empty non void many sorted signature $\mathcal{A}$, a non-empty many sorted set $\mathcal{B}$ indexed by $\mathcal{A}$, a binary functor $\mathcal{F}$ yielding a set, and a binary functor $\mathcal{G}$ yielding a set, and states that:

There exists a many sorted set F indexed by $\mathcal{A}$-Terms$(\mathcal{B})$ such that

(i) for every sort symbol s of $\mathcal{A}$ and for every element x of $\mathcal{B}(s)$ holds F(the root tree of $\langle x, s\rangle) = \mathcal{F}(x, s)$, and

(ii) for every operation symbol o of $\mathcal{A}$ and for every argument sequence p of $\mathrm{Sym}(o, \mathcal{B})$ holds $F(\mathrm{Sym}(o, \mathcal{B})\text{-tree}(p)) = \mathcal{G}(o, F \cdot p)$

for all values of the parameters.

The scheme *TermDefUniq* deals with a non empty non void many sorted signature $\mathcal{A}$, a non-empty many sorted set $\mathcal{B}$ indexed by $\mathcal{A}$, a binary functor $\mathcal{F}$ yielding a set, a binary functor $\mathcal{G}$ yielding a set, and many sorted sets $\mathcal{C}$, $\mathcal{D}$ indexed by $\mathcal{A}$-Terms($\mathcal{B}$), and states that:

$\mathcal{C} = \mathcal{D}$

provided the following conditions are satisfied:

- For every sort symbol s of $\mathcal{A}$ and for every element x of $\mathcal{B}(s)$ holds $\mathcal{C}(\text{the root tree of } \langle x,\, s\rangle) = \mathcal{F}(x, s)$,
- For every operation symbol o of $\mathcal{A}$ and for every argument sequence p of $\mathrm{Sym}(o, \mathcal{B})$ holds $\mathcal{C}(\mathrm{Sym}(o, \mathcal{B})\text{-tree}(p)) = \mathcal{G}(o, \mathcal{C} \cdot p)$,
- For every sort symbol s of $\mathcal{A}$ and for every element x of $\mathcal{B}(s)$ holds $\mathcal{D}(\text{the root tree of } \langle x,\, s\rangle) = \mathcal{F}(x, s)$, and
- For every operation symbol o of $\mathcal{A}$ and for every argument sequence p of $\mathrm{Sym}(o, \mathcal{B})$ holds $\mathcal{D}(\mathrm{Sym}(o, \mathcal{B})\text{-tree}(p)) = \mathcal{G}(o, \mathcal{D} \cdot p)$.

Let us consider Σ, X, let w be a many sorted function from X into (the carrier of Σ) $\longmapsto \mathbb{N}$, and let τ be a function. Let us assume that τ is an element of $\mathrm{Free}_\Sigma(X)$. The functor $\#_w^\tau$ yields an element of $\mathrm{T}_\Sigma(\mathbb{N})$ and is defined by the condition (Def. 15).

(Def. 15) There exists a many sorted set F indexed by Σ-Terms(X) such that

(i) $\#_w^\tau = F(\tau)$,

(ii) for every sort symbol s of Σ and for every element x of $X(s)$ holds $F(\text{the root tree of } \langle x,\, s\rangle) = \text{the root tree of } \langle w(s)(x),\, s\rangle$, and

(iii) for every operation symbol o of Σ and for every argument sequence p of $\mathrm{Sym}(o, X)$ holds $F(\mathrm{Sym}(o, X)\text{-tree}(p)) = \mathrm{Sym}(o, (\text{the carrier of } \Sigma) \longmapsto \mathbb{N})\text{-tree}(F \cdot p)$.

