Contents

Formaliz. Math. 22 (**2**)

Special Issue: 25 years of the Mizar Mathematical Library

Volume 22 **2014**

2

Formalized Mathematics

(a computer assisted approach)

University of Białystok

ISSN 1426 - 2630

Special Issue: 25 years of the Mizar Mathematical Library

Volume 22 2014

2

Formalized Mathematics

(a computer assisted approach)

University of Białystok

ISSN 1426 - 2630

Formalized Mathematics
Established in 1990.
In the years 1990 – 1993 published by the
Université Catholique de Louvain.

All papers are checked by the Mizar system, automatically translated into English and automatically typset in LaTeX.

ISSN 1426 – 2630.

This issue has been supported by the *Foundation for Informatics, Logic and Mathematics*, Warsaw, Poland.

Formalized Mathematics

This publication was automatically translated into English and automatically typeset using LaTeX and mizTeX interface system (implemented by G. Bancerek).

Formalized Mathematics is issued quarterly and publishes *Mizar articles* contributed to the Mizar Mathematical Library (MML).

Preparation of the papers. All articles should be written in *Mizar* language and checked by the Mizar system, followed by a bibliography file which summarizes the article, address of the author(s), MML identifier, financial support etc. Articles should be submitted to:

Adam Grabowski,
Association of Mizar Users,
ul.Akademicka 2,
15-267 Białystok, Poland,
e-mail: mml@mizar.uwb.edu.pl
http://mizar.org

All papers are reviewed by at least three experts from the relevant field (double-blind review process). The reviewing process is described in detail in the following paper, pp.239-240:
http://dx.doi.org/10.1007/978-3-540-73086-6_20 .

Questions or comments concerning subscriptions, correspondence, including changes of address should be addressed to:

Foundation for Informatics, Logic and Mathematics
Krochmalna 3/917
00-864 Warsaw
Poland

fax: +48 85 745.74.78
e-mail: romat@mizar.org

Available electronically at
http://www.degruyter.com/view/j/forma
Open Access Policy: this journal provides immediate open access to its content.

Contents

Formaliz. Math. 22 (**2**)

Preface

25 years ago, at the beginning of 1989, the Mizar Mathematical Library (MML) was started.

To celebrate 25 years of the Mizar Mathematical Library, the Editorial Board of *Formalized Mathematics* have decided to dedicate a Special Issue collecting articles of considerable importance to the field of formally verified mathematics.

Amongst the papers published in this Special Issue, there are formalizations of four problems from the *Formalizing 100 Theorems* list maintained by Freek Wiedijk at `http://www.cs.ru.nl/F.Wiedijk/100/` :

#19 `Four Squares Theorem`: page 109, *Lagrange's Four-Square Theorem* by Yasushige Watase, theorem (18), statement in Mizar:

```
theorem ::LAGRA4SQ:18
for n be Nat holds ex x1,x2,x3,x4 be Nat st n = x1^2 + x2^2 +
x3^2 + x4^2 ;
```

#30 `The Ballot Problem`: page 122, *Bertrand's Ballot Theorem* by Karol Pąk, theorem (28), statement in Mizar:

```
theorem ::BALLOT_1:28
A <> B & n >= k implies prob DominatedElection(A,n,B,k) =
(n-k) / (n+k) ;
```

#38 `Arithmetic Mean/Geometric Mean`: page 165, *Cauchy Mean Theorem* by Adam Grabowski, theorem (47), statement in Mizar:

```
theorem ::RVSUM_3:47
for f being non empty positive real-valued FinSequence holds
GMean f <= Mean f ;
```

#54 `Konigsberg Bridges Problem`: page 178, *A Note on the Seven Bridges of Königsberg Problem* by Adam Naumowicz, theorem (5), statement in Mizar:

```
theorem ::GRAPH_3A:5
not ex p being Path of KoenigsbergBridges st p is cyclic
Eulerian ;
```

The Editors

Special Issue: 25 years of the Mizar Mathematical Library

FORMALIZED MATHEMATICS
Vol. 22, No. 2, Pages 99–103, 2014
DOI: 10.2478/forma-2014-0011

DE GRUYTER OPEN
degruyter.com/view/j/forma

Pseudo-Canonical Formulae are Classical

Marco B. Caminati[1]
School of Computer Science
University of Birmingham
Birmingham, B15 2TT
United Kingdom

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

Summary. An original result about Hilbert Positive Propositional Calculus introduced in [11] is proven. That is, it is shown that the pseudo-canonical formulae of that calculus (and hence also the canonical ones, see [17]) are a subset of the classical tautologies.

MSC: 03B20 03B35

Keywords: Hilbert positive propositional calculus; classical logic; canonical formulae

MML identifier: `HILBERT4`, version: `8.1.03 5.23.1207`

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

1. Preliminaries about Injectivity, Involutiveness, Fixed Points

From now on a, b, c, x, y, z, A, B, C, X, Y denote sets, f, g denote functions, V denotes a SetValuation, P denotes a permutation of V, p, q, r, s denote elements of HP-WFF, and n denotes an element of $\mathbb{N}$.

Let us consider X and Y. Let f be a relation between X and Y. Note that $\mathrm{id}_X \cdot f$ reduces to f and $f \cdot \mathrm{id}_Y$ reduces to f.

Now we state the proposition:

(1) Let us consider one-to-one functions f, g. If $f^{-1} = g^{-1}$, then $f = g$.

[1] My work has been partially supported by EPSRC grant EP/J007498/1 and an LMS Computer Science Small Grant.

ISSN 1426–2630(Print), 1898-9934(Online)

One can verify that there exists a function which is involutive.

Let us consider A. Let us observe that there exists a permutation of A which is involutive.

Now we state the propositions:

(2) Let us consider an involutive function f. Suppose $\operatorname{rng} f \subseteq \operatorname{dom} f$. Then $f \cdot f = \mathrm{id}_{\operatorname{dom} f}$.

(3) Let us consider a function f. If $f \cdot f = \mathrm{id}_{\operatorname{dom} f}$, then f is involutive.

(4) Let us consider an involutive function f from A into A. Then $f \cdot f = \mathrm{id}_A$. The theorem is a consequence of (2).

(5) Let us consider a function f from A into A. If $f \cdot f = \mathrm{id}_A$, then f is involutive. The theorem is a consequence of (3).

Observe that every function which is involutive is also one-to-one.

Let us consider A. Let f be an involutive permutation of A. One can verify that f^{-1} is involutive.

Let n be a non zero natural number. Observe that $[0 \longmapsto n, n \longmapsto 0]$ is without fixpoints.

Let z be a zero natural number. Note that $\operatorname{fixpoints}[z \longmapsto n, n \longmapsto z]$ is empty.

Let X be a non empty set. Observe that there exists a permutation of X which is non empty and involutive.

Let us consider A and B. Let f be an involutive function from A into A and g be an involutive function from B into B. Observe that $f \times g$ is involutive.

Let A, B be non empty sets, f be an involutive permutation of A, and g be an involutive permutation of B. Observe that $f \Rightarrow g$ is involutive.

2. Facts about Perm's Fixed Points

Now we state the propositions:

(6) If x is a fixpoint of $\operatorname{Perm}(P, q)$, then $\operatorname{SetVal}(V, p) \longmapsto x$ is a fixpoint of $\operatorname{Perm}(P, p \Rightarrow q)$.

(7) If $\operatorname{Perm}(P, q)$ has fixpoints, then $\operatorname{Perm}(P, p \Rightarrow q)$ has fixpoints. The theorem is a consequence of (6).

(8) If $\operatorname{Perm}(P, p)$ has fixpoints and $\operatorname{Perm}(P, q)$ is without fixpoints, then $\operatorname{Perm}(P, p \Rightarrow q)$ is without fixpoints.

3. Axiom of Choice in Functional Form via the Fraenkel Operator

Let X be a set. The functor $\operatorname{ChoiceOn} X$ yielding a set is defined by the term

(Def. 1) $\{\langle x, \text{the element of } x\rangle, \text{ where } x \text{ is an element of } X \setminus \{\emptyset\} : x \in X \setminus \{\emptyset\}\}$.

One can check that ChoiceOn X is relation-like and function-like.

Let us consider f. The functor FieldCover f yielding a set is defined by the term

(Def. 2) $\{\{x, f(x)\}$, where x is an element of $\operatorname{dom} f : x \in \operatorname{dom} f\}$.

The functor SomePoints f yielding a set is defined by the term

(Def. 3) field $f \setminus \operatorname{rng}$ ChoiceOn FieldCover f.

The functor OtherPoints f yielding a set is defined by the term

(Def. 4) (field $f \setminus$ fixpoints $f) \setminus$ SomePoints f.

Let us consider g. Let us observe that OtherPoints $g \cap$SomePoints g is empty.

4. Building a Suitable Set Valuation and a Suitable Permutation of It

Let us consider x. The functor ToHilb(x) yielding a set is defined by the term

(Def. 5) $(\mathrm{id}_1 {+\cdot} (1 \times \emptyset^x) \cdot (\emptyset^x \times \{1\})) {+\cdot} (\{1\} \times \emptyset^x) \cdot (\emptyset^x \times \{0\})$.

Note that ToHilb(x) is function-like and relation-like.

Now we state the propositions:

(9) If $x \neq \emptyset$, then ToHilb$(x) = \mathrm{id}_1$.

(10) ToHilb$(\emptyset) = [0 \longmapsto 1, 1 \longmapsto 0]$.

Let v be a function. The functor ToHilbPerm(v) yielding a set is defined by the term

(Def. 6) the set of all $\langle n$, ToHilb$(v(n))\rangle$ where n is an element of $\mathbb{N}$.

The functor ToHilbVal(v) yielding a set is defined by the term

(Def. 7) the set of all $\langle n$, dom ToHilb$(v(n))\rangle$ where n is an element of $\mathbb{N}$.

One can check that ToHilbVal(v) is function-like and relation-like and ToHilbPerm (v) is function-like and relation-like and ToHilbVal(v) is $\mathbb{N}$-defined and ToHilbVal(v) is total and ToHilbPerm(v) is $\mathbb{N}$-defined and ToHilbPerm(v) is total.

One can verify that ToHilbVal(v) is non-empty.

Let us consider x. Let us note that ToHilb(x) is symmetric.

Let v be a function. Observe that the functor ToHilbPerm(v) yields a permutation of ToHilbVal(v).

A set valuation is a many sorted set indexed by $\mathbb{N}$. From now on v denotes a set valuation.

Let us consider p and v. Note that Perm(ToHilbPerm$(v), p)$ is involutive.

5. Classical Semantics via SetVal_0, an Extension of SetVal

Let V be a set valuation. The functor $\mathrm{SetVal}_0\, V$ yielding a many sorted set indexed by HP-WFF is defined by

(Def. 8) (i) $it(\mathrm{VERUM}) = 1$, and

(ii) for every n, $it(\mathrm{prop}\, n) = V(n)$, and

(iii) for every p and q, $it(p \wedge q) = it(p) \times it(q)$ and $it(p \Rightarrow q) = (it(q))^{it(p)}$.

Let us consider v and p. The functor $\mathrm{SetVal}_0(v, p)$ yielding a set is defined by the term

(Def. 9) $(\mathrm{SetVal}_0\, v)(p)$.

We say that p is classical if and only if

(Def. 10) $\mathrm{SetVal}_0(v, p) \neq \emptyset$.

One can check that every element of HP-WFF which is pseudo-canonical is also classical.

Let us consider v. Let p be a classical element of HP-WFF. Note that $\mathrm{SetVal}_0(v, p)$ is non empty.

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] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[4] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[5] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.
[6] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.
[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] Marco B. Caminati. Preliminaries to classical first order model theory. *Formalized Mathematics*, 19(**3**):155–167, 2011. doi:10.2478/v10037-011-0025-2.
[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[11] Adam Grabowski. Hilbert positive propositional calculus. *Formalized Mathematics*, 8(**1**): 69–72, 1999.
[12] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[13] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.
[14] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.
[15] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.
[16] Andrzej Trybulec. Defining by structural induction in the positive propositional language. *Formalized Mathematics*, 8(**1**):133–137, 1999.
[17] Andrzej Trybulec. The canonical formulae. *Formalized Mathematics*, 9(**3**):441–447, 2001.
[18] Andrzej Trybulec. Classes of independent partitions. *Formalized Mathematics*, 9(**3**): 623–625, 2001.

[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[20] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[21] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[22] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Received May 25, 2014

Special Issue: 25 years of the Mizar Mathematical Library

FORMALIZED MATHEMATICS
Vol. 22, No. 2, Pages 105–110, 2014
DOI: 10.2478/forma-2014-0012

DE GRUYTER OPEN
degruyter.com/view/j/forma

Lagrange's Four-Square Theorem

Yasushige Watase
Suginami-ku Matsunoki 6
3-21 Tokyo, Japan

Summary. This article provides a formalized proof of the so-called "the four-square theorem", namely any natural number can be expressed by a sum of four squares, which was proved by Lagrange in 1770. An informal proof of the theorem can be found in the number theory literature, e.g. in [14], [1] or [23].

This theorem is item `#19` from the "Formalizing 100 Theorems" list maintained by Freek Wiedijk at `http://www.cs.ru.nl/F.Wiedijk/100/` .

MSC: 11P99 03B35

Keywords: Lagrange's four-square theorem

MML identifier: `LAGRA4SQ`, version: `8.1.03 5.23.1207`

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

1. Preliminaries

Let n be a natural number. We say that n is a sum of four squares if and only if

(Def. 1) There exist natural numbers n_1, n_2, n_3, n_4 such that $n = {n_1}^{\mathbf{2}} + {n_2}^{\mathbf{2}} + {n_3}^{\mathbf{2}} + {n_4}^{\mathbf{2}}$.

Note that there exists a natural number which is a sum of four squares.

Let y be an integer object. Let us note that $|y|$ is natural.

Now we state the proposition:

(1) Let us consider natural numbers n_1, n_2, n_3, n_4, m_1, m_2, m_3, m_4. Then $({n_1}^{\mathbf{2}} + {n_2}^{\mathbf{2}} + {n_3}^{\mathbf{2}} + {n_4}^{\mathbf{2}}) \cdot ({m_1}^{\mathbf{2}} + {m_2}^{\mathbf{2}} + {m_3}^{\mathbf{2}} + {m_4}^{\mathbf{2}}) = (n_1 \cdot m_1 - n_2 \cdot m_2 - n_3 \cdot m_3 - n_4 \cdot m_4)^{\mathbf{2}} + (n_1 \cdot m_2 + n_2 \cdot m_1 + n_3 \cdot m_4 - n_4 \cdot m_3)^{\mathbf{2}} + (n_1 \cdot m_3 - n_2 \cdot m_4 + n_3 \cdot m_1 + n_4 \cdot m_2)^{\mathbf{2}} + (n_1 \cdot m_4 + n_2 \cdot m_3 - n_3 \cdot m_2 + n_4 \cdot m_1)^{\mathbf{2}}$.

ISSN 1426–2630(Print), 1898-9934(Online)

Let m, n be natural numbers. Let us note that $m \cdot n$ is a sum of four squares and there exists a prime natural number which is odd.

From now on i, j, k, v, w denote natural numbers, j_1, j_2, m, n, s, t, x, y denote integers, and p denotes an odd prime natural number.

Let us consider p. The functor ModMap(p) yielding a function from $\mathbb{Z}$ into $\mathbb{Z}_p$ is defined by

(Def. 2) Let us consider an element x of $\mathbb{Z}$. Then $it(x) = x \bmod p$.

Let us consider v. The functor Lag4SqF(v) yielding a finite sequence of elements of $\mathbb{Z}$ is defined by

(Def. 3) (i) $\operatorname{len} it = v$, and

(ii) for every natural number i such that $i \in \operatorname{dom} it$ holds $it(i) = (i-1)^{\mathbf{2}}$.

The functor Lag4SqG(v) yielding a finite sequence of elements of $\mathbb{Z}$ is defined by

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

(ii) for every natural number i such that $i \in \operatorname{dom} it$ holds $it(i) = -1 - (i-1)^{\mathbf{2}}$.

Now we state the propositions:

(2) Lag4SqF(v) is one-to-one.

(3) Lag4SqG(v) is one-to-one.