We now state the proposition

(55) Let w be a many sorted function from X into (the carrier of Σ) $\longmapsto \mathbb{N}$ and F be a many sorted set indexed by Σ-Terms(X). Suppose that

(i) for every sort symbol s of Σ and for every element x of $X(s)$ holds $F(\text{the root tree of } \langle x,\, s\rangle) = \text{the root tree of } \langle w(s)(x),\, s\rangle$, and

(ii) for every operation symbol o of Σ and for every argument sequence p of $\mathrm{Sym}(o, X)$ holds $F(\mathrm{Sym}(o, X)\text{-tree}(p)) = \mathrm{Sym}(o, (\text{the carrier of } \Sigma) \longmapsto \mathbb{N})\text{-tree}(F \cdot p)$.

Let τ be an element of $\mathrm{Free}_\Sigma(X)$. Then $F(\tau) = \#_w^\tau$.

Let us consider Σ, X, let G be a non-empty subset of $\mathrm{Free}_\Sigma(X)$, and let s be a sort symbol of Σ. Observe that every element of $G(s)$ is relation-like and function-like.

Next we state several propositions:

(56) Let w be a many sorted function from X into (the carrier of Σ) $\longmapsto \mathbb{N}$. Then there exists a many sorted function h from $\mathrm{Free}_\Sigma(X)$ into $\mathrm{T}_\Sigma(\mathbb{N})$ such that

(i) h is a homomorphism of $\mathrm{Free}_\Sigma(X)$ into $\mathrm{T}_\Sigma(\mathbb{N})$, and

(ii) for every sort symbol s of Σ and for every element τ of $\mathrm{Free}_\Sigma(X)$ from s holds $\#_w^\tau = h(s)(\tau)$.

(57) Let w be a many sorted function from X into (the carrier of Σ) $\longmapsto \mathbb{N}$, s be a sort symbol of Σ, and x be an element of $X(s)$. Then $\#_w^{\text{the root tree of }\langle x, s\rangle}$ = the root tree of $\langle w(s)(x), s\rangle$.

(58) Let w be a many sorted function from X into (the carrier of Σ) $\longmapsto \mathbb{N}$, o be an operation symbol of Σ, p be an argument sequence of $\mathrm{Sym}(o, X)$, and q be a finite sequence. Suppose $\operatorname{dom} q = \operatorname{dom} p$ and for every natural number i and for every element τ of $\mathrm{Free}_\Sigma(X)$ such that $i \in \operatorname{dom} p$ and $\tau = p(i)$ holds $q(i) = \#_w^\tau$. Then $\#_w^{\mathrm{Sym}(o,X)\text{-tree}(p)} = \mathrm{Sym}(o,$ (the carrier of Σ) $\longmapsto \mathbb{N}$)-tree(q).

(59) For every many sorted subset Y of X holds $\mathrm{Free}_\Sigma(Y)$ is a subalgebra of $\mathrm{Free}_\Sigma(X)$.

(60) Let w be a many sorted function from X into (the carrier of Σ) $\longmapsto \mathbb{N}$ and τ be a term of Σ over X. Then $\#_w^\tau$ is an element of $\mathrm{Free}_\Sigma(\mathrm{rng}_\kappa\, w(\kappa))$ from the sort of τ and $\#_w^\tau$ is an element of $\mathrm{T}_\Sigma(\mathbb{N})$ from the sort of τ.

(61) Let w be a many sorted function from X into (the carrier of Σ) $\longmapsto \mathbb{N}$ and F be a many sorted set indexed by Σ-Terms(X). Suppose that

(i) for every sort symbol s of Σ and for every element x of $X(s)$ holds F(the root tree of $\langle x, s\rangle$) = the root tree of $\langle w(s)(x), s\rangle$, and

(ii) for every operation symbol o of Σ and for every argument sequence p of $\mathrm{Sym}(o, X)$ holds $F(\mathrm{Sym}(o, X)\text{-tree}(p)) = \mathrm{Sym}(o,$ (the carrier of Σ) $\longmapsto \mathbb{N}$)-tree$(F \cdot p)$.