In the sequel a denotes a real number and b denotes an integer.

Let us consider an odd prime natural number p, a natural number s, j_1, and j_2. Now we state the propositions:

(4) If $2 \cdot s = p + 1$ and j_1, $j_2 \in \operatorname{rng}$ Lag4SqF(s), then $j_1 = j_2$ or $j_1 \bmod p \neq j_2 \bmod p$. PROOF: Consider s such that $p+1 = 2 \cdot s$. For every integers j_1, j_2 such that j_1, $j_2 \in \operatorname{rng}$ Lag4SqF(s) and $j_1 \neq j_2$ holds $j_1 \bmod p \neq j_2 \bmod p$ by [21, (3), (55)], [16, (80)], [18, (22)]. $\square$

(5) If $2 \cdot s = p + 1$ and j_1, $j_2 \in \operatorname{rng}$ Lag4SqG(s), then $j_1 = j_2$ or $j_1 \bmod p \neq j_2 \bmod p$. PROOF: Consider s such that $p + 1 = 2 \cdot s$. For every j_1 and j_2 such that j_1, $j_2 \in \operatorname{rng}$ Lag4SqG(s) and $j_1 \neq j_2$ holds $j_1 \bmod p \neq j_2 \bmod p$ by [21, (3), (55)], [16, (80)], [20, (7)]. $\square$

2. Any Prime Number can be Expressed as a Sum of Four Squares

Now we state the propositions:

(6) There exist natural numbers x_1, x_2, x_3, x_4, h such that

(i) $0 < h < p$, and

(ii) $h \cdot p = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$.

Proof: Consider s such that $2 \cdot s = p + 1$. Set $f = \mathrm{Lag4SqF}(s)$. Set $g = \mathrm{Lag4SqG}(s)$. f is one-to-one. g is one-to-one. $\operatorname{rng} f$ misses $\operatorname{rng} g$. $\overline{\overline{\operatorname{rng}(g \frown f)}} = p + 1$ by [2, (70)], [6, (57), (31)], [3, (35), (36)]. Set $A = \operatorname{dom}(\mathrm{ModMap}(p) \restriction \operatorname{rng}(g \frown f))$. Set $B = \operatorname{rng}(\mathrm{ModMap}(p) \restriction \operatorname{rng}(g \frown f))$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists an element m_1 of $\mathbb{Z}$ such that $\$_1 \in A$ and $\$_2 = m_1$ and $(\mathrm{ModMap}(p) \restriction \operatorname{rng}(g \frown f))(\$_1) = m_1$. For every object x such that $x \in A$ there exists an object y such that $y \in B$ and $\mathcal{P}[x, y]$ by [8, (3)]. Consider h being a function from A into B such that for every object x such that $x \in A$ holds $\mathcal{P}[x, h(x)]$ from [9, Sch. 1]. Consider m_1, m_2 being objects such that $m_1 \in A$ and $m_2 \in A$ and $m_1 \neq m_2$ and $h(m_1) = h(m_2)$. If $m_1 \in \operatorname{rng} f$, then $m_2 \in \operatorname{rng} g$. If $m_1 \in \operatorname{rng} g$, then $m_2 \in \operatorname{rng} f$. There exist natural numbers x_1, x_2, x_3, x_4, h such that $h > 0$ and $h < p$ and $h \cdot p = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$ by [20, (7)], [21, (3)]. □

(7) Let us consider natural numbers x_1, h. Suppose $1 < h$. Then there exists an integer y_1 such that

(i) $x_1 \bmod h = y_1 \bmod h$, and

(ii) $-h < 2 \cdot y_1 \leqslant h$, and

(iii) ${x_1}^{\mathbf{2}} \bmod h = {y_1}^{\mathbf{2}} \bmod h$.

Proof: Consider q_1, r_1 being integers such that $x_1 = h \cdot q_1 + r_1$ and $0 \leqslant r_1$ and $r_1 < h$. There exists an integer y_1 such that $x_1 \bmod h = y_1 \bmod h$ and $-h < 2 \cdot y_1 \leqslant h$ and ${x_1}^{\mathbf{2}} \bmod h = {y_1}^{\mathbf{2}} \bmod h$ by [21, (3)], [18, (23)]. □

(8) Let us consider natural numbers i_1, i_2, c. If $i_1 \leqslant c$ and $i_2 \leqslant c$, then $i_1 + i_2 < 2 \cdot c$ or $i_1 = c$ and $i_2 = c$.

(9) Let us consider natural numbers i_1, i_2, i_3, i_4, c. Suppose

(i) $i_1 \leqslant c$, and

(ii) $i_2 \leqslant c$, and

(iii) $i_3 \leqslant c$, and

(iv) $i_4 \leqslant c$.

Then

(v) $i_1 + i_2 + i_3 + i_4 < 4 \cdot c$, or

(vi) $i_1 = c$ and $i_2 = c$ and $i_3 = c$ and $i_4 = c$.

The theorem is a consequence of (8).

Let us consider natural numbers x_1, h and an integer y_1. Now we state the propositions:

(10) Suppose $1 < h$ and $x_1 \bmod h = y_1 \bmod h$ and $-h < 2 \cdot y_1$ and $(2 \cdot y_1)^{\mathbf{2}} = h^{\mathbf{2}}$. Then

(i) $2 \cdot y_1 = h$, and

(ii) there exists a natural number m_1 such that $2 \cdot x_1 = (2 \cdot m_1 + 1) \cdot h$.

(11) If $1 < h$ and $x_1 \bmod h = y_1 \bmod h$ and $y_1 = 0$, then there exists an integer m_1 such that $x_1 = h \cdot m_1$.

Now we state the proposition:

(12) Let us consider an odd prime number p and natural numbers x_1, x_2, x_3, x_4, h. Suppose

(i) $1 < h < p$, and

(ii) $h \cdot p = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$.

Then there exist integers y_1, y_2, y_3, y_4 and there exists a natural number r such that $0 < r < h$ and $r \cdot p = {y_1}^{\mathbf{2}} + {y_2}^{\mathbf{2}} + {y_3}^{\mathbf{2}} + {y_4}^{\mathbf{2}}$. The theorem is a consequence of (7), (9), (10), and (11).

Let us consider a prime number p. Now we state the propositions:

(13) If p is even, then $p = 2$.

(14) There exist natural numbers x_1, x_2, x_3, x_4 such that $p = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$.

Now we state the proposition:

(15) Let us consider prime numbers p_1, p_2. Then there exist natural numbers x_1, x_2, x_3, x_4 such that $p_1 \cdot p_2 = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$. The theorem is a consequence of (14).

Let p_1, p_2 be prime numbers. Let us observe that $p_1 \cdot p_2$ is a sum of four squares.

Now we state the proposition:

(16) Let us consider a prime number p and a natural number n. Then there exist natural numbers x_1, x_2, x_3, x_4 such that $p^n = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ there exist natural numbers x_1, x_2, x_3, x_4 such that $p^{\$_1} = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by (14), [7, (75)], [16, (6)]. $\mathcal{P}[0]$ by [16, (4)]. For every natural number n, $\mathcal{P}[n]$ from [4, Sch. 2]. $\square$

Let p be a prime number and n be a natural number. Observe that p^n is a sum of four squares.

3. Proof of Lagrange's theorem

Now we state the proposition:

(17) Let us consider a non zero natural number n. Then there exist natural numbers x_1, x_2, x_3, x_4 such that $\prod \mathrm{PPF}(n) = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every non zero natural number n such that $\overline{\overline{\mathrm{support\,PPF}(n)}} = \$_1$ there exist natural numbers x_1, x_2, x_3, x_4 such that $\prod \mathrm{PPF}(n) = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$. $\mathcal{P}[0]$ by [15, (20)]. For

every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [15, (34), (28), (25)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. $\square$

Now we state the proposition:

(18) Lagrange's four-square theorem:
Let us consider a natural number n. Then there exist natural numbers x_1, x_2, x_3, x_4 such that $n = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$. The theorem is a consequence of (17).

One can verify that every natural number is a sum of four squares.

References

[1] Alan Baker. *A Concise Introduction to the Theory of Numbers.* Cambridge University Press, 1984.

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

[3] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 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. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 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] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.

[14] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, 1980.

[15] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.

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

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

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

[19] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[20] Christoph Schwarzweller. Modular integer arithmetic. *Formalized Mathematics*, 16(**3**): 247–252, 2008. doi:10.2478/v10037-008-0029-8.

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

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

[23] Hideo Wada. *The World of Numbers (in Japanese).* Iwanami Shoten, 1984.

[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 June 4, 2014

Special Issue: 25 years of the Mizar Mathematical Library

FORMALIZED MATHEMATICS
Vol. 22, No. 2, Pages 111–118, 2014
DOI: 10.2478/forma-2014-0013

DE GRUYTER OPEN
degruyter.com/view/j/forma

Proth Numbers

Christoph Schwarzweller
WSB Schools of Banking
Gdańsk, Poland

Summary. In this article we introduce Proth numbers and prove two theorems on such numbers being prime [3]. We also give revised versions of Pocklington's theorem and of the Legendre symbol. Finally, we prove Pepin's theorem and that the fifth Fermat number is not prime.

MSC: 11A41 03B35

Keywords: prime numbers; Pocklington's theorem; Proth's theorem; Pepin's theorem

MML identifier: NAT_6, version: 8.1.03 5.23.1207

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

1. Preliminaries

Let n be a positive natural number. Let us note that $n-1$ is natural.

Let n be a non trivial natural number. Observe that $n-1$ is positive.

Let x be an integer number and n be a natural number. Let us observe that x^n is integer.

Let us observe that 1^n reduces to 1.

Let n be an even natural number. Let us observe that $(-1)^n$ reduces to 1.

Let n be an odd natural number. One can verify that $(-1)^n$ reduces to -1.

Now we state the propositions:

(1) Let us consider a positive natural number a and natural numbers n, m. If $n \geqslant m$, then $a^n \geqslant a^m$.

(2) Let us consider a non trivial natural number a and natural numbers n, m. If $n > m$, then $a^n > a^m$. The theorem is a consequence of (1).

ISSN 1426–2630(Print), 1898-9934(Online)

(3) Let us consider a non zero natural number n. Then there exists a natural number k and there exists an odd natural number l such that $n = l \cdot 2^k$.

(4) Let us consider an even natural number n. Then $n \operatorname{div} 2 = \frac{n}{2}$.

(5) Let us consider an odd natural number n. Then $n \operatorname{div} 2 = \frac{n-1}{2}$.

Let n be an even integer number. Let us observe that $\frac{n}{2}$ is integer.

Let n be an even natural number. One can check that $\frac{n}{2}$ is natural.

2. Some Properties of Congruences and Prime Numbers

Let us observe that every natural number which is prime is also non trivial.

Now we state the propositions:

(6) Let us consider a prime natural number p and an integer number a. Then $\gcd(a, p) \neq 1$ if and only if $p \mid a$.

(7) Let us consider integer numbers i, j and a prime natural number p. If $p \mid i \cdot j$, then $p \mid i$ or $p \mid j$. The theorem is a consequence of (6).

(8) Let us consider prime natural numbers x, p and a non zero natural number k. Then $x \mid p^k$ if and only if $x = p$.

(9) Let us consider integer numbers x, y, n. Then $x \equiv y \pmod{n}$ if and only if there exists an integer k such that $x = k \cdot n + y$.

(10) Let us consider an integer number i and a non zero integer number j. Then $i \equiv i \bmod j \pmod{j}$.

(11) Let us consider integer numbers x, y and a positive integer number n. Then $x \equiv y \pmod{n}$ if and only if $x \bmod n = y \bmod n$. The theorem is a consequence of (9) and (10).

(12) Let us consider integer numbers i, j and a natural number n. If $n < j$ and $i \equiv n \pmod{j}$, then $i \bmod j = n$.

(13) Let us consider a non zero natural number n and an integer number x. Then $x \equiv 0 \pmod{n}$ or ... or $x \equiv n - 1 \pmod{n}$. The theorem is a consequence of (10).

(14) Let us consider a non zero natural number n, an integer number x, and natural numbers k, l. Suppose
   (i) $k < n$, and
   (ii) $l < n$, and
   (iii) $x \equiv k \pmod{n}$, and
   (iv) $x \equiv l \pmod{n}$.

   Then $k = l$. The theorem is a consequence of (12).

(15) Let us consider an integer number x. Then
   (i) $x^2 \equiv 0 \pmod{3}$, or

(ii) $x^2 \equiv 1 \pmod{3}$.

The theorem is a consequence of (13).

(16) Let us consider a prime natural number p, elements x, y of $\mathbb{Z}/p\mathbb{Z}^*$, and integer numbers i, j. If $x = i$ and $y = j$, then $x \cdot y = i \cdot j \bmod p$.

(17) Let us consider a prime natural number p, an element x of $\mathbb{Z}/p\mathbb{Z}^*$, an integer number i, and a natural number n. If $x = i$, then $x^n = i^n \bmod p$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv x^{\$_1} = i^{\$_1} \bmod p$. For every natural number k, $\mathcal{P}[k]$ from [1, Sch. 2]. □

(18) Let us consider a prime natural number p and an integer number x. Then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. The theorem is a consequence of (7).

(19) Let us consider a natural number n. Then $-1 \equiv 1 \pmod{n}$ if and only if $n = 2$ or $n = 1$.

(20) Let us consider an integer number i. Then $-1 \equiv 1 \pmod{i}$ if and only if $i = 2$ or $i = 1$ or $i = -2$ or $i = -1$. The theorem is a consequence of (19).

3. Some basic properties of relation “>”

Let n, x be natural numbers. We say that x is greater than n if and only if

(Def. 1) $x > n$.

Let n be a natural number. Observe that there exists a natural number which is greater than n and odd and there exists a natural number which is greater than n and even.

Let us observe that every natural number which is greater than n is also n or greater.

One can check that every natural number which is $(n+1)$ or greater is also n or greater and every natural number which is greater than $(n+1)$ is also greater than n and every natural number which is greater than n is also $(n+1)$ or greater.

Let m be a non trivial natural number. One can verify that every natural number which is m or greater is also non trivial.

Let a be a positive natural number, m be a natural number, and n be an m or greater natural number. Let us note that a^n is a^m or greater.

Let a be a non trivial natural number. Let n be a greater than m natural number. Let us observe that a^n is greater than a^m and every natural number which is 2 or greater is also non trivial and every natural number which is non trivial is also 2 or greater and every natural number which is non trivial and odd is also greater than 2.

Let n be a greater than 2 natural number. One can verify that $n - 1$ is non trivial.

Let n be a 2 or greater natural number. Let us observe that $n-2$ is natural.

Let m be a non zero natural number and n be an m or greater natural number. One can check that $n-1$ is natural and every prime natural number which is greater than 2 is also odd.

Let n be a natural number. One can check that there exists a natural number which is greater than n and prime.

4. Pocklington's Theorem Revisited

Let n be a natural number.

A divisor of n is a natural number and is defined by

(Def. 2) $it \mid n$.

Let n be a non trivial natural number. One can check that there exists a divisor of n which is non trivial.

Note that every divisor of n is non zero.

Let n be a positive natural number. One can verify that every divisor of n is positive.

Let n be a non zero natural number. Observe that every divisor of n is n or smaller.

Let us note that there exists a divisor of n which is prime.

Let n be a natural number and q be a divisor of n. Let us note that $\frac{n}{q}$ is natural.

Let s be a divisor of n and q be a divisor of s. Let us note that $\frac{n}{q}$ is natural.

Now we state the proposition:

(21) Pocklington's theorem:
Let us consider a greater than 2 natural number n and a non trivial divisor s of $n-1$. Suppose
 (i) $s > \sqrt{n}$, and
 (ii) there exists a natural number a such that $a^{n-1} \equiv 1 \pmod{n}$ and for every prime divisor q of s, $\gcd(a^{\frac{n-1}{q}} - 1, n) = 1$.

Then n is prime.

5. Euler's Criterion

Let a be an integer number and p be a natural number.

Now we state the propositions:

(22) Let us consider a positive natural number p and an integer number a. Then a is quadratic residue modulo p if and only if there exists an integer number x such that $x^2 \equiv a \pmod{p}$. Proof: If a is quadratic residue

modulo p, then there exists an integer number x such that $x^2 \equiv a \pmod{p}$ by [13, (59)], [8, (81)]. $\square$

(23) 2 is quadratic non residue modulo 3. The theorem is a consequence of (15), (14), and (22).

Let p be a natural number and a be an integer number. The Legendre symbol(a,p) yielding an integer number is defined by the term

$$\text{(Def. 3)} \quad \begin{cases} 1, & \textbf{if } \gcd(a,p) = 1 \text{ and } a \text{ is quadratic residue modulo } p \text{ and } p \neq 1, \\ 0, & \textbf{if } p \mid a, \\ -1, & \textbf{if } \gcd(a,p) = 1 \text{ and } a \text{ is quadratic non residue modulo } p \text{ and} \\ & p \neq 1. \end{cases}$$

Let p be a prime natural number. Note that the Legendre symbol(a,p) is defined by the term

$$\text{(Def. 4)} \quad \begin{cases} 1, & \textbf{if } \gcd(a,p) = 1 \text{ and } a \text{ is quadratic residue modulo } p, \\ 0, & \textbf{if } p \mid a, \\ -1, & \textbf{if } \gcd(a,p) = 1 \text{ and } a \text{ is quadratic non residue modulo } p. \end{cases}$$

Let p be a natural number. We introduce $(\frac{a}{p})$ as a synonym of the Legendre symbol(a,p).

Let us consider a prime natural number p and an integer number a. Now we state the propositions:

(24) (i) $(\frac{a}{p}) = 1$, or

(ii) $(\frac{a}{p}) = 0$, or

(iii) $(\frac{a}{p}) = -1$.

Proof: $\gcd(a,p) = 1$ by [9, (21)]. $\square$

(25) (i) $(\frac{a}{p}) = 1$ iff $\gcd(a,p) = 1$ and a is quadratic residue modulo p, and

(ii) $(\frac{a}{p}) = 0$ iff $p \mid a$, and

(iii) $(\frac{a}{p}) = -1$ iff $\gcd(a,p) = 1$ and a is quadratic non residue modulo p.

The theorem is a consequence of (6).

Now we state the propositions:

(26) Let us consider a natural number p. Then $(\frac{p}{p}) = 0$.

(27) Let us consider an integer number a. Then $(\frac{a}{2}) = a \bmod 2$. The theorem is a consequence of (22).

Let us consider a greater than 2 prime natural number p and integer numbers a, b. Now we state the propositions:

(28) If $\gcd(a,p) = 1$ and $\gcd(b,p) = 1$ and $a \equiv b \pmod{p}$, then $(\frac{a}{p}) = (\frac{b}{p})$.

(29) If $\gcd(a,p) = 1$ and $\gcd(b,p) = 1$, then $(\frac{a \cdot b}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$.

Now we state the proposition:

(30) Let us consider greater than 2 prime natural numbers p, q. Suppose $p \neq q$. Then $(\frac{p}{q}) \cdot (\frac{q}{p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$. The theorem is a consequence of (4).

Now we state the proposition:

(31) Euler's criterion:
Let us consider a greater than 2 prime natural number p and an integer number a. Suppose $\gcd(a,p) = 1$. Then $a^{\frac{p-1}{2}} \equiv$ the Legendre symbol(a,p) $\pmod p$. The theorem is a consequence of (4).

6. Proth Numbers

Let p be a natural number. We say that p is Proth if and only if

(Def. 5) There exists an odd natural number k and there exists a positive natural number n such that $2^n > k$ and $p = k \cdot 2^n + 1$.

One can check that there exists a natural number which is Proth and prime and there exists a natural number which is Proth and non prime and every natural number which is Proth is also non trivial and odd.

Now we state the propositions:

(32) 3 is Proth.

(33) 5 is Proth.

(34) 9 is Proth.

(35) 13 is Proth.

(36) 17 is Proth.

(37) 641 is Proth.

(38) 11777 is Proth.

(39) 13313 is Proth.

Now we state the proposition:

(40) Proth's theorem - version 1:
Let us consider a Proth natural number n. Then n is prime if and only if there exists a natural number a such that $a^{\frac{n-1}{2}} \equiv -1 \pmod n$. The theorem is a consequence of (1), (8), (20), (21), (17), (10), (12), and (18).

Now we state the propositions:

(41) Proth's theorem - version 2:
Let us consider a 2 or greater natural number l and a positive natural number k. Suppose
  (i) $3 \nmid k$, and
  (ii) $k \leqslant 2^l - 1$.
Then $k \cdot 2^l + 1$ is prime if and only if $3^{k \cdot 2^{l-1}} \equiv -1 \pmod{k \cdot 2^l + 1}$. The theorem is a consequence of (1), (8), (20), (21), (15), (6), (13), (30), (28), (23), and (31).

(42) 641 is prime. The theorem is a consequence of (40) and (37).

7. Fermat Numbers

Let l be a natural number. Note that Fermat l is Proth.

Now we state the propositions:

(43) Pepin's theorem:

Let us consider a non zero natural number l. Then Fermat l is prime if and only if $3^{\frac{\mathrm{Fermat}\, l-1}{2}} \equiv -1 \pmod{\mathrm{Fermat}\, l}$. The theorem is a consequence of (1), (4), and (41).

(44) Fermat 5 is not prime. The theorem is a consequence of (2).

8. Cullen Numbers

Let n be a natural number. The Cullen number of n yielding a natural number is defined by the term

(Def. 6) $n \cdot 2^n + 1$.

Let n be a non zero natural number. Let us observe that the Cullen number of n is Proth.

References

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

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

[3] J. Buchmann and V. Müller. Primality testing. 1992.

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

[5] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.

[6] Yuichi Futa, Hiroyuki Okazaki, Daichi Mizushima, and Yasunari Shidama. Operations of points on elliptic curve in projective coordinates. *Formalized Mathematics*, 20(**1**):87–95, 2012. doi:10.2478/v10037-012-0012-2.

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

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

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

[10] Hiroyuki Okazaki and Yasunari Shidama. Uniqueness of factoring an integer and multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$. *Formalized Mathematics*, 16(**2**):103–107, 2008. doi:10.2478/v10037-008-0015-1.

[11] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[12] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

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

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

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

[16] Li Yan, Xiquan Liang, and Junjie Zhao. Gauss lemma and law of quadratic reciprocity. *Formalized Mathematics*, 16(**1**):23–28, 2008. doi:10.2478/v10037-008-0004-4.

Received June 9, 2014

Special Issue: 25 years of the Mizar Mathematical Library

FORMALIZED MATHEMATICS
Vol. 22, No. 2, Pages 119–123, 2014
DOI: 10.2478/forma-2014-0014

DE GRUYTER OPEN
degruyter.com/view/j/forma

Bertrand's Ballot Theorem[1]

Karol Pąk
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

Summary. In this article we formalize the Bertrand's Ballot Theorem based on [17]. Suppose that in an election we have two candidates: A that receives n votes and B that receives k votes, and additionally $n \geqslant k$. Then this theorem states that the probability of the situation where A maintains more votes than B throughout the counting of the ballots is equal to $(n-k)/(n+k)$.

This theorem is item `#30` from the "Formalizing 100 Theorems" list maintained by Freek Wiedijk at `http://www.cs.ru.nl/F.Wiedijk/100/` .

MSC: 60C05 03B35

Keywords: ballot theorem; probability

MML identifier: `BALLOT_1`, version: `8.1.03 5.23.1210`

The notation and terminology used in this paper have been introduced in the following articles: [24], [1], [14], [15], [18], [4], [5], [10], [21], [6], [12], [3], [11], [25], [26], [16], [8], [13], [23], and [9].

1. Preliminaries

From now on D, D_1, D_2 denote non empty sets, d, d_1, d_2 denote finite 0-sequences of D, and n, k, i, j denote natural numbers.

Now we state the propositions:

(1) $\mathrm{XFS2FS}(d \restriction n) = \mathrm{XFS2FS}(d) \restriction n$.

(2) $\mathrm{rng}\, d = \mathrm{rng}\, \mathrm{XFS2FS}(d)$.

(3) Let us consider a finite 0-sequence d_1 of D_1 and a finite 0-sequence d_2 of D_2. If $d_1 = d_2$, then $\mathrm{XFS2FS}(d_1) = \mathrm{XFS2FS}(d_2)$.

[1]The paper has been financed by the resources of the Polish National Science Centre granted by decision no DEC-2012/07/N/ST6/02147.

ISSN 1426–2630(Print), 1898-9934(Online)

(4) If $\mathrm{XFS2FS}(d_1) = \mathrm{XFS2FS}(d_2)$, then $d_1 = d_2$. PROOF: For every i such that $i < \mathrm{len}\, d_1$ holds $d_1(i) = d_2(i)$ by [2, (13), (11)]. $\square$

(5) Let us consider a finite sequence d of elements of D. Then $\mathrm{XFS2FS}(\mathrm{FS2XFS}(d)) = d$.

(6) Let us consider a finite sequence f and objects x, y. Suppose

(i) $\mathrm{rng}\, f \subseteq \{x, y\}$, and

(ii) $x \neq y$.

Then $\overline{\overline{f^{-1}(\{x\})}} + \overline{\overline{f^{-1}(\{y\})}} = \mathrm{len}\, f$.

(7) Let us consider functions f, g. Suppose f is one-to-one. Let us consider an object x. If $x \in \mathrm{dom}\, f$, then $\mathrm{Coim}(f \cdot g, f(x)) = \mathrm{Coim}(g, x)$. PROOF: Set $f_3 = f \cdot g$. $\mathrm{Coim}(f_3, f(x)) \subseteq \mathrm{Coim}(g, x)$ by [6, (11), (12)]. $\square$

(8) Let us consider a real number r and a real-valued finite sequence f. Suppose $\mathrm{rng}\, f \subseteq \{0, r\}$. Then $\sum f = r \cdot \overline{\overline{f^{-1}(\{r\})}}$. PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every real-valued finite sequence f such that $\mathrm{len}\, f = \$_1$ and $\mathrm{rng}\, f \subseteq \{0, r\}$ holds $\sum f = r \cdot \overline{\overline{f^{-1}(\{r\})}}$. $\mathcal{P}[0]$ by [8, (72)]. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [22, (55)], [8, (74)], [25, (70)], [2, (11)]. For every n, $\mathcal{P}[n]$ from [2, Sch. 2]. $\square$

2. Properties of Elections

In the sequel A, B denote objects, v denotes an element of $\{A, B\}^{n+k}$, and f, g denote finite sequences.

Let us consider A, n, B, and k. The functor $\mathrm{Election}(A, n, B, k)$ yielding a subset of $\{A, B\}^{n+k}$ is defined by

(Def. 1) $v \in it$ if and only if $\overline{\overline{v^{-1}(\{A\})}} = n$.

Let us note that $\mathrm{Election}(A, n, B, k)$ is finite. Now we state the propositions:

(9) $\mathrm{Election}(A, n, A, 0) = \{n \mapsto A\}$. PROOF: $\mathrm{Election}(A, n, A, 0) \subseteq \{n \mapsto A\}$ by [19, (29)], [9, (33)], [21, (9)]. $\square$

(10) If $k > 0$, then $\mathrm{Election}(A, n, A, k)$ is empty.

Let us consider A and n. Let k be a non empty natural number. Let us observe that $\mathrm{Election}(A, n, A, k)$ is empty. Now we state the proposition:

(11) $\mathrm{Election}(A, n, B, k) = \mathrm{Choose}(\mathrm{Seg}(n+k), n, A, B)$. PROOF: $\mathrm{Election}(A, n, B, k) \subseteq \mathrm{Choose}(\mathrm{Seg}(n+k), n, A, B)$ by [7, (2)]. $\square$

Let us assume that $A \neq B$. Now we state the propositions:

(12) $v \in \mathrm{Election}(A, n, B, k)$ if and only if $\overline{\overline{v^{-1}(\{B\})}} = k$. The theorem is a consequence of (6).

(13) $\overline{\overline{\mathrm{Election}(A, n, B, k)}} = \binom{n+k}{n}$. The theorem is a consequence of (11).

3. Properties of Dominated Elections

Let us consider A, n, B, and k. Let v be a finite sequence. We say that v is an (A, n, B, k)-dominated-election if and only if

(Def. 2) (i) $v \in \text{Election}(A, n, B, k)$, and

(ii) for every i such that $i > 0$ holds $\overline{\overline{(v{\restriction}i)^{-1}(\{A\})}} > \overline{\overline{(v{\restriction}i)^{-1}(\{B\})}}$.

Let us assume that f is an (A, n, B, k)-dominated-election. Now we state the propositions:

(14) $A \neq B$.

(15) $n > k$. The theorem is a consequence of (14) and (12).

Now we state the propositions:

(16) If $A \neq B$ and $n > 0$, then $n \mapsto A$ is an (A, n, B, 0)-dominated-election.

(17) If f is an (A, n, B, k)-dominated-election and $i < n-k$, then $f \frown (i \mapsto B)$ is an (A, n, B, $(k+i)$)-dominated-election. The theorem is a consequence of (14) and (12).

(18) Suppose f is an (A, n, B, k)-dominated-election and g is an (A, i, B, j)-dominated-election. Then $f \frown g$ is an (A, $(n+i)$, B, $(k+j)$)-dominated-election. The theorem is a consequence of (14), (12), and (15).

Let us consider A, n, B, and k. The functor DominatedElection(A, n, B, k) yielding a subset of Election(A, n, B, k) is defined by

(Def. 3) $f \in it$ if and only if f is an (A, n, B, k)-dominated-election.

(19) If $A = B$ or $n \leqslant k$, then DominatedElection(A, n, B, k) is empty. The theorem is a consequence of (14) and (15).

(20) If $n > k$ and $A \neq B$, then $n \mapsto A \frown (k \mapsto B) \in$ DominatedElection(A, n, B, k). The theorem is a consequence of (17) and (16).

(21) If $A \neq B$, then $\overline{\overline{\text{DominatedElection}(A, n, B, k)}} = \overline{\overline{\text{DominatedElection}(0, n, 1, k)}}$. Proof: Set $T = [A \longmapsto 0, B \longmapsto 1]$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ for every f such that $f = \$_1$ holds $T \cdot f = \$_2$. For every object x such that $x \in$ DominatedElection(A, n, B, k) there exists an object y such that $y \in$ DominatedElection$(0, n, 1, k)$ and $\mathcal{P}[x, y]$ by [25, (27), (26)], [5, (92)], (7). Consider C being a function from DominatedElection(A, n, B, k) into DominatedElection$(0, n, 1, k)$ such that for every object x such that $x \in$ DominatedElection(A, n, B, k) holds $\mathcal{P}[x, C(x)]$ from [7, Sch. 1]. DominatedElection$(0, n, 1, k) \subseteq \operatorname{rng} C$ by [25, (27), (26)], [5, (92)], (7). $\square$

(22) Let us consider a finite sequence p of elements of $\mathbb{N}$. Then p is a (0, n, 1, k)-dominated-election if and only if p is an $(n+k)$-tuple of $\{0, 1\}$ and $n > 0$ and $\sum p = k$ and for every i such that $i > 0$ holds $2 \cdot \sum(p{\restriction}i) < i$. Proof: If p is a (0, n, 1, k)-dominated-election, then p is an $(n+k)$-tuple of $\{0, 1\}$

and $n > 0$ and $\sum p = k$ and for every i such that $i > 0$ holds $2 \cdot \sum (p \restriction i) < i$ by (8), (12), (15), [25, (70)]. $1 \cdot \overline{\overline{p^{-1}(\{1\})}} = k$. $\overline{\overline{p^{-1}(\{1\})}} + \overline{\overline{p^{-1}(\{0\})}} = \operatorname{len} p$. $1 \cdot \overline{\overline{(p \restriction i)^{-1}(\{1\})}} = \sum (p \restriction i)$. $\overline{\overline{(p \restriction i)^{-1}(\{1\})}} + \overline{\overline{(p \restriction i)^{-1}(\{0\})}} = \operatorname{len}(p \restriction i)$. $\square$

(23) If f is an (A, n, B, k)-dominated-election, then $f(1) = A$. The theorem is a consequence of (15).