Let o be an operation symbol of Σ and p be an argument sequence of $\mathrm{Sym}(o, X)$. Then $F \cdot p \in \mathrm{Args}(o, \mathrm{Free}_\Sigma(\mathrm{rng}_\kappa\, w(\kappa)))$ and $F \cdot p \in \mathrm{Args}(o, \mathrm{Free}_\Sigma($(the carrier of Σ) $\longmapsto \mathbb{N}$)).

(62) Let w be a many sorted function from (the carrier of Σ) $\longmapsto \mathbb{N}$ into X. Then there exists a many sorted function h from $\mathrm{T}_\Sigma(\mathbb{N})$ into $\mathfrak{A}$ such that

(i) h is a homomorphism of $\mathrm{T}_\Sigma(\mathbb{N})$ into $\mathfrak{A}$, and

(ii) for every sort symbol s of Σ and for every natural number i holds $h(s)$(the root tree of $\langle i, s\rangle$) = the root tree of $\langle w(s)(i), s\rangle$.

(63) Let w be a many sorted function from X into (the carrier of Σ) $\longmapsto \mathbb{N}$. Then there exists a many sorted function h from FreeGenerator(X) into the sorts of $\mathrm{T}_\Sigma(\mathbb{N})$ such that for every sort symbol s of Σ and for every element i of $X(s)$ holds $h(s)$(the root tree of $\langle i, s\rangle$) = the root tree of $\langle w(s)(i), s\rangle$.

7. Free Algebras

In the sequel X_0 is a non-empty countable many sorted set indexed by Σ and $\mathfrak{A}_0$ is a free in itself including Σ-terms over X_0 algebra over Σ with all variables and inheriting operations.

The following propositions are true:

(64) Let h be a many sorted function from $\mathrm{T}_\Sigma(\mathbb{N})$ into $\mathfrak{A}_0$. Suppose h is a homomorphism of $\mathrm{T}_\Sigma(\mathbb{N})$ into $\mathfrak{A}_0$. Let w be a many sorted function from X_0 into (the carrier of Σ) $\longmapsto \mathbb{N}$. Suppose w is "1-1". Then there exists a non-empty many sorted subset Y of (the carrier of Σ) $\longmapsto \mathbb{N}$ and there exists a subset B of $\mathrm{T}_\Sigma(\mathbb{N})$ and there exists a many sorted function w_1 from $\mathrm{Free}_\Sigma(Y)$ into $\mathfrak{A}_0$ and there exists a many sorted function g from $\mathfrak{A}_0$ into $\mathfrak{A}_0$ such that $Y = \mathrm{rng}_\kappa\, w(\kappa)$ and $B =$ the sorts of $\mathrm{Free}_\Sigma(Y)$ and $\mathrm{FreeGenerator}(\mathrm{rng}_\kappa\, w(\kappa)) \subseteq B$ and w_1 is a homomorphism of $\mathrm{Free}_\Sigma(Y)$ into $\mathfrak{A}_0$ and g is a homomorphism of $\mathfrak{A}_0$ into $\mathfrak{A}_0$ and $h \restriction B = g \circ w_1$ and for every sort symbol s of Σ and for every natural number i such that $i \in Y(s)$ there exists an element x of $X_0(s)$ such that $w(s)(x) = i$ and $w_1(s)$(the root tree of $\langle i, s\rangle$) $=$ the root tree of $\langle x, s\rangle$.

(65) Let h be a many sorted function from $\mathrm{Free}_\Sigma(X_0)$ into $\mathfrak{A}_0$. Suppose h is a homomorphism of $\mathrm{Free}_\Sigma(X_0)$ into $\mathfrak{A}_0$. Then there exists a many sorted function g from $\mathfrak{A}_0$ into $\mathfrak{A}_0$ such that g is a homomorphism of $\mathfrak{A}_0$ into $\mathfrak{A}_0$ and $h = g \circ$ the canonical homomorphism of $\mathfrak{A}_0$.