(24) Let us consider a finite 0-sequence d of $\mathbb{N}$. Then $d \in \mathrm{Domin}_0(n+k, k)$ if and only if $\langle 0 \rangle \frown \mathrm{XFS2FS}(d) \in \mathrm{DominatedElection}(0, n+1, 1, k)$. Proof: Set $X_1 = \mathrm{XFS2FS}(d)$. Set $Z = \langle 0 \rangle$. Set $Z_1 = Z \frown X_1$. Reconsider $D = d$ as a finite 0-sequence of $\mathbb{R}$. $\mathrm{XFS2FS}(d) = \mathrm{XFS2FS}(D)$. If $d \in \mathrm{Domin}_0(n+k, k)$, then $Z_1 \in \mathrm{DominatedElection}(0, n+1, 1, k)$ by [15, (20)], (2), [4, (31), (22)]. Z_1 is an $(n+1+k)$-tuple of $\{0, 1\}$. For every k such that $k \leqslant \operatorname{dom} d$ holds $2 \cdot \sum (d \restriction k) \leqslant k$ by [20, (14)], [8, (76)], (1), (3). d is dominated by 0. $\sum d = k$. $\square$

(25) $\overline{\overline{\mathrm{Domin}_0(n+k, k)}} = \overline{\overline{\mathrm{DominatedElection}(0, n+1, 1, k)}}$. Proof: Set $D = \mathrm{Domin}_0(n+k, k)$. Set $B = \mathrm{DominatedElection}(0, n+1, 1, k)$. Set $Z = \langle 0 \rangle$. Define $\mathcal{F}[\text{object}, \text{object}] \equiv$ for every finite 0-sequence d of $\mathbb{N}$ such that $d = \$_1$ holds $\$_2 = Z \frown \mathrm{XFS2FS}(d)$. For every object x such that $x \in D$ there exists an object y such that $y \in B$ and $\mathcal{F}[x, y]$. Consider f being a function from D into B such that for every object x such that $x \in D$ holds $\mathcal{F}[x, f(x)]$ from [7, Sch. 1]. $\square$

(26) $\overline{\overline{\mathrm{Domin}_0(n+k, k)}} = \overline{\overline{\mathrm{DominatedElection}(0, n+1, 1, k)}}$. Proof: Set $D = \mathrm{Domin}_0(n+k, k)$. Set $B = \mathrm{DominatedElection}(0, n+1, 1, k)$. Set $Z = \langle 0 \rangle$. Define $\mathcal{F}[\text{object}, \text{object}] \equiv$ for every finite 0-sequence d of $\mathbb{N}$ such that $d = \$_1$ holds $\$_2 = Z \frown \mathrm{XFS2FS}(d)$. For every object x such that $x \in D$ there exists an object y such that $y \in B$ and $\mathcal{F}[x, y]$. Consider f being a function from D into B such that for every object x such that $x \in D$ holds $\mathcal{F}[x, f(x)]$ from [7, Sch. 1]. $\square$

(27) If $A \neq B$ and $n > k$, then $\overline{\overline{\mathrm{DominatedElection}(A, n, B, k)}} = \frac{n-k}{n+k} \cdot \binom{n+k}{k}$. The theorem is a consequence of (21) and (26).

4. Main Theorem

(28) Bertrand's Ballot Theorem:
If $A \neq B$ and $n \geqslant k$, then $\mathrm{P}(\mathrm{DominatedElection}(A, n, B, k)) = \frac{n-k}{n+k}$. The theorem is a consequence of (13), (19), and (27).

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. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[11] Artur Korniłowicz. On the real valued functions. *Formalized Mathematics*, 13(**1**):181–187, 2005.
[12] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[13] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[14] Karol Pąk. Cardinal numbers and finite sets. *Formalized Mathematics*, 13(**3**):399–406, 2005.
[15] Karol Pąk. The Catalan numbers. Part II. *Formalized Mathematics*, 14(**4**):153–159, 2006. doi:10.2478/v10037-006-0019-7.
[16] Jan Popiołek. Introduction to probability. *Formalized Mathematics*, 1(**4**):755–760, 1990.
[17] M. Renault. Four proofs of the ballot theorem. *Mathematics Magazine*, 80(5):345–352, December 2007.
[18] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.
[19] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[20] Andrzej Trybulec. On the decomposition of finite sequences. *Formalized Mathematics*, 5 (**3**):317–322, 1996.
[21] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.
[22] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.
[23] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[24] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.
[25] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[26] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received June 13, 2014

Special Issue: 25 years of the Mizar Mathematical Library

FORMALIZED MATHEMATICS
Vol. 22, No. 2, Pages 125–155, 2014
DOI: 10.2478/forma-2014-0015

DE GRUYTER OPEN
degruyter.com/view/j/forma

Term Context

Grzegorz Bancerek
Association of Mizar Users
Białystok, Poland

Summary. Two construction functors: simple term with a variable and compound term with an operation and argument terms and schemes of term induction are introduced. The degree of construction as a number of used operation symbols is defined. Next, the term context is investigated. An x-context is a term which includes a variable x once only. The compound term is x-context iff the argument terms include an x-context once only. The context induction is shown and used many times. As a key concept, the context substitution is introduced. Finally, the translations and endomorphisms are expressed by context substitution.

MSC: 08A35 03B35

Keywords: construction degree; context; translation; endomorphism

MML identifier: `MSAFREE5`, version: `8.1.03 5.23.1210`

The notation and terminology used in this paper have been introduced in the following articles: [1], [2], [3], [4], [6], [43], [24], [22], [26], [53], [33], [45], [27], [28], [29], [8], [25], [9], [51], [39], [46], [47], [41], [48], [23], [10], [11], [49], [36], [37], [12], [13], [14], [15], [31], [50], [34], [55], [56], [16], [38], [54], [17], [18], [19], [20], [21], [35], and [32].

1. Preliminaries

Let Σ be a non empty non void many sorted signature, $\mathfrak{A}$ be a non-empty algebra over Σ, and σ be a sort symbol of Σ.

An element of $\mathfrak{A}$ from σ is an element of (the sorts of $\mathfrak{A}$)(σ). From now on a, b denote objects, I, J denote sets, f denotes a function, R denotes a binary relation, i, j, n denote natural numbers, m denotes an element of $\mathbb{N}$, Σ denotes a non empty non void many sorted signature, σ, σ_1, σ_2 denote sort symbols of Σ, o denotes an operation symbol of Σ, X denotes a non-empty many sorted set

ISSN 1426–2630(Print), 1898-9934(Online)

indexed by the carrier of Σ, x, x_1, x_2 denote elements of $X(\sigma)$, x_{11} denotes an element of $X(\sigma_1)$, T denotes a free in itself including Σ-terms over X algebra over Σ with all variables and inheriting operations, g denotes a translation in $\mathfrak{F}_\Sigma(X)$ from σ_1 into σ_2, and h denotes an endomorphism of $\mathfrak{F}_\Sigma(X)$.

Let us consider Σ and X. Let T be an including Σ-terms over X algebra over Σ with all variables and ρ be an element of T. The functor ${}^@\rho$ yielding an element of $\mathfrak{F}_\Sigma(X)$ is defined by the term

(Def. 1) ρ.

Let us consider T. Observe that every element of T is finite and every set which is natural-membered is also $\subseteq$-linear.

In the sequel ρ, ρ_1, ρ_2 denote elements of T and τ, τ_1, τ_2 denote elements of $\mathfrak{F}_\Sigma(X)$.

Let us consider Σ. Let $\mathfrak{A}$ be an algebra over Σ. Let us consider a. We say that $a \in \mathfrak{A}$ if and only if

(Def. 2) $a \in \bigcup(\text{the sorts of } \mathfrak{A})$.

Let us consider b. We say that b is a-different if and only if

(Def. 3) $b \neq a$.

Let I be a non trivial set. Note that there exists an element of I which is a-different.

Now we state the proposition:

(1) Let us consider trees τ, τ_1 and finite sequences p, q of elements of $\mathbb{N}$. Suppose
  - (i) $p \in \tau$, and
  - (ii) $q \in \tau \text{ with-replacement}(p, \tau_1)$.

  Then
  - (iii) if $p \not\preceq q$, then $q \in \tau$, and
  - (iv) for every finite sequence ρ of elements of $\mathbb{N}$ such that $q = p \frown \rho$ holds $\rho \in \tau_1$.

  PROOF: If $p \not\preceq q$, then $q \in \tau$ by [17, (1)]. $\square$

Let R be a finite binary relation. Let us consider a. Let us note that $\mathrm{Coim}(R, a)$ is finite.

Let us consider finite sequences p, q, ρ. Now we state the propositions:

(2) If $p \frown q \preceq \rho$, then $p \preceq \rho$.

(3) If $p \frown q \preceq p \frown \rho$, then $q \preceq \rho$.

Now we state the propositions:

(4) Let us consider finite sequences p, q. Suppose $i \leqslant \operatorname{len} p$. Then $(p \frown q) \restriction \operatorname{Seg} i = p \restriction \operatorname{Seg} i$.

(5) Let us consider finite sequences p, q, ρ. If $q \preceq p \frown \rho$, then $q \preceq p$ or $p \preceq q$. The theorem is a consequence of (4).

Let us consider Σ. We say that Σ is sufficiently rich if and only if

(Def. 4) There exists o such that $\sigma \in \operatorname{rng} \operatorname{Arity}(o)$.

We say that Σ is growable if and only if

(Def. 5) There exists τ such that $\operatorname{height} \operatorname{dom} \tau = n$.

Let us consider n. We say that Σ is n-ary operation including if and only if

(Def. 6) There exists o such that $\operatorname{len} \operatorname{Arity}(o) = n$.

Let us note that there exists a non empty non void many sorted signature which is n-ary operation including and there exists a non empty non void many sorted signature which is sufficiently rich.

Let us consider R. We say that R is nontrivial if and only if

(Def. 7) If $I \in \operatorname{rng} R$, then I is not trivial.

We say that R is infinite-yielding if and only if

(Def. 8) If $I \in \operatorname{rng} R$, then I is infinite.

Let us observe that every binary relation which is nontrivial is also non-empty and every binary relation which is infinite-yielding is also nontrivial.

Let I be a set. Observe that there exists a many sorted set indexed by I which is infinite-yielding and there exists a finite sequence which is infinite-yielding.

Let I be a non empty set, f be a nontrivial many sorted set indexed by I, and a be an element of I. Let us note that $f(a)$ is non trivial.

Let f be an infinite-yielding many sorted set indexed by I. Note that $f(a)$ is infinite.

Let us consider Σ, X, and o. Let us note that every element of $\operatorname{Args}(o, \mathfrak{F}_\Sigma(X))$ is decorated tree yielding.

In the sequel Y denotes an infinite-yielding many sorted set indexed by the carrier of Σ, y, y_1 denote elements of $Y(\sigma)$, y_{11} denotes an element of $Y(\sigma_1)$, Q denotes a free in itself including Σ-terms over Y algebra over Σ with all variables and inheriting operations, q, q_1 denote elements of $\operatorname{Args}(o, \mathfrak{F}_\Sigma(Y))$, u, $u1$, $u2$ denote elements of Q, v, v_1, v_2 denote elements of $\mathfrak{F}_\Sigma(Y)$, Z denotes a nontrivial many sorted set indexed by the carrier of Σ, z, z_1 denote elements of $Z(\sigma)$, l, $l1$ denote elements of $\mathfrak{F}_\Sigma(Z)$, R denotes a free in itself including Σ-terms over Z algebra over Σ with all variables and inheriting operations, and k, $k1$ denote elements of $\operatorname{Args}(o, \mathfrak{F}_\Sigma(Z))$.

Let p be a finite sequence. Note that $p \frown \emptyset$ reduces to p and $\emptyset \frown p$ reduces to p.

Let I be a finite sequence-membered set. The functor $p \frown I$ yielding a set is defined by the term

(Def. 9) $\{p \frown q$, where q is an element of $I : q \in I\}$.

Let us observe that $p \frown I$ is finite sequence-membered.

Let f be a finite sequence and E be an empty set. One can verify that $f \frown E$ reduces to E.

Let p be a decorated tree yielding finite sequence. Let us consider a. Let us note that $p(a)$ is relation-like and every set which is tree-like is also finite sequence-membered.

Let p be a decorated tree yielding finite sequence. Let us consider a. One can check that $\mathrm{dom}(p(a))$ is finite sequence-membered.

Let τ, τ_1 be trees. One can check that τ_1 with-replacement$(\varepsilon_{\mathbb{N}}, \tau)$ reduces to τ.

Let d, d_1 be decorated trees. One can check that d_1 with-replacement$(\varepsilon_{\mathbb{N}}, d)$ reduces to d.

Now we state the proposition:

(6) Let us consider finite sequences ξ, w of elements of $\mathbb{N}$, tree yielding finite sequences p, q, and trees d, τ. Suppose

(i) $i < \mathrm{len}\, p$, and

(ii) $\xi = \langle i \rangle \frown w$, and

(iii) $d = p(i+1)$, and

(iv) $q = p +\cdot (i+1, d \text{ with-replacement}(w, \tau))$, and

(v) $\xi \in \overbrace{p}$.

Then $\overbrace{p}$ with-replacement$(\xi, \tau) = \overbrace{q}$. The theorem is a consequence of (2).

Let F be a function yielding function and f be a function. Let us consider a. Note that $F +\cdot (a, f)$ is function yielding.

Now we state the propositions:

(7) Let us consider a function yielding function F and a function f. Then $\mathrm{dom}_\kappa(F +\cdot (a, f))(\kappa) = \mathrm{dom}_\kappa F(\kappa) +\cdot (a, \mathrm{dom}\, f)$.

(8) Let us consider finite sequences ξ, w of elements of $\mathbb{N}$, decorated tree yielding finite sequences p, q, and decorated trees d, τ. Suppose

(i) $i < \mathrm{len}\, p$, and

(ii) $\xi = \langle i \rangle \frown w$, and

(iii) $d = p(i+1)$, and

(iv) $q = p +\cdot (i+1, d \text{ with-replacement}(w, \tau))$, and

(v) $\xi \in \overbrace{\mathrm{dom}_\kappa\, p(\kappa)}$.

Then $(a\text{-tree}(p))$ with-replacement$(\xi, \tau) = a\text{-tree}(q)$. The theorem is a consequence of (7), (6), (2), and (3).

(9) Let us consider a set a and a decorated tree yielding finite sequence w. Then $\mathrm{dom}(a\text{-tree}(w)) = \{\emptyset\} \cup \bigcup \{\langle i \rangle \frown \mathrm{dom}(w(i+1)) : i < \mathrm{len}\, w\}$. Proof: Set $\mathfrak{A} = \{\langle i \rangle \frown \mathrm{dom}(w(i+1)) : i < \mathrm{len}\, w\}$. $\mathrm{dom}(a\text{-tree}(w)) \subseteq \{\emptyset\} \cup \bigcup \mathfrak{A}$ by [20, (11)]. $\square$

Let p be a decorated tree yielding finite sequence. Let us consider a and I. Note that $p(a)^{-1}(I)$ is finite sequence-membered.

Now we state the proposition:

(10) Let us consider a finite sequence-membered set I and a finite sequence p. Then $\overline{\overline{p \frown I}} = \overline{\overline{I}}$. Proof: Define $\mathcal{F}(\text{element of } I) = p \frown \$_1$. Consider f such that $\operatorname{dom} f = I$ and for every element q of I such that $q \in I$ holds $f(q) = \mathcal{F}(q)$ from [7, Sch. 2]. $\operatorname{rng} f = p \frown I$. f is one-to-one by [22, (33)]. $\square$

Let I be a finite finite sequence-membered set and p be a finite sequence. Note that $p \frown I$ is finite.

Now we state the proposition:

(11) Let us consider finite sequence-membered sets I, J and finite sequences p, q. Suppose

(i) $\operatorname{len} p = \operatorname{len} q$, and

(ii) $p \neq q$.

Then $p \frown I$ misses $q \frown J$.

Let us consider i. Let us note that $\overline{\overline{i}}$ reduces to i. Let us consider j. We identify $i + j$ with $i + j$.

The scheme *CardUnion* deals with a unary functor $\mathcal{I}$ yielding a set and a finite sequence f of elements of $\mathbb{N}$ and states that

(Sch. 1) $\overline{\overline{\bigcup\{\mathcal{I}(i) : i < \operatorname{len} f\}}} = \sum f$

provided

- for every i and j such that $i < \operatorname{len} f$ and $j < \operatorname{len} f$ and $i \neq j$ holds $\mathcal{I}(i)$ misses $\mathcal{I}(j)$ and
- for every i such that $i < \operatorname{len} f$ holds $\overline{\overline{\mathcal{I}(i)}} = f(i+1)$.

Let f be a finite sequence. Note that $\{f\}$ is finite sequence-membered.

Now we state the propositions:

(12) Let us consider finite sequences f, g. Then $f \frown \{g\} = \{f \frown g\}$.

(13) Let us consider finite sequence-membered sets I, J and a finite sequence f. Then $I \subseteq J$ if and only if $f \frown I \subseteq f \frown J$.

In the sequel c, c_1, c_2 denote sets and d, d_1 denote decorated trees.

Now we state the proposition:

(14) Leaves(the elementary tree of 0) $= \{\emptyset\}$.

Let us note that sethood property holds for trees.

Now we state the propositions:

(15) Let us consider a non empty tree yielding finite sequence p. Then $\operatorname{Leaves}(\widehat{p}) = \{\langle i \rangle \frown q$, where q is a finite sequence of elements of $\mathbb{N}, d$ is a tree : $q \in \operatorname{Leaves}(d)$ and $i + 1 \in \operatorname{dom} p$ and $d = p(i+1)\}$.

PROOF: Set i_0 = the element of $\operatorname{dom} p$. Leaves($\widehat{p}$) $\subseteq \{\langle i \rangle \frown q$, where q is a finite sequence of elements of $\mathbb{N}, d$ is a tree : $q \in$ Leaves(d) and $i+1 \in \operatorname{dom} p$ and $d = p(i+1)\}$ by [13, (11), (13)], [52, (25)], [17, (1)].□

(16) Leaves(the root tree of c) = $\{c\}$.

(17) $\operatorname{dom} d \subseteq \operatorname{dom} d_{c \leftarrow d_1}$.

Let us consider c and d. Observe that (the root tree of c)$_{c \leftarrow d}$ reduces to d. Now we state the proposition:

(18) Suppose $c_1 \neq c_2$. Then (the root tree of c_1)$_{c_2 \leftarrow d}$ = the root tree of c_1. PROOF: dom(the root tree of c_1)$_{c_2 \leftarrow d}$ = dom(the root tree of c_1) by [20, (3)], [17, (29)], [40, (15)]. □

Let f be a non empty function yielding function. Note that $\operatorname{dom}_\kappa f(\kappa)$ is non empty and $\operatorname{rng}_\kappa f(\kappa)$ is non empty.

Now we state the proposition:

(19) Let us consider non empty decorated tree yielding finite sequences p, q. Suppose

(i) $\operatorname{dom} q = \operatorname{dom} p$, and

(ii) for every i and d_1 such that $i \in \operatorname{dom} p$ and $d_1 = p(i)$ holds $q(i) = {d_1}_{c \leftarrow d}$.

Then (b-tree(p))$_{c \leftarrow d}$ = b-tree(q). PROOF: Leaves($\overbrace{\operatorname{dom}_\kappa p(\kappa)}$) = $\{\langle i \rangle ^\frown q$, where q is a finite sequence of elements of $\mathbb{N}, d$ is a tree : $q \in$ Leaves(d) and $i+1 \in \operatorname{dom}(\operatorname{dom}_\kappa p(\kappa))$ and $d = (\operatorname{dom}_\kappa p(\kappa))(i+1)\}$. dom($b$-tree($p$))$_{c \leftarrow d}$ = dom(b-tree(q)) by [17, (22)], [13, (11), (13)], [52, (25)]. □

Let us consider Σ and σ. Let $\mathfrak{A}$ be a non empty algebra over Σ and a be an element of $\mathfrak{A}$. We say that a is σ-sort if and only if

(Def. 10) $a \in$ (the sorts of $\mathfrak{A}$)(σ).

Let $\mathfrak{A}$ be a non-empty algebra over Σ. One can verify that there exists an element of $\mathfrak{A}$ which is σ-sort and every element of (the sorts of $\mathfrak{A}$)(σ) is σ-sort.

Let $\mathfrak{A}$ be a non empty algebra over Σ. Assume $\mathfrak{A}$ is disjoint valued. Let a be an element of $\mathfrak{A}$. The functor the sort of a yielding a sort symbol of Σ is defined by

(Def. 11) $a \in$ (the sorts of $\mathfrak{A}$)(it).

Now we state the propositions:

(20) Let us consider a disjoint valued non-empty algebra $\mathfrak{A}$ over Σ and a σ-sort element a of $\mathfrak{A}$. Then the sort of $a = \sigma$.

(21) Let us consider a disjoint valued non empty algebra $\mathfrak{A}$ over Σ. Then every element of $\mathfrak{A}$ is (the sort of a)-sort.

(22) The sort of ${}^@\rho$ = the sort of ρ.

(23) Let us consider an element ρ of (the sorts of T)(σ). Then the sort of $\rho = \sigma$.

(24) Let us consider a term u of Σ over X. Suppose $\tau = u$. Then the sort of $\tau =$ the sort of u.

Let us consider Σ, X, o, and T. One can verify that every element of $\mathrm{Args}(o, T)$ is ($\bigcup$(the sorts of T))-valued.

Now we state the proposition:

(25) Let us consider an element q of $\mathrm{Args}(o, T)$. Suppose $i \in \mathrm{dom}\, q$. Then the sort of $q_i = \mathrm{Arity}(o)_i$.

Let us consider Σ. Let $\mathfrak{A}$, $\mathcal{B}$ be non-empty algebras over Σ and f be a many sorted function from $\mathfrak{A}$ into $\mathcal{B}$. Assume $\mathfrak{A}$ is disjoint valued. Let a be an element of $\mathfrak{A}$. The functor $f(a)$ yielding an element of $\mathcal{B}$ is defined by the term

(Def. 12) f(the sort of a)(a).

Let us consider a disjoint valued non-empty algebra $\mathfrak{A}$ over Σ, a non-empty algebra $\mathcal{B}$ over Σ, a many sorted function f from $\mathfrak{A}$ into $\mathcal{B}$, and an element a of (the sorts of $\mathfrak{A}$)(σ). Now we state the propositions:

(26) $f(a) = f(\sigma)(a)$.

(27) $f(a)$ is an element of (the sorts of $\mathcal{B}$)(σ). The theorem is a consequence of (26).

Now we state the propositions:

(28) Let us consider disjoint valued non-empty algebras $\mathfrak{A}$, $\mathcal{B}$ over Σ, a many sorted function f from $\mathfrak{A}$ into $\mathcal{B}$, and an element a of $\mathfrak{A}$. Then the sort of $f(a) =$ the sort of a.

(29) Let us consider disjoint valued non-empty algebras $\mathfrak{A}$, $\mathcal{B}$ over Σ, a non-empty algebra $\mathcal{C}$ over Σ, a many sorted function f from $\mathfrak{A}$ into $\mathcal{B}$, a many sorted function g from $\mathcal{B}$ into $\mathcal{C}$, and an element a of $\mathfrak{A}$. Then $(g \circ f)(a) = g(f(a))$. The theorem is a consequence of (28).

(30) Let us consider a disjoint valued non-empty algebra $\mathfrak{A}$ over Σ, a non-empty algebra $\mathcal{B}$ over Σ, and many sorted functions f_1, f_2 from $\mathfrak{A}$ into $\mathcal{B}$. If for every element a of $\mathfrak{A}$, $f_1(a) = f_2(a)$, then $f_1 = f_2$. The theorem is a consequence of (26).

Let us consider Σ. Let $\mathfrak{A}$, $\mathcal{B}$ be algebras over Σ. Assume there exists a many sorted function h from $\mathfrak{A}$ into $\mathcal{B}$ such that h is a homomorphism of $\mathfrak{A}$ into $\mathcal{B}$.

A homomorphism from $\mathfrak{A}$ to $\mathcal{B}$ is a many sorted function from $\mathfrak{A}$ into $\mathcal{B}$ and is defined by

(Def. 13) *it* is a homomorphism of $\mathfrak{A}$ into $\mathcal{B}$.

Now we state the proposition:

(31) Let us consider a many sorted function h from $\mathfrak{F}_\Sigma(X)$ into T. Then h is a homomorphism from $\mathfrak{F}_\Sigma(X)$ to T if and only if h is a homomorphism of

$\mathfrak{F}_\Sigma(X)$ into T.

Let us consider Σ, X, and T. Observe that the functor the canonical homomorphism of T yields a homomorphism from $\mathfrak{F}_\Sigma(X)$ to T. Let us consider ρ. One can check that (the canonical homomorphism of T)($^{@}\rho$) reduces to ρ.

Now we state the proposition:

(32) Suppose $\tau_2 =$ (the canonical homomorphism of T)(τ_1). Then (the canonical homomorphism of T)(τ_1) = (the canonical homomorphism of T)(τ_2). The theorem is a consequence of (22) and (28).

2. Constructing Terms

In the sequel w denotes an element of $\mathrm{Args}(o, T)$ and p, p_1 denote elements of $\mathrm{Args}(o, \mathfrak{F}_\Sigma(X))$.

Let us consider Σ, X, σ, and x. The functor x-term yielding an element of (the sorts of $\mathfrak{F}_\Sigma(X)$)(σ) is defined by the term

(Def. 14) The root tree of $\langle x, \sigma\rangle$.

Let us consider o and p. The functor o-term p yielding an element of $\mathfrak{F}_\Sigma(X)$ from the result sort of o is defined by the term

(Def. 15) $\langle o$, the carrier of $\Sigma\rangle$-tree(p).

Now we state the propositions:

(33) The sort of x-term $= \sigma$.

(34) The sort of o-term $p =$ the result sort of o. The theorem is a consequence of (24).

(35) Let us consider an object i. Then $i \in$ (FreeGenerator(T))(σ) if and only if there exists x such that $i = x$-term.

Let us consider Σ, X, σ, and x. Let us note that x-term is non compound.

Let us consider o and p. One can check that o-term p is compound and (the result sort of o)-sort.

Now we state the propositions:

(36) (i) there exists σ and there exists x such that $\tau = x$-term, or

(ii) there exists o and there exists p such that $\tau = o$-term p.

(37) If τ is not compound, then there exists σ and there exists x such that $\tau = x$-term.

(38) If τ is compound, then there exists o and there exists p such that $\tau = o$-term p.

(39) x-term $\neq o$-term p.

Let us consider Σ. Let X be a non-empty many sorted set indexed by the carrier of Σ. Note that there exists an element of $\mathfrak{F}_\Sigma(X)$ which is compound.

Let us consider X. Let e be a compound element of $\mathfrak{F}_\Sigma(X)$. Let us note that the functor main-constr e yields an operation symbol of Σ. One can check that the functor args e yields an element of $\mathrm{Args}(\text{main-constr}\, e, \mathfrak{F}_\Sigma(X))$. Now we state the propositions:

(40) $\mathrm{args}(x\text{-term}) = \emptyset$.

(41) Let us consider a compound element τ of $\mathfrak{F}_\Sigma(X)$.
Then $\tau = \text{main-constr}\, \tau\text{-term}\, \mathrm{args}\, \tau$. The theorem is a consequence of (38).

(42) $x\text{-term} \in T$.

Let us consider Σ, X, T, σ, and x. Note that (the canonical homomorphism of T)(x-term) reduces to x-term.

The scheme *TermInd* deals with a unary predicate $\mathcal{P}$ and a non empty non void many sorted signature Σ and a non-empty many sorted set $\mathcal{X}$ indexed by the carrier of Σ and an element τ of $\mathfrak{F}_\Sigma(\mathcal{X})$ and states that

(Sch. 2) $\mathcal{P}[\tau]$

provided

- for every sort symbol σ of Σ and for every element x of $\mathcal{X}(\sigma)$, $\mathcal{P}[x\text{-term}]$ and

- for every operation symbol o of Σ and for every element p of $\mathrm{Args}(o, \mathfrak{F}_\Sigma(\mathcal{X}))$ such that for every element τ of $\mathfrak{F}_\Sigma(\mathcal{X})$ such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[o\text{-term}\, p]$.

The scheme *TermAlgebraInd* deals with a unary predicate $\mathcal{P}$ and a non empty non void many sorted signature Σ and a non-empty many sorted set $\mathcal{X}$ indexed by the carrier of Σ and a free in itself including Σ-terms over $\mathcal{X}$ algebra $\mathfrak{A}$ over Σ with all variables and inheriting operations and an element τ of $\mathfrak{A}$ and states that

(Sch. 3) $\mathcal{P}[\tau]$

provided

- for every sort symbol σ of Σ and for every element x of $\mathcal{X}(\sigma)$ and for every element ρ of $\mathfrak{A}$ such that $\rho = x\text{-term}$ holds $\mathcal{P}[\rho]$ and

- for every operation symbol o of Σ and for every element p of $\mathrm{Args}(o, \mathfrak{F}_\Sigma(\mathcal{X}))$ and for every element ρ of $\mathfrak{A}$ such that $\rho = o\text{-term}\, p$ and for every element τ of $\mathfrak{A}$ such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[\rho]$.

3. Construction Degree

Let us consider Σ, X, T, and ρ. The functors: the construction degree of ρ and height ρ yielding natural numbers are defined by terms,

(Def. 16) $\overline{\overline{\rho^{-1}(\alpha \times \{\beta\})}}$, where α is the carrier' of Σ and β is the carrier of Σ,

(Def. 17) height dom ρ,

respectively. We introduce $\deg \rho$ as a synonym of the construction degree of ρ.

Now we state the propositions:

(43) $\deg {}^{@}\rho = \deg \rho$.

(44) height ${}^{@}\rho =$ height ρ.

(45) height(x-term) $= 0$.

One can verify that every set which is natural-membered is also ordinal-membered and finite-membered.

Let I be a finite natural-membered set. One can verify that $\bigcup I$ is natural.

Let I be a non empty finite natural-membered set. We identify $\bigcup I$ with $\max I$. Now we state the propositions:

(46) (i) $\{\text{height}\,\tau_1 : \tau_1 \in \text{rng}\,p\}$ is natural-membered and finite, and

(ii) $\bigcup\{\text{height}\,\tau : \tau \in \text{rng}\,p\}$ is a natural number.

Proof: Set $I = \{\text{height}\,\tau : \tau \in \text{rng}\,p\}$. I is natural-membered. Define $\mathcal{F}(\text{element of } \mathfrak{F}_\Sigma(X)) = \text{height}\,\$_1$. $\{\mathcal{F}(\tau_1) : \tau_1 \in \text{rng}\,p\}$ is finite from [44, Sch. 21]. $\square$

(47) Suppose $\text{Arity}(o) \neq \emptyset$ and $n = \bigcup\{\text{height}\,\tau_1 : \tau_1 \in \text{rng}\,p\}$. Then $\text{height}(o\text{-term}\,p) = n + 1$. Proof: Set $I = \{\text{height}\,\tau_1 : \tau_1 \in \text{rng}\,p\}$. I is natural-membered. Define $\mathcal{F}(\text{element of } \mathfrak{F}_\Sigma(X)) = \text{height}\,\$_1$. $\{\mathcal{F}(\tau_1) : \tau_1 \in \text{rng}\,p\}$ is finite from [44, Sch. 21]. $\square$

(48) If $\text{Arity}(o) = \emptyset$, then $\text{height}(o\text{-term}\,p) = 0$.

(49) $\deg(x\text{-term}) = 0$.

(50) $\deg \tau \neq 0$ if and only if there exists o and there exists p such that $\tau = o\text{-term}\,p$. Proof: Define $\mathcal{P}[\text{element of } \mathfrak{F}_\Sigma(X)] \equiv \deg \$_1 \neq 0$ iff there exists o and there exists p such that $\$_1 = o\text{-term}\,p$. $\mathcal{P}[x\text{-term}]$. $\mathcal{P}[\tau]$ from *TermInd*. $\square$

Let τ be a decorated tree. Let us consider I. Observe that $\tau^{-1}(I)$ is finite sequence-membered.