(66) Let o be an operation symbol of Σ, x be an element of $\mathrm{Args}(o, \mathfrak{A}_0)$, and x_0 be an element of $\mathrm{Args}(o, \mathrm{Free}_\Sigma(X_0))$. If $x_0 = x$, then (the canonical homomorphism of $\mathfrak{A}_0$)$\# x_0 = x$.

(67) Let o be an operation symbol of Σ and x be an element of $\mathrm{Args}(o, \mathfrak{A}_0)$. Then $(\mathrm{Den}(o, \mathfrak{A}_0))(x) =$ (the canonical homomorphism of $\mathfrak{A}_0$)(the result sort of o)($(\mathrm{Den}(o, \mathrm{Free}_\Sigma(X_0)))(x)$).

(68) Let h be a many sorted function from $\mathrm{Free}_\Sigma(X_0)$ into $\mathfrak{A}_0$. Suppose h is a homomorphism of $\mathrm{Free}_\Sigma(X_0)$ into $\mathfrak{A}_0$. Let o be an operation symbol of Σ and x be an element of $\mathrm{Args}(o, \mathfrak{A}_0)$. Then h(the result sort of o)($(\mathrm{Den}(o, \mathfrak{A}_0))(x)$) $= h$(the result sort of o)($(\mathrm{Den}(o, \mathrm{Free}_\Sigma(X_0)))(x)$).

(69) Let h be a many sorted function from $\mathrm{Free}_\Sigma(X_0)$ into $\mathfrak{A}_0$. Suppose h is a homomorphism of $\mathrm{Free}_\Sigma(X_0)$ into $\mathfrak{A}_0$. Let o be an operation symbol of Σ and x be an element of $\mathrm{Args}(o, \mathrm{Free}_\Sigma(X_0))$. Then h(the result sort of o)($(\mathrm{Den}(o, \mathrm{Free}_\Sigma(X_0)))(x)$) $= h$(the result sort of o)($(\mathrm{Den}(o, \mathrm{Free}_\Sigma(X_0)))$((the canonical homomorphism of $\mathfrak{A}_0$)$\# x$)).

(70) Let X_0, Y_0 be non-empty countable many sorted sets indexed by Σ, $\mathfrak{A}$ be an including Σ-terms over X_0 algebra over Σ with all variables and inheriting operations, and h be a many sorted function from $\mathrm{Free}_\Sigma(Y_0)$ into $\mathfrak{A}$. Suppose h is a homomorphism of $\mathrm{Free}_\Sigma(Y_0)$ into $\mathfrak{A}$. Then there

exists a many sorted function g from $\mathrm{Free}_\Sigma(Y_0)$ into $\mathrm{Free}_\Sigma(X_0)$ such that

(i) g is a homomorphism of $\mathrm{Free}_\Sigma(Y_0)$ into $\mathrm{Free}_\Sigma(X_0)$,

(ii) $h =$ (the canonical homomorphism of $\mathfrak{A}$) $\circ\, g$, and

(iii) for every generator set G of $\mathrm{Free}_\Sigma(Y_0)$ such that $G = \mathrm{FreeGenerator}(Y_0)$ holds $g \restriction G = h \restriction G$.

(71) Let w be a many sorted function from X_0 into (the carrier of Σ) $\longmapsto \mathbb{N}$, s be a sort symbol of Σ, τ be an element of $\mathrm{Free}_\Sigma(X_0)$ from s, and τ_1, τ_2 be elements of $\mathrm{T}_\Sigma(\mathbb{N})$ from s. Suppose $\tau_1 = \#_w^\tau$ and $\tau_2 = \#_w^{(\text{the canonical homomorphism of } \mathfrak{A}_0)(s)(\tau)}$. Then $\mathfrak{A}_0 \models \tau_1{=}\tau_2$.