Let us consider a. Let J, K be sets. Let us observe that the functor $\text{IFIN}(a, I, J, K)$ yields a set. Now we state the propositions:

(51) Suppose $J = \langle o, \text{the carrier of } \Sigma \rangle$. Then $(o\text{-term}\,p)^{-1}(I) = \text{IFIN}(J, I, \{\emptyset\}, \emptyset) \cup \bigcup\{\langle i \rangle ^\frown p(i+1)^{-1}(I) : i < \text{len}\,p\}$. Proof: Set $X = \{\langle i \rangle ^\frown p(i+1)^{-1}(I) : i < \text{len}\,p\}$. $(o\text{-term}\,p)^{-1}(I) \subseteq \text{IFIN}(J, I, \{\emptyset\}, \emptyset) \cup \bigcup X$ by [20, (10)], [13, (11), (13)], [52, (25)]. $\square$

(52) Suppose there exists a finite sequence f of elements of $\mathbb{N}$ such that $i = \sum f$ and $\operatorname{dom} f = \operatorname{dom}\operatorname{Arity}(o)$ and for every i and τ such that $i \in \operatorname{dom}\operatorname{Arity}(o)$ and $\tau = p(i)$ holds $f(i) = \deg\tau$. Then $\deg(o\text{-term}\, p) = i+1$.
PROOF: Set $\tau = o$-term p. Set $I =$ (the carrier' of Σ) $\times$ {the carrier of Σ}. Set $\mathfrak{A} = \{\langle i\rangle \frown p(i+1)^{-1}(I) : i < \operatorname{len} p\}$. $\emptyset \notin \bigcup\mathfrak{A}$. $\tau^{-1}(I) = \{\emptyset\} \cup \bigcup\mathfrak{A}$. Define $\mathcal{J}$(natural number) $= \langle \$_1\rangle \frown p(\$_1+1)^{-1}(I)$. For every i and j such that $i < \operatorname{len} f$ and $j < \operatorname{len} f$ and $i \neq j$ holds $\mathcal{J}(i)$ misses $\mathcal{J}(j)$ by [22, (40)], (11). For every i such that $i < \operatorname{len} f$ holds $\overline{\overline{\mathcal{J}(i)}} = f(i+1)$ by [13, (12), (13)], [52, (25)], [12, (2)]. $\overline{\overline{\bigcup\{\mathcal{J}(i) : i < \operatorname{len} f\}}} = \sum f$ from *CardUnion*. □

Let us consider Σ, X, T, and i. The functor $T\deg_{\leqslant} i$ yielding a subset of T is defined by the term

(Def. 18) $\{\rho : \deg\rho \leqslant i\}$.

The functor $T\,\text{height}_{\leqslant} i$ yielding a subset of T is defined by the term

(Def. 19) $\{\tau : \tau \in T$ and height $\tau \leqslant i\}$.

Now we state the propositions:

(53) $\rho \in T\deg_{\leqslant} i$ if and only if $\deg\rho \leqslant i$.

(54) $T\deg_{\leqslant} 0 =$ the set of all x-term. PROOF: $T\deg_{\leqslant} 0 \subseteq$ the set of all x-term by [10, (39)], (36), (50). Consider σ, x such that $a = x$-term. $\deg(x\text{-term}) = 0 \leqslant 0$ and x-term $\in T$. Reconsider $\rho = x$-term as an element of T. $\deg\rho = \deg{}^{@}\rho = 0$. □

(55) $T\,\text{height}_{\leqslant} 0 =$ the set of all x-term $\cup$ $\{o$-term p : o-term $p \in T$ and $\operatorname{Arity}(o) = \emptyset\}$. The theorem is a consequence of (36), (46), (47), (42), and (48).

(56) $T\deg_{\leqslant} 0 = \bigcup$FreeGenerator$(T)$. PROOF: $T\deg_{\leqslant} 0 =$ the set of all x-term. $T\deg_{\leqslant} 0 \subseteq \bigcup$FreeGenerator$(T)$ by [5, (2)]. Consider b such that $b \in \operatorname{dom}$FreeGenerator(T) and $a \in$ (FreeGenerator(T))(b). Consider y being a set such that $y \in X(b)$ and $a =$ the root tree of $\langle y, b\rangle$. □

(57) $\rho \in T\,\text{height}_{\leqslant} i$ if and only if height $\rho \leqslant i$.

Let us consider Σ, X, T, and i. One can check that $T\deg_{\leqslant} i$ is non empty and $T\,\text{height}_{\leqslant} i$ is non empty.

Let us assume that $i \leqslant j$. Now we state the propositions:

(58) $T\deg_{\leqslant} i \subseteq T\deg_{\leqslant} j$.

(59) $T\,\text{height}_{\leqslant} i \subseteq T\,\text{height}_{\leqslant} j$.

Now we state the propositions:

(60) $T\deg_{\leqslant}(i+1) = (T\deg_{\leqslant} 0) \cup \{o$-term p : there exists a finite sequence f of elements of $\mathbb{N}$ such that $i \geqslant \sum f$ and $\operatorname{dom} f = \operatorname{dom}\operatorname{Arity}(o)$ and for every i and τ such that $i \in \operatorname{dom}\operatorname{Arity}(o)$ and $\tau = p(i)$ holds $f(i) = \deg\tau\} \cap \bigcup$(the sorts of T). PROOF: Set $I = \{o$-term p : there exists a finite sequence f of elements of $\mathbb{N}$ such that $i \geqslant \sum f$ and $\operatorname{dom} f =$

dom Arity(o) and for every i and τ such that $i \in$ dom Arity(o) and $\tau = p(i)$ holds $f(i) = \deg \tau\}$. $T \deg_{\leqslant}(i+1) \subseteq (T \deg_{\leqslant} 0) \cup I \cap \bigcup$(the sorts of T) by [10, (39)], (36), (54), [36, (6)]. $T \deg_{\leqslant} 0 \subseteq T \deg_{\leqslant}(i+1)$. $I \cap \bigcup$(the sorts of T) $\subseteq T \deg_{\leqslant}(i+1)$. $\square$

(61) $T\,\mathrm{height}_{\leqslant}(i+1) = (T\,\mathrm{height}_{\leqslant} 0) \cup \{o\text{-term}\, p : \bigcup\{\mathrm{height}\, \tau : \tau \in \mathrm{rng}\, p\} \subseteq i\} \cap \bigcup$(the sorts of T). PROOF: Set $I = \{o\text{-term}\, p : \bigcup\{\mathrm{height}\, \tau : \tau \in \mathrm{rng}\, p\} \subseteq i\}$. $T\,\mathrm{height}_{\leqslant}(i+1) \subseteq (T\,\mathrm{height}_{\leqslant} 0) \cup I \cap \bigcup$(the sorts of T) by (36), (55), (46), (47). $T\,\mathrm{height}_{\leqslant} 0 \subseteq T\,\mathrm{height}_{\leqslant}(i+1)$. $I \cap \bigcup$(the sorts of T) $\subseteq T\,\mathrm{height}_{\leqslant}(i+1)$ by (46), (47), [13, (39)], (48). $\square$

(62) $\deg \tau \geqslant \mathrm{height}\, \tau$. PROOF: Define $\mathcal{P}$[element of $\mathfrak{F}_{\Sigma}(X)$] $\equiv \deg \$_1 \geqslant \mathrm{height}\, \$_1$. For every operation symbol o of Σ and for every element p of $\mathrm{Args}(o, \mathfrak{F}_{\Sigma}(X))$ such that for every element τ of $\mathfrak{F}_{\Sigma}(X)$ such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[o\text{-term}\, p]$ by (48), [36, (6)], (46), [42, (9)]. $\mathcal{P}[\tau]$ from *TermInd*. $\square$

(63) $\bigcup$(the sorts of T) $= \bigcup\{T \deg_{\leqslant} i :$ not contradiction$\}$.

(64) $\bigcup$(the sorts of T) $= \bigcup\{T\,\mathrm{height}_{\leqslant} i :$ not contradiction$\}$. The theorem is a consequence of (57).

(65) $T \deg_{\leqslant} i \subseteq \mathfrak{F}_{\Sigma}(X) \deg_{\leqslant} i$. PROOF: Define $\mathcal{P}$[natural number] $\equiv T \deg_{\leqslant} \$_1 \subseteq \mathfrak{F}_{\Sigma}(X) \deg_{\leqslant} \$_1$. $T \deg_{\leqslant} 0 = \bigcup \mathrm{FreeGenerator}(T)$ and $\mathfrak{F}_{\Sigma}(X) \deg_{\leqslant} 0 = \bigcup \mathrm{FreeGenerator}(\mathfrak{F}_{\Sigma}(X))$. For every i, $\mathcal{P}[i]$ from [13, Sch. 2]. $\square$

4. CONTEXT

Let us consider Σ, X, T, σ, x, and ρ. We say that ρ is x-context if and only if

(Def. 20) $\overline{\overline{\mathrm{Coim}(\rho, \langle x, \sigma \rangle)}} = 1$.

We say that ρ is x-omitting if and only if

(Def. 21) $\mathrm{Coim}(\rho, \langle x, \sigma \rangle) = \emptyset$.

The functor $\mathrm{vf}\, \rho$ yielding a set is defined by the term

(Def. 22) $\pi_1(\mathrm{rng}\, \rho \cap (\bigcup X \times (\text{the carrier of } \Sigma)))$.

Now we state the propositions:

(66) $\mathrm{vf}\, \rho = \bigcup \mathrm{Var}_X\, \rho$. PROOF: $\mathrm{vf}\, \rho \subseteq \bigcup \mathrm{Var}_X\, \rho$ by [32, (87)], [5, (2)], [10, (44)], [23, (9)]. $\square$

(67) $\mathrm{vf}(x\text{-term}) = \{x\}$.

(68) $\mathrm{vf}(o\text{-term}\, p) = \bigcup\{\mathrm{vf}\, \tau : \tau \in \mathrm{rng}\, p\}$. PROOF: $\mathrm{vf}(o\text{-term}\, p) \subseteq \bigcup\{\mathrm{vf}\, \tau : \tau \in \mathrm{rng}\, p\}$ by (66), [5, (2)], [23, (13)], [55, (167)]. $\square$

Let us consider Σ, X, T, and ρ. Note that $\mathrm{vf}\, \rho$ is finite.

Now we state the proposition:

(69) If $x \notin \mathrm{vf}\, \rho$, then ρ is x-omitting.

Let us consider Σ, X, σ, and τ. We say that τ is σ-context if and only if

(Def. 23) There exists x such that τ is x-context.

Let us consider x. Let us observe that every element of $\mathfrak{F}_\Sigma(X)$ which is x-context is also σ-context.

One can verify that x-term is x-context.

One can check that there exists an element of $\mathfrak{F}_\Sigma(X)$ which is x-context and non compound and every element of $\mathfrak{F}_\Sigma(X)$ which is x-omitting is also non x-context.

Now we state the proposition:

(70) Let us consider sort symbols σ_1, σ_2 of Σ, an element x_1 of $X(\sigma_1)$, and an element x_2 of $X(\sigma_2)$. Then $\sigma_1 \neq \sigma_2$ or $x_1 \neq x_2$ if and only if x_1-term is x_2-omitting.

Let us consider Σ, σ, σ_1, Z, and z. Let z' be a z-different element of $Z(\sigma_1)$. One can check that z'-term is z-omitting.

One can check that there exists an element of $\mathfrak{F}_\Sigma(Z)$ which is z-omitting.

Let us consider σ_1. Let z_1 be a z-different element of $Z(\sigma_1)$. Observe that there exists an element of $\mathfrak{F}_\Sigma(Z)$ which is z-omitting and z_1-context.

Let us consider X. Let us consider x.

A context of x is an x-context element of $\mathfrak{F}_\Sigma(X)$. Now we state the proposition:

(71) Let us consider a sort symbol ρ of Σ and an element y of $X(\rho)$. Then x-term is a context of y if and only if $\rho = \sigma$ and $x = y$.

Let us consider Σ, X, and σ.

A context of σ and X is a σ-context element of $\mathfrak{F}_\Sigma(X)$. In the sequel $\mathcal{C}$ denotes a context of x, $\mathcal{C}_1$ denotes a context of y, $\mathcal{C}'$ denotes a context of z, $\mathcal{C}_{11}$ denotes a context of x_{11}, $\mathcal{C}_{12}$ denotes a context of y_{11}, and D denotes a context of σ and X.

Now we state the propositions:

(72) $\mathcal{C}$ is a context of σ and X.

(73) $x \in \mathrm{vf}\,\mathcal{C}$.

Let us consider Σ, o, σ, X, x, and p. We say that p is x-context including once only if and only if

(Def. 24) There exists i such that

(i) $i \in \operatorname{dom} p$, and

(ii) $p(i)$ is a context of x, and

(iii) for every j and τ such that $j \in \operatorname{dom} p$ and $j \neq i$ and $\tau = p(j)$ holds τ is x-omitting.

Let us note that every element of $\mathrm{Args}(o, \mathfrak{F}_\Sigma(X))$ which is x-context including once only is also non empty.

Now we state the propositions:

(74) p is x-context including once only if and only if o-term p is a context of x. PROOF: Set $I = \{\langle x, \sigma\rangle\}$. Set $k = p$. $(o\text{-term}\, k)^{-1}(I) = \emptyset \cup \bigcup\{\langle i\rangle ^\frown k(i+1)^{-1}(I) : i < \operatorname{len} k\}$. If k is x-context including once only, then o-term k is a context of x by [3, (42)], [52, (25)], [13, (10), (13), (11)]. □

(75) for every i such that $i \in \operatorname{dom} p$ holds p_i is x-omitting if and only if o-term p is x-omitting. The theorem is a consequence of (51) and (13).

(76) for every τ such that $\tau \in \operatorname{rng} p$ holds τ is x-omitting if and only if o-term p is x-omitting. The theorem is a consequence of (75).

Let us consider Σ, σ, and o. We say that o is σ-dependent if and only if

(Def. 25) $\sigma \in \operatorname{rng} \operatorname{Arity}(o)$.

Let Σ be a sufficiently rich non void non empty many sorted signature and σ be a sort symbol of Σ. Let us note that there exists an operation symbol of Σ which is σ-dependent.

In the sequel Σ' denotes a sufficiently rich non empty non void many sorted signature, σ' denotes a sort symbol of Σ', o' denotes a σ'-dependent operation symbol of Σ', X' denotes a nontrivial many sorted set indexed by the carrier of Σ', and x' denotes an element of $X'(\sigma')$.

Let us consider Σ', σ', o', X', and x'. Let us observe that there exists an element of $\operatorname{Args}(o', \mathfrak{F}_{\Sigma'}(X'))$ which is x'-context including once only.

Let p' be an x'-context including once only element of $\operatorname{Args}(o', \mathfrak{F}_{\Sigma'}(X'))$. One can check that o'-term p' is x'-context.

Let us consider Σ, o, σ, X, x, and p. Assume p is x-context including once only. The functor the x-context position in p yielding a natural number is defined by

(Def. 26) $p(it)$ is a context of x.

The functor the x-context in p yielding a context of x is defined by

(Def. 27) $it \in \operatorname{rng} p$.

Now we state the propositions:

(77) Suppose p is x-context including once only. Then

(i) the x-context position in $p \in \operatorname{dom} p$, and

(ii) the x-context in $p = p$(the x-context position in p).

(78) Suppose p is x-context including once only and the x-context position in $p \neq i \in \operatorname{dom} p$. Then p_i is x-omitting.

Let us assume that p is x-context including once only. Now we state the propositions:

(79) p yields the x-context in p just once. The theorem is a consequence of (77).

(80) $p \leftarrow$ (the x-context in p) = the x-context position in p. The theorem is a consequence of (79).

Now we state the proposition:

(81) (i) $\mathcal{C} = x$-term, or

(ii) there exists o and there exists p such that p is x-context including once only and $\mathcal{C} = o$-term p.

The theorem is a consequence of (36), (71), and (74).

Let us consider Σ', X', σ', and x'. One can verify that there exists an element of $\mathfrak{F}_{\Sigma'}(X')$ which is x'-context and compound.

The scheme *ContextInd* deals with a unary predicate $\mathcal{P}$ and a non empty non void many sorted signature Σ and a sort symbol σ of Σ and a non-empty many sorted set $\mathcal{X}$ indexed by the carrier of Σ and an element x of $\mathcal{X}(\sigma)$ and a context $\mathcal{C}$ of x and states that

(Sch. 4) $\mathcal{P}[\mathcal{C}]$

provided

- $\mathcal{P}[x\text{-term}]$ and
- for every operation symbol o of Σ and for every element w of $\mathrm{Args}(o, \mathfrak{F}_{\Sigma}(\mathcal{X}))$ such that w is x-context including once only holds if $\mathcal{P}$[the x-context in w], then for every context $\mathcal{C}$ of x such that $\mathcal{C} = o$-term w holds $\mathcal{P}[\mathcal{C}]$.

Now we state the propositions:

(82) If τ is x-omitting, then $\tau_{\langle x,\sigma\rangle \leftarrow \tau_1} = \tau$.

(83) Suppose the sort of $\tau_1 = \sigma$. Then $\tau_{\langle x,\sigma\rangle \leftarrow \tau_1} \in$ (the sorts of $\mathfrak{F}_{\Sigma}(X)$)(the sort of τ). PROOF: Define $\mathcal{P}$[element of $\mathfrak{F}_{\Sigma}(X)$] $\equiv \$_1{}_{\langle x,\sigma\rangle \leftarrow \tau_1} \in$ (the sorts of $\mathfrak{F}_{\Sigma}(X)$)(the sort of $\$_1$). For every σ_1 and for every element y of $X(\sigma_1)$, $\mathcal{P}[y\text{-term}]$. For every o and p such that for every τ_2 such that $\tau_2 \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau_2]$ holds $\mathcal{P}[o\text{-term}\, p]$ by [20, (20)], (18), [52, (29)], [12, (2)]. $\mathcal{P}[\tau]$ from *TermInd*. $\square$

Let us consider Σ, X, σ, x, $\mathcal{C}$, and τ. Assume the sort of $\tau = \sigma$. The functor $\mathcal{C}[\tau]$ yielding an element of (the sorts of $\mathfrak{F}_{\Sigma}(X)$)(the sort of $\mathcal{C}$) is defined by the term

(Def. 28) $\mathcal{C}_{\langle x,\sigma\rangle \leftarrow \tau}$.

Now we state the proposition:

(84) If the sort of $\tau = \sigma$, then x-term$[\tau] = \tau$.

Let us consider Σ, X, σ, x, and $\mathcal{C}$. Observe that $\mathcal{C}[x\text{-term}]$ reduces to $\mathcal{C}$.

Now we state the propositions:

(85) Let us consider an element w of $\mathrm{Args}(o, \mathfrak{F}_{\Sigma}(Z))$ and an element τ of $\mathfrak{F}_{\Sigma}(Z)$. Suppose

(i) w is z-context including once only, and

(ii) the sort of $\tau = \mathrm{Arity}(o)$(the z-context position in w).

Then $w +\cdot$ (the z-context position in $w, \tau) \in \mathrm{Args}(o, \mathfrak{F}_\Sigma(Z))$.

(86) Suppose the sort of $\mathcal{C}' = \sigma_1$. Let us consider a z-different element z_1 of $Z(\sigma_1)$ and a z-omitting context $\mathcal{C}_1$ of z_1. Then $\mathcal{C}_1[\mathcal{C}']$ is a context of z. PROOF: Define $\mathcal{P}$[element of $\mathfrak{F}_\Sigma(Z)] \equiv$ if $\$_1$ is z-omitting, then $\$_{1\langle z_1, \sigma_1\rangle \leftarrow \mathcal{C}'}$ is a context of z. For every o and k such that k is z_1-context including once only holds if $\mathcal{P}$[the z_1-context in k], then for every context $\mathcal{C}$ of z_1 such that $\mathcal{C} = o$-term k holds $\mathcal{P}[\mathcal{C}]$. $\mathcal{P}[\mathcal{C}_1]$ from *ContextInd*. □

(87) Let us consider elements w, p of $\mathrm{Args}(o, \mathfrak{F}_\Sigma(Z))$ and an element τ of $\mathfrak{F}_\Sigma(Z)$. Suppose

(i) w is z-context including once only, and

(ii) $\mathcal{C}' = o$-term w, and

(iii) $p = w +\cdot$ (the z-context position in w, (the z-context in $w)[\tau]$), and

(iv) the sort of $\tau = \sigma$.

Then $\mathcal{C}'[\tau] = o$-term p. The theorem is a consequence of (77), (78), (82), and (19).

(88) The sort of $\mathcal{C}[\tau] =$ the sort of $\mathcal{C}$.

(89) If $\tau(a) = \langle x, \sigma\rangle$, then $a \in \mathrm{Leaves}(\mathrm{dom}\,\tau)$. The theorem is a consequence of (36).

(90) Let us consider a sort symbol σ_0 of Σ and an element x_0 of $X(\sigma_0)$. Suppose

(i) the sort of $\tau = \sigma$, and

(ii) $\mathcal{C}$ is x_0-omitting, and

(iii) τ is x_0-omitting.

Then $\mathcal{C}[\tau]$ is x_0-omitting. The theorem is a consequence of (89).

(91) Suppose p is x-context including once only. Then the sort of the x-context in $p = \mathrm{Arity}(o)$(the x-context position in p). The theorem is a consequence of (77).

(92) Let us consider a disjoint valued non-empty algebra $\mathfrak{A}$ over Σ, a non-empty algebra $\mathcal{B}$ over Σ, an operation symbol o of Σ, elements p, q of $\mathrm{Args}(o, \mathfrak{A})$, a many sorted function h from $\mathfrak{A}$ into $\mathcal{B}$, an element a of $\mathfrak{A}$, and i. Suppose

(i) $i \in \mathrm{dom}\,p$, and

(ii) $q = p +\cdot (i, a)$.

Then $h\#q = h\#p +\cdot (i, h(a))$.

(93) Let us consider an element τ of $\mathfrak{F}_\Sigma(Z)$. Suppose the sort of $\tau = \sigma$. Then (the canonical homomorphism of $R)(\mathcal{C}'[\tau]) =$ (the canonical homomorphism of $R)(\mathcal{C}'[^{@}$((the canonical homomorphism of $R)(\tau))]). PROOF: Set $H =$

the canonical homomorphism of R. Define $\mathcal{P}$[context of z] $\equiv H(\$_1[\tau]) = H(\$_1[{}^{@}(H(\tau))])$. The sort of ${}^{@}(H(\tau))$ = the sort of $H(\tau)$. $\mathcal{P}$[z-term] by (84), [10, (48)], [28, (15)]. $\mathcal{P}[\mathcal{C}']$ from *ContextInd*. $\square$

Let us consider Σ, X, T, σ, and x. Let h be a many sorted function from $\mathfrak{F}_\Sigma(X)$ into T. We say that h is x-constant if and only if

(Def. 29) (i) $h(x\text{-term}) = x\text{-term}$, and

(ii) for every σ_1 and for every element x_1 of $X(\sigma_1)$ such that $x_1 \neq x$ or $\sigma \neq \sigma_1$ holds $h(x_1\text{-term})$ is x-omitting.

Now we state the proposition:

(94) The canonical homomorphism of T is x-constant. The theorem is a consequence of (70).

Let us consider Σ, X, T, σ, and x. Note that there exists a homomorphism from $\mathfrak{F}_\Sigma(X)$ to T which is x-constant.

From now on h_1 denotes an x-constant homomorphism from $\mathfrak{F}_\Sigma(X)$ to T and h_2 denotes a y-constant homomorphism from $\mathfrak{F}_\Sigma(Y)$ to Q.

Let x, y be objects. The functor $x \leftrightarrow y$ yielding a function is defined by the term

(Def. 30) $\{\langle x, y\rangle, \langle y, x\rangle\}$.

Let us observe that the functor is commutative.

Now we state the proposition:

(95) (i) $\mathrm{dom}(a \leftrightarrow b) = \{a, b\}$, and

(ii) $(a \leftrightarrow b)(a) = b$, and

(iii) $(a \leftrightarrow b)(b) = a$, and

(iv) $\mathrm{rng}(a \leftrightarrow b) = \{a, b\}$.

Let $\mathfrak{A}$ be a non empty set and a, b be elements of $\mathfrak{A}$. One can verify that $a \leftrightarrow b$ is $\mathfrak{A}$-valued and $\mathfrak{A}$-defined.

Let $\mathfrak{A}$ be a set, $\mathcal{B}$ be a non empty set, f be a function from $\mathfrak{A}$ into $\mathcal{B}$, and g be a $\mathfrak{A}$-defined $\mathcal{B}$-valued function. Let us note that the functor $f{+}{\cdot}g$ yields a function from $\mathfrak{A}$ into $\mathcal{B}$. Let I be a non empty set, $\mathfrak{A}$, $\mathcal{B}$ be many sorted sets indexed by I, f be a many sorted function from $\mathfrak{A}$ into $\mathcal{B}$, x be an element of I, and g be a function from $\mathfrak{A}(x)$ into $\mathcal{B}(x)$. One can verify that the functor $f +\cdot (x, g)$ yields a many sorted function from $\mathfrak{A}$ into $\mathcal{B}$. Let us consider Σ, X, T, σ, x_1, and x_2. The functor $\mathrm{Hom}(T, x_1, x_2)$ yielding an endomorphism of T is defined by

(Def. 31) (i) $it(\sigma)(x_1\text{-term}) = x_2\text{-term}$, and

(ii) $it(\sigma)(x_2\text{-term}) = x_1\text{-term}$, and

(iii) for every σ_1 and for every element y of $X(\sigma_1)$ such that $\sigma_1 \neq \sigma$ or $y \neq x_1$ and $y \neq x_2$ holds $it(\sigma_1)(y\text{-term}) = y\text{-term}$.

Now we state the propositions:

(96) Let us consider an endomorphism h of T. Suppose $h(\sigma)(x\text{-term}) = x\text{-term}$. Then $h = \mathrm{id}_\alpha$, where α is the sorts of T. PROOF: $h \restriction \mathrm{FreeGenerator}(T) = \mathrm{id}_\alpha \restriction \mathrm{FreeGenerator}(T)$, where α is the sorts of T by [27, (49), (18)]. $\square$

(97) $\mathrm{Hom}(T, x, x) = \mathrm{id}_\alpha$, where α is the sorts of T. The theorem is a consequence of (96).

(98) $\mathrm{Hom}(T, x_1, x_2) = \mathrm{Hom}(T, x_2, x_1)$.

(99) $\mathrm{Hom}(T, x_1, x_2) \circ \mathrm{Hom}(T, x_1, x_2) = \mathrm{id}_\alpha$, where α is the sorts of T. PROOF: Set $h = \mathrm{Hom}(T, x_1, x_2)$. For every σ and x, $(h \circ h)(\sigma)(x\text{-term}) = x\text{-term}$ by [28, (15)], [36, (2)]. $\square$

(100) If ρ is x_1-omitting and x_2-omitting, then $(\mathrm{Hom}(T, x_1, x_2))(\rho) = \rho$. PROOF: Define $\mathcal{P}[\text{element of } T] \equiv$ if $\$_1$ is x_1-omitting and x_2-omitting, then $(\mathrm{Hom}(T, x_1, x_2))(\text{the sort of } \$_1)(\$_1) = \$_1$. For every σ, x, and ρ such that $\rho = x\text{-term}$ holds $\mathcal{P}[\rho]$. For every o, p, and ρ such that $\rho = o\text{-term}\, p$ and for every element τ of T such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[\rho]$ by (22), (34), [10, (13)], [36, (6)]. $\mathcal{P}[\rho]$ from *TermAlgebraInd*. $\square$

Let us consider Σ, X, T, σ, and x. Let us observe that (the canonical homomorphism of T)$(\sigma)(x\text{-term})$ reduces to $x\text{-term}$.

Now we state the propositions:

(101) (The canonical homomorphism of T) $\circ\, \mathrm{Hom}(\mathfrak{F}_\Sigma(X), x, x_1) = \mathrm{Hom}(T, x, x_1) \circ$ (the canonical homomorphism of T). PROOF: Set $H =$ the canonical homomorphism of T. Set $h = \mathrm{Hom}(T, x, x_1)$. Set $g = \mathrm{Hom}(\mathfrak{F}_\Sigma(X), x, x_1)$. Define $\mathcal{P}[\text{element of } \mathfrak{F}_\Sigma(X)] \equiv (H \circ g)(\$_1) = (h \circ H)(\$_1)$. For every σ and x, $\mathcal{P}[x\text{-term}]$ by [36, (2)], [28, (15)]. For every operation symbol o of Σ and for every element p of $\mathrm{Args}(o, \mathfrak{F}_\Sigma(X))$ such that for every element τ of $\mathfrak{F}_\Sigma(X)$ such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[o\text{-term}\, p]$ by [10, (13)], (34), [36, (6)], [52, (29), (25)]. $(H \circ g)(\sigma) = (h \circ H)(\sigma)$. $\square$

(102) Let us consider an element ρ of T from σ. Then $(\mathrm{Hom}(T, x_1, x_2))(\sigma)(\rho) =$ ((the canonical homomorphism of T) $\circ\, \mathrm{Hom}(\mathfrak{F}_\Sigma(X), x_1, x_2))(\sigma)(\rho)$. The theorem is a consequence of (101).

(103) If $x_1 \neq x_2$ and τ is x_2-omitting, then $(\mathrm{Hom}(\mathfrak{F}_\Sigma(X), x_1, x_2))(\tau)$ is x_1-omitting. PROOF: Set $T = \mathfrak{F}_\Sigma(X)$. Set $h = \mathrm{Hom}(T, x_1, x_2)$. Define $\mathcal{P}[\text{element of } T] \equiv$ if $\$_1$ is x_2-omitting, then $h(\$_1)$ is x_1-omitting. For every σ and x, $\mathcal{P}[x\text{-term}]$. For every o and p such that for every element τ of T such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[o\text{-term}\, p]$ by (34), [10, (13)], [36, (6)], [12, (2)]. $\mathcal{P}[\tau]$ from *TermInd*. $\square$

(104) Let us consider a finite subset $\mathfrak{A}$ of $\bigcup$(the sorts of $\mathfrak{F}_\Sigma(Y)$). Then there exists y such that for every v such that $v \in \mathfrak{A}$ holds v is y-omitting. PROOF: Define $\mathcal{F}(\text{element of } \mathfrak{F}_\Sigma(Y)) = \mathrm{vf}\, \$_1$. $\{\mathcal{F}(v) : v \in \mathfrak{A}\}$ is finite from [44, Sch. 21]. $\square$

Let us consider Σ, X, and T. We say that T is structure-invariant if and only if

(Def. 32) Let us consider an element p of $\mathrm{Args}(o,T)$. Suppose $(\mathrm{Den}(o,T))(p) = (\mathrm{Den}(o,\mathfrak{F}_\Sigma(X)))(p)$. $(\mathrm{Den}(o,T))(\mathrm{Hom}(T,x_1,x_2)\#p) = (\mathrm{Den}(o,\mathfrak{F}_\Sigma(X)))(\mathrm{Hom}(T,x_1,x_2)\#p)$.

Now we state the propositions:

(105) Suppose T is structure-invariant. Let us consider an element ρ of T from σ. Then $(\mathrm{Hom}(T,x_1,x_2))(\sigma)(\rho) = (\mathrm{Hom}(\mathfrak{F}_\Sigma(X),x_1,x_2))(\sigma)(\rho)$. PROOF: Set $h = \mathrm{Hom}(T,x_1,x_2)$. Set $g = \mathrm{Hom}(\mathfrak{F}_\Sigma(X),x_1,x_2)$. Define $\mathcal{P}[$element of $T] \equiv h($the sort of $\$_1)(\$_1) = g($the sort of $\$_1)(\$_1)$. For every σ, x, and ρ such that $\rho = x$-term holds $\mathcal{P}[\rho]$. For every o, p, and ρ such that $\rho = o$-term p and for every element τ of T such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[\rho]$ by [10, (13)], (22), [36, (6)], [52, (29), (25)]. $\mathcal{P}[\rho]$ from *TermAlgebraInd*. $\square$

(106) If T is structure-invariant and $x_1 \neq x_2$ and ρ is x_2-omitting, then $(\mathrm{Hom}(T,x_1,x_2))(\rho)$ is x_1-omitting. PROOF: Set $h = \mathrm{Hom}(T,x_1,x_2)$. Define $\mathcal{P}[$element of $T] \equiv$ if $\$_1$ is x_2-omitting, then $h(\$_1)$ is x_1-omitting. For every σ, x, and ρ such that $\rho = x$-term holds $\mathcal{P}[\rho]$. For every o, p, and ρ such that $\rho = o$-term p and for every element τ of T such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[\rho]$ by (22), (34), [10, (13), (41)]. $\mathcal{P}[\rho]$ from *TermAlgebraInd*. $\square$

(107) Suppose Q is structure-invariant and v is y-omitting. Then (the canonical homomorphism of $Q)(v)$ is y-omitting. The theorem is a consequence of (104), (29), (101), (100), (98), and (106).