(72) Let w be a many sorted function from X_0 into (the carrier of Σ) $\longmapsto \mathbb{N}$, o be an operation symbol of Σ, p be an element of $\mathrm{Args}(o, \mathrm{Free}_\Sigma(X_0))$, and q be an element of $\mathrm{Args}(o, \mathfrak{A}_0)$. Suppose (the canonical homomorphism of $\mathfrak{A}_0$)$\#p = q$. Let τ_1, τ_2 be terms of Σ over X_0. Suppose $\tau_1 = (\mathrm{Den}(o, \mathrm{Free}_\Sigma(X_0)))(p)$ and $\tau_2 = (\mathrm{Den}(o, \mathfrak{A}_0))(q)$. Let τ_3, τ_4 be elements of $\mathrm{T}_\Sigma(\mathbb{N})$ from the result sort of o. If $\tau_3 = \#_w^{\tau_1}$ and $\tau_4 = \#_w^{\tau_2}$, then $\mathfrak{A}_0 \models \tau_3{=}\tau_4$.

(73) Let w be a many sorted function from X_0 into (the carrier of Σ) $\longmapsto \mathbb{N}$. Suppose w is "1-1". Then there exists a many sorted function g from $\mathrm{T}_\Sigma(\mathbb{N})$ into $\mathrm{Free}_\Sigma(X_0)$ such that

(i) g is a homomorphism of $\mathrm{T}_\Sigma(\mathbb{N})$ into $\mathrm{Free}_\Sigma(X_0)$, and

(ii) for every sort symbol s of Σ and for every element τ of $\mathrm{Free}_\Sigma(X_0)$ from s holds $g(s)(\#_w^\tau) = \tau$.

(74) Let $\mathfrak{B}$ be a non-empty algebra over Σ and h be a many sorted function from $\mathrm{Free}_\Sigma(X_0)$ into $\mathfrak{B}$. Suppose h is a homomorphism of $\mathrm{Free}_\Sigma(X_0)$ into $\mathfrak{B}$. Let w be a many sorted function from X_0 into (the carrier of Σ) $\longmapsto \mathbb{N}$. Suppose w is "1-1". Let s be a sort symbol of Σ, τ_1, τ_2 be elements of $\mathrm{Free}_\Sigma(X_0)$ from s, and τ_3, τ_4 be elements of $\mathrm{T}_\Sigma(\mathbb{N})$ from s. If $\tau_3 = \#_w^{\tau_1}$ and $\tau_4 = \#_w^{\tau_2}$, then if $\mathfrak{B} \models \tau_3{=}\tau_4$, then $h(s)(\tau_1) = h(s)(\tau_2)$.

(75) For every generator set G of $\mathfrak{A}_0$ such that $G = \mathrm{FreeGenerator}(X_0)$ holds G is $\mathrm{Equations}(\Sigma, \mathfrak{A}_0)$-free.

(76) $\mathfrak{A}_0$ is $\mathrm{Equations}(\Sigma, \mathfrak{A}_0)$-free.

8. Algebras of Normal Forms

Let I be a set, let X, Y be many sorted sets indexed by I, let R be a many sorted relation between X and Y, and let x be a set. Then $R(x)$ is a relation between $X(x)$ and $Y(x)$.

Let I be a set, let X be a many sorted set indexed by I, and let R be a many sorted relation indexed by X. We say that R is terminating if and only if:

(Def. 16) For every set x such that $x \in I$ holds $R(x)$ is strongly-normalizing.

We say that R has unique normal form property if and only if:

(Def. 17) For every set x such that $x \in I$ holds $R(x)$ has unique normal form property.

Let us mention that every empty set is strongly-normalizing and has unique normal form property.

One can prove the following proposition

(77) Let I be a set and A be a many sorted set indexed by I. Then there exists a many sorted relation R indexed by A such that $R = I \longmapsto \emptyset$ and R is terminating.

Let I be a set and let X be a many sorted set indexed by I. One can verify that every many sorted relation indexed by X which is empty yielding is also terminating and has unique normal form property and there exists a many sorted relation indexed by X which is empty yielding.

Let I be a set, let X be a many sorted set indexed by I, let R be a terminating many sorted relation indexed by X, and let i be a set. Note that $R(i)$ is strongly-normalizing as a binary relation.

Let R be a many sorted relation indexed by X with unique normal form property, and let i be a set. Note that $R(i)$ has unique normal form property as a binary relation.

Let us consider Σ, X and let R be a many sorted relation indexed by $\mathrm{Free}_{\Sigma}(X)$. We say that R has NF-variables if and only if:

(Def. 18) For every sort symbol s of Σ holds every element of $\mathrm{FreeGenerator}(X)(s)$ is a normal form w.r.t. $R(s)$.

We now state the proposition

(78) x is a normal form w.r.t. $\emptyset$.

Let us consider Σ, X. Note that every many sorted relation indexed by $\mathrm{Free}_{\Sigma}(X)$ which is empty yielding is also invariant and stable and has NF-variables.

Let us consider Σ, X. Observe that there exists an invariant stable many sorted relation indexed by $\mathrm{Free}_{\Sigma}(X)$ which is terminating and has NF-variables and unique normal form property.

Now we present two schemes. The scheme A deals with sets $\mathcal{A}$, $\mathcal{B}$, a binary relation $\mathcal{C}$, and a unary predicate $\mathcal{P}$, and states that:

$\mathcal{P}[\mathcal{B}]$

provided the parameters satisfy the following conditions:

- $\mathcal{P}[\mathcal{A}]$,
- $\mathcal{C}$ reduces $\mathcal{A}$ to $\mathcal{B}$, and
- For all sets y, z such that $\mathcal{C}$ reduces $\mathcal{A}$ to y and $\langle y, z\rangle \in \mathcal{C}$ and $\mathcal{P}[y]$ holds $\mathcal{P}[z]$.

The scheme B deals with sets $\mathcal{A}$, $\mathcal{B}$, a binary relation $\mathcal{C}$, and a unary predicate $\mathcal{P}$, and states that:

$\mathcal{P}[\mathcal{A}]$

provided the parameters meet the following requirements:

- $\mathcal{P}[\mathcal{B}]$,
- $\mathcal{C}$ reduces $\mathcal{A}$ to $\mathcal{B}$, and
- For all sets y, z such that $\langle y, z \rangle \in \mathcal{C}$ and $\mathcal{P}[z]$ holds $\mathcal{P}[y]$.

Let X be a non empty set, let R be a strongly-normalizing binary relation on X with unique normal form property, and let x be an element of X. Then $\mathrm{nf}_R(x)$ is an element of X.

Let I be a non empty set, let X be a non-empty many sorted set indexed by I, and let R be a terminating many sorted relation indexed by X with unique normal form property. The functor $\mathrm{NForms}(R)$ yields a non-empty many sorted subset of X and is defined as follows:

(Def. 19) For every element i of I holds $(\mathrm{NForms}(R))(i) = \{\mathrm{nf}_{R(i)}(x) : x$ ranges over elements of $X(i)\}$.

The scheme *MSFLambda* deals with a non empty set $\mathcal{A}$, a unary functor $\mathcal{F}$ yielding a non empty set, and a binary functor $\mathcal{G}$ yielding a set, and states that:

> There exists a many sorted function f indexed by $\mathcal{A}$ such that for every element o of $\mathcal{A}$ holds
>
> $\operatorname{dom} f(o) = \mathcal{F}(o)$ and for every element x of $\mathcal{F}(o)$ holds $f(o)(x) = \mathcal{G}(o, x)$

for all values of the parameters.

Let us consider Σ, X and let R be a terminating invariant stable many sorted relation indexed by $\mathrm{Free}_\Sigma(X)$ with unique normal form property. The algebra of normal forms of R yields a non-empty strict algebra over Σ and is defined by the conditions (Def. 20).

(Def. 20)(i) The sorts of the algebra of normal forms of $R = \mathrm{NForms}(R)$, and

(ii) for every operation symbol o of Σ and for every element a of $\mathrm{Args}(o,$ the algebra of normal forms of $R)$ holds $(\mathrm{Den}(o,$ the algebra of normal forms of $R))(a) = \mathrm{nf}_{R(\text{the result sort of } o)}((\mathrm{Den}(o, \mathrm{Free}_\Sigma(X)))(a))$.

We now state several propositions:

(79) Let R be a terminating invariant stable many sorted relation indexed by $\mathrm{Free}_\Sigma(X)$ with unique normal form property and a be a sort symbol of Σ. If $x \in (\mathrm{NForms}(R))(a)$, then $\mathrm{nf}_{R(a)}(x) = x$.

(80) Let R be a terminating invariant stable many sorted relation indexed by $\mathrm{Free}_\Sigma(X)$ with unique normal form property and g be a many sorted function from $\mathrm{Free}_\Sigma(X)$ into $\mathrm{Free}_\Sigma(X)$. Suppose g is a homomorphism of $\mathrm{Free}_\Sigma(X)$ into $\mathrm{Free}_\Sigma(X)$. Let s be a sort symbol of Σ and a be an element of $\mathrm{Free}_\Sigma(X)$ from s. Then $\mathrm{nf}_{R(s)}(g(s)(\mathrm{nf}_{R(s)}(a))) = \mathrm{nf}_{R(s)}(g(s)(a))$.

(81) For every finite sequence p holds $p_{\restriction 0} = p$ and for every natural number i such that $i \geq \operatorname{len} p$ holds $p_{\restriction i} = \emptyset$.

(82) For all finite sequences p, q holds $p \frown \langle x \rangle \frown q +\cdot (\operatorname{len} p + 1, y) = p \frown \langle y \rangle \frown q$.

(83) For every finite sequence p and for every natural number i such that $i+1 \leq \operatorname{len} p$ holds $p{\restriction}(i+1) = (p{\restriction}i) \mathbin{^\frown} \langle p(i+1)\rangle$.

(84) For every finite sequence p and for every natural number i such that $i+1 \leq \operatorname{len} p$ holds $p_{\downharpoonleft i} = \langle p(i+1)\rangle \mathbin{^\frown} (p_{\downharpoonleft i+1})$.

(85) Let R be a terminating invariant stable many sorted relation indexed by $\mathrm{Free}_\Sigma(X)$ with unique normal form property and g be a many sorted function from $\mathrm{Free}_\Sigma(X)$ into $\mathrm{Free}_\Sigma(X)$. Suppose g is a homomorphism of $\mathrm{Free}_\Sigma(X)$ into $\mathrm{Free}_\Sigma(X)$. Let h be a many sorted function from the algebra of normal forms of R into the algebra of normal forms of R. Suppose that for every sort symbol s of Σ and for every element x of the algebra of normal forms of R from s holds $h(s)(x) = \mathrm{nf}_{R(s)}(g(s)(x))$. Let s be a sort symbol of Σ and o be an operation symbol of Σ. Suppose $s =$ the result sort of o. Let x be an element of $\mathrm{Args}(o,$the algebra of normal forms of $R)$ and y be an element of $\mathrm{Args}(o, \mathrm{Free}_\Sigma(X))$. Suppose $x = y$. Then $\mathrm{nf}_{R(s)}((\mathrm{Den}(o,$the algebra of normal forms of $R))(h\#x)) = \mathrm{nf}_{R(s)}((\mathrm{Den}(o, \mathrm{Free}_\Sigma(X)))(g\#y))$.

Let us consider Σ, X and let R be a terminating invariant stable many sorted relation indexed by $\mathrm{Free}_\Sigma(X)$ with unique normal form property. One can verify that the algebra of normal forms of R is including Σ-terms over X.

Let us consider Σ, X and let R be a terminating invariant stable many sorted relation indexed by $\mathrm{Free}_\Sigma(X)$ with NF-variables and unique normal form property. Note that the algebra of normal forms of R is free in itself, has all variables, and inherits operations.

References

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

[2] Grzegorz Bancerek. Introduction to trees. *Formalized Mathematics*, 1(**2**):421–427, 1990.

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

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

[5] Grzegorz Bancerek. Cartesian product of functions. *Formalized Mathematics*, 2(**4**):547–552, 1991.

[6] Grzegorz Bancerek. König's lemma. *Formalized Mathematics*, 2(**3**):397–402, 1991.

[7] Grzegorz Bancerek. Sets and functions of trees and joining operations of trees. *Formalized Mathematics*, 3(**2**):195–204, 1992.

[8] Grzegorz Bancerek. Joining of decorated trees. *Formalized Mathematics*, 4(**1**):77–82, 1993.

[9] Grzegorz Bancerek. Reduction relations. *Formalized Mathematics*, 5(**4**):469–478, 1996.

[10] Grzegorz Bancerek. Subtrees. *Formalized Mathematics*, 5(**2**):185–190, 1996.

[11] Grzegorz Bancerek. Terms over many sorted universal algebra. *Formalized Mathematics*, 5(**2**):191–198, 1996.

[12] Grzegorz Bancerek. Translations, endomorphisms, and stable equational theories. *Formalized Mathematics*, 5(**4**):553–564, 1996.

[13] Grzegorz Bancerek. Algebra of morphisms. *Formalized Mathematics*, 6(**2**):303–310, 1997.

[14] Grzegorz Bancerek. Institution of many sorted algebras. Part I: Signature reduct of an algebra. *Formalized Mathematics*, 6(**2**):279–287, 1997.

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

[16] Grzegorz Bancerek and Artur Korniłowicz. Yet another construction of free algebra. *Formalized Mathematics*, 9(**4**):779–785, 2001.

[17] Grzegorz Bancerek and Piotr Rudnicki. On defining functions on trees. *Formalized Mathematics*, 4(**1**):91–101, 1993.

[18] Grzegorz Bancerek and Piotr Rudnicki. The set of primitive recursive functions. *Formalized Mathematics*, 9(**4**):705–720, 2001.

[19] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

[20] Ewa Burakowska. Subalgebras of many sorted algebra. Lattice of subalgebras. *Formalized Mathematics*, 5(**1**):47–54, 1996.

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

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

[23] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

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

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

[26] Artur Korniłowicz. Some basic properties of many sorted sets. *Formalized Mathematics*, 5(**3**):395–399, 1996.

[27] Artur Korniłowicz. Equations in many sorted algebras. *Formalized Mathematics*, 6(**3**):363–369, 1997.

[28] Małgorzata Korolkiewicz. Homomorphisms of many sorted algebras. *Formalized Mathematics*, 5(**1**):61–65, 1996.

[29] Małgorzata Korolkiewicz. Many sorted quotient algebra. *Formalized Mathematics*, 5(**1**):79–84, 1996.

[30] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.

[31] Adam Naumowicz. On Segre's product of partial line spaces. *Formalized Mathematics*, 9(**2**):383–390, 2001.

[32] Andrzej Nędzusiak. Probability. *Formalized Mathematics*, 1(**4**):745–749, 1990.

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

[34] Beata Perkowska. Free many sorted universal algebra. *Formalized Mathematics*, 5(**1**):67–74, 1996.

[35] D.M. Gabbay S. Abramsky and T.S.E. Maibaum, editors. *Handbook of Logic in Computer Science*, chapter Term Rewriting Systems, pages 1–116. Oxford University Press, New York, 1992. `http://www.informatik.uni-bremen.de/agbkb/lehre/-rbs/texte/Klop-TR.pdf`.

[36] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[37] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.

[38] Andrzej Trybulec. Many sorted algebras. *Formalized Mathematics*, 5(**1**):37–42, 1996.

[39] Andrzej Trybulec. A scheme for extensions of homomorphisms of many sorted algebras. *Formalized Mathematics*, 5(**2**):205–209, 1996.

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

[41] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

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

[43] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Received May 15, 2012