(108) Suppose Q is structure-invariant. Let us consider an element p of $\mathrm{Args}(o,Q)$. Suppose an element τ of Q. If $\tau \in \mathrm{rng}\, p$, then τ is y-omitting. Let us consider an element τ of Q. If $\tau = (\mathrm{Den}(o,Q))(p)$, then τ is y-omitting. The theorem is a consequence of (76), (34), and (107).

(109) If Q is structure-invariant and v is y-omitting, then $h_2(v)$ is y-omitting. PROOF: Define $\mathcal{P}[$element of $\mathfrak{F}_\Sigma(Y)] \equiv$ if $\$_1$ is y-omitting, then $h_2(\$_1)$ is y-omitting. For every σ and y, $\mathcal{P}[y$-term$]$. For every o and q such that for every v such that $v \in \mathrm{rng}\, q$ holds $\mathcal{P}[v]$ holds $\mathcal{P}[o$-term $q]$ by (34), [10, (13)], [36, (6)], [12, (2)]. $\mathcal{P}[v]$ from *TermInd*. $\square$

Let us consider a terminating invariant stable many sorted relation R indexed by $\mathfrak{F}_\Sigma(X)$ with NF-variables and unique normal form property. Now we state the propositions:

(110) (i) for every element τ of the algebra of normal forms of R, $(\mathrm{Hom}(\mathfrak{F}_\Sigma(X), x_1,x_2))($the sort of $\tau)(\tau) = (\mathrm{Hom}($the algebra of normal forms of $R,x_1,x_2))(\tau)$, and

(ii) $\mathrm{Hom}(\mathfrak{F}_\Sigma(X),x_1,x_2) \restriction \mathrm{NForms}(R) = \mathrm{Hom}($the algebra of normal forms of R, x_1, x_2).

PROOF: Set $F = \mathfrak{F}_\Sigma(X)$. Set $T =$ the algebra of normal forms of R. Set $H_3 = \mathrm{Hom}(F, x_1, x_2)$. Set $H_2 = \mathrm{Hom}(T, x_1, x_2)$. Define $\mathcal{P}[\text{element of } T] \equiv H_3(\text{the sort of } \$_1)(\$_1) = H_2(\$_1)$. For every sort symbol σ of Σ and for every element x of $X(\sigma)$ and for every element ρ of T such that $\rho = x$-term holds $\mathcal{P}[\rho]$. For every operation symbol o of Σ and for every element p of $\mathrm{Args}(o, \mathfrak{F}_\Sigma(X))$ and for every element ρ of T such that $\rho = o$-term p and for every element τ of T such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[\rho]$ by (22), (34), [10, (13)], [16, (54)]. $(\mathrm{Hom}(\mathfrak{F}_\Sigma(X), x_1, x_2) \restriction \mathrm{NForms}(R))(\sigma) =$ (Hom(the algebra of normal forms of R, x_1, x_2))(σ) by [27, (49)]. $\square$

(111) Suppose $i \in \mathrm{dom}\, p$ and $R(\mathrm{Arity}(o)_i)$ reduces τ_1 to τ_2. Then R(the result sort of o) reduces $(\mathrm{Den}(o, \mathfrak{F}_\Sigma(X)))(p +\cdot (i, \tau_1))$ to $(\mathrm{Den}(o, \mathfrak{F}_\Sigma(X)))(p +\cdot (i, \tau_2))$. PROOF: Consider ρ being a reduction sequence w.r.t. $R(\mathrm{Arity}(o)_i)$ such that $\rho(1) = \tau_1$ and $\rho(\mathrm{len}\, \rho) = \tau_2$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant \mathrm{len}\, \rho$, then R(the result sort of o) reduces $(\mathrm{Den}(o, \mathfrak{F}_\Sigma(X)))(p +\cdot (i, \tau_1))$ to $(\mathrm{Den}(o, \mathfrak{F}_\Sigma(X)))(p +\cdot (i, \rho(\$_1)))$. For every i such that $1 \leqslant i$ and $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [13, (13)], [52, (25)], [32, (87)], [12, (7), (2)]. For every i such that $i \geqslant 1$ holds $\mathcal{P}[i]$ from [13, Sch. 8]. $\square$

Now we state the propositions:

(112) Let us consider a terminating invariant stable many sorted relation R indexed by $\mathfrak{F}_\Sigma(X)$ with NF-variables and unique normal form property and τ. Then R(the sort of τ) reduces τ to (the canonical homomorphism of the algebra of normal forms of R)(τ). PROOF: Set $T =$ the algebra of normal forms of R. Set $H =$ the canonical homomorphism of T. Define $\mathcal{P}[\text{element of } \mathfrak{F}_\Sigma(X)] \equiv R(\text{the sort of } \$_1)$ reduces $\$_1$ to $H(\$_1)$. For every o and p such that for every τ such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[o\text{-term}\, p]$ by [10, (13)], (34), [16, (54)], [12, (2)]. $\mathcal{P}[\tau]$ from *TermInd*. $\square$

(113) Let us consider a terminating invariant stable many sorted relation R indexed by $\mathfrak{F}_\Sigma(X)$ with NF-variables and unique normal form property, o, and p. Then R(the result sort of o) reduces o-term p to (Den(o, the algebra of normal forms of R))((the canonical homomorphism of the algebra of normal forms of R)$\#p$). The theorem is a consequence of (34) and (112).

(114) Let us consider a terminating invariant stable many sorted relation R indexed by $\mathfrak{F}_\Sigma(X)$ with NF-variables and unique normal form property, o, p, and an element q of Args(o, the algebra of normal forms of R). Suppose $p = q$. Then R(the result sort of o) reduces o-term p to (Den(o, the algebra of normal forms of R))(q). The theorem is a consequence of (113).

Let us consider Σ and X. Let R be a terminating invariant stable many sorted relation indexed by $\mathfrak{F}_\Sigma(X)$ with NF-variables and unique normal form property. Observe that the algebra of normal forms of R is structure-invariant.

Let us note that there exists a free in itself including Σ-terms over X algebra over Σ with all variables and inheriting operations which is structure-invariant.

5. Context vs. Translations

Let us consider Σ, σ_1, and σ_2. We say that σ_2 is σ_1-reachable if and only if

(Def. 33) TranslRel(Σ) reduces σ_1 to σ_2.

One can verify that there exists a sort symbol of Σ which is σ_1-reachable.

From now on σ_2 denotes a σ_1-reachable sort symbol of Σ and g_1 denotes a translation in $\mathfrak{F}_\Sigma(Y)$ from σ_1 into σ_2.

Now we state the proposition:

(115) TranslRel(Σ) reduces σ to the sort of $\mathcal{C}'$. Proof: Define $\mathcal{P}$[element of $\mathfrak{F}_\Sigma(Z)] \equiv$ TranslRel(Σ) reduces σ to the sort of $\$_1$. $\mathcal{P}[\mathcal{C}']$ from *ContextInd*. $\square$

Let us consider Σ, X, σ, x, and $\mathcal{C}$. Observe that the sort of $\mathcal{C}$ is σ-reachable.

Let us consider σ_1, σ_2, and g. Let τ be an element of (the sorts of $\mathfrak{F}_\Sigma(X)$)(σ_1). One can check that the functor $g(\tau)$ yields an element of (the sorts of $\mathfrak{F}_\Sigma(X)$)(σ_2).

Let us consider σ, x, and $\mathcal{C}$. We say that $\mathcal{C}$ is basic if and only if

(Def. 34) There exists o and there exists p such that $\mathcal{C} = o$-term p and the x-context in $p = x$-term.

The functor transl $\mathcal{C}$ yielding a function from (the sorts of $\mathfrak{F}_\Sigma(X)$)(σ) into (the sorts of $\mathfrak{F}_\Sigma(X)$)(the sort of $\mathcal{C}$) is defined by

(Def. 35) If the sort of $\tau = \sigma$, then $it(\tau) = \mathcal{C}[\tau]$.

Now we state the propositions:

(116) If $\mathcal{C} = x$-term, then transl $\mathcal{C} = \mathrm{id}_{\alpha(\sigma)}$, where α is the sorts of $\mathfrak{F}_\Sigma(X)$. The theorem is a consequence of (84).

(117) Suppose $\mathcal{C}' = o$-term k and the z-context in $k = z$-term and $k1 = k +\cdot$ (the z-context position in k, l). Then $\mathcal{C}'[l] = o$-term $k1$. The theorem is a consequence of (74), (77), (84), and (87).

(118) If $\mathcal{C}'$ is basic, then transl $\mathcal{C}'$ is an elementary translation in $\mathfrak{F}_\Sigma(Z)$ from σ into the sort of $\mathcal{C}'$. The theorem is a consequence of (34), (74), (77), and (117).

(119) Let us consider a finite set V. Suppose

(i) $m \in \operatorname{dom} q$, and

(ii) $\mathrm{Arity}(o)_m = \sigma$.

Then there exists y and there exists $\mathcal{C}_1$ and there exists q_1 such that $y \notin V$ and $\mathcal{C}_1 = o$-term q_1 and $q_1 = q +\cdot (m, y$-term) and q_1 is y-context including once only and $m =$ the y-context position in q_1 and the y-context in $q_1 = y$-term. Proof: Set $y =$ the element of $Y(\sigma) \setminus (V \cup \pi_1(\mathrm{rng}(o\text{-term}\, q)))$.

Reconsider $q_1 = q +\cdot (m, y\text{-term})$ as an element of $\mathrm{Args}(o, \mathfrak{F}_\Sigma(Y))$. q_1 is y-context including once only by [25, (30), (31), (32)], [52, (25)]. □

(120) Let us consider sort symbols σ_1, σ_2 of Σ and a finite set V. Suppose

(i) $m \in \mathrm{dom}\, q$, and

(ii) $\sigma_1 = \mathrm{Arity}(o)_m$.

Then there exists an element y of $Y(\sigma_1)$ and there exists a context $\mathcal{C}$ of y and there exists q_1 such that $y \notin V$ and $q_1 = q +\cdot (m, y\text{-term})$ and q_1 is y-context including once only and the y-context in $q_1 = y$-term and $\mathcal{C} = o\text{-term}\, q_1$ and $m =$ the y-context position in q_1 and $\mathrm{transl}\, \mathcal{C} = o_m^{\mathfrak{F}_\Sigma(Y)}(q, -)$. The theorem is a consequence of (119) and (117).

Let us consider Σ, X, τ, and a. One can verify that $\mathrm{Coim}(\tau, a)$ is finite sequence-membered.

Now we state the propositions:

(121) Suppose X is nontrivial and the sort of $\tau = \sigma$. Then $\overline{\overline{\mathrm{Coim}(\tau, a)}} \subseteq \overline{\overline{\mathrm{Coim}(\mathcal{C}[\tau], a)}}$. Proof: Define $\mathcal{P}[\text{context of } x] \equiv$ for every $\mathcal{C}$ such that $\mathcal{C} = \$_1$ holds $\overline{\overline{\mathrm{Coim}(\tau, a)}} \subseteq \overline{\overline{\mathrm{Coim}(\mathcal{C}[\tau], a)}}$. $\mathcal{P}[x\text{-term}]$. For every o and p such that p is x-context including once only holds if $\mathcal{P}[\text{the } x\text{-context in } p]$, then for every context $\mathcal{C}$ of x such that $\mathcal{C} = o\text{-term}\, p$ holds $\mathcal{P}[\mathcal{C}]$ by (77), [36, (6)], [13, (10)], [52, (25)]. $\mathcal{P}[\mathcal{C}]$ from *ContextInd*. □

(122) If p is x-context including once only and $i \in \mathrm{dom}\, p$, then p_i is not x-omitting iff p_i is x-context.

Let us assume that X is nontrivial and the sort of $\mathcal{C} = \sigma_1$. Now we state the propositions:

(123) Let us consider an element x_1 of $X(\sigma_1)$, a context $\mathcal{C}_1$ of x_1, and a context $\mathcal{C}_2$ of x. Suppose $\mathcal{C}_2 = \mathcal{C}_1[\mathcal{C}]$. If the sort of $\tau = \sigma$, then $\mathcal{C}_2[\tau] = \mathcal{C}_1[\mathcal{C}[\tau]]$. Proof: Define $\mathcal{P}[\text{context of } x_1] \equiv$ for every context $\mathcal{C}_1$ of x_1 for every context $\mathcal{C}_2$ of x such that $\mathcal{C}_1 = \$_1$ and $\mathcal{C}_2 = \mathcal{C}_1[\mathcal{C}]$ holds $\mathcal{C}_2[\tau] = \mathcal{C}_1[\mathcal{C}[\tau]]$. $\mathcal{P}[x_1\text{-term}]$. For every o and for every element w of $\mathrm{Args}(o, \mathfrak{F}_\Sigma(X))$ such that w is x_1-context including once only holds if $\mathcal{P}[\text{the } x_1\text{-context in } w]$, then for every context $\mathcal{C}$ of x_1 such that $\mathcal{C} = o\text{-term}\, w$ holds $\mathcal{P}[\mathcal{C}]$ by (77), [36, (6)], [12, (2), (7)]. $\mathcal{P}[\mathcal{C}_1]$ from *ContextInd*. □

(124) Let us consider an element x_1 of $X(\sigma_1)$, a context $\mathcal{C}_1$ of x_1, and a context $\mathcal{C}_2$ of x. Suppose $\mathcal{C}_2 = \mathcal{C}_1[\mathcal{C}]$. Then $\mathrm{transl}\, \mathcal{C}_2 = \mathrm{transl}\, \mathcal{C}_1 \cdot \mathrm{transl}\, \mathcal{C}$. Proof: Reconsider $f = \mathrm{transl}\, \mathcal{C}$ as a function from (the sorts of $\mathfrak{F}_\Sigma(X))(\sigma)$ into (the sorts of $\mathfrak{F}_\Sigma(X))(\sigma_1)$. $\mathrm{transl}\, \mathcal{C}_2 = \mathrm{transl}\, \mathcal{C}_1 \cdot f$ by [28, (15)], (123). □

Now we state the proposition:

(125) There exists y_{11} and there exists $\mathcal{C}_{12}$ such that the sort of $\mathcal{C}_{12} = \sigma_2$ and $g_1 = \mathrm{transl}\, \mathcal{C}_{12}$. Proof: Define $\mathcal{P}[\text{function}, \text{sort symbol of } \Sigma, \text{sort symbol of } \Sigma] \equiv$ for every finite set V, there exists an element x of $Y(\$_2)$ and

there exists a context $\mathcal{C}$ of x such that $x \notin V$ and the sort of $\mathcal{C} = \$_3$ and $\$_1 = \operatorname{transl} \mathcal{C}$. For every σ, $\mathcal{P}[\mathrm{id}_{\alpha(\sigma)}, \sigma, \sigma]$, where α is the sorts of $\mathfrak{F}_\Sigma(Y)$. For every sort symbols σ_1, σ_2, σ_3 of Σ such that TranslRel(Σ) reduces σ_1 to σ_2 for every translation τ in $\mathfrak{F}_\Sigma(Y)$ from σ_1 into σ_2 such that $\mathcal{P}[\tau, \sigma_1, \sigma_2]$ for every function f such that f is an elementary translation in $\mathfrak{F}_\Sigma(Y)$ from σ_2 into σ_3 holds $\mathcal{P}[f \cdot \tau, \sigma_1, \sigma_3]$ by [12, (2)], (120), (73), (69). For every sort symbols σ_1, σ_2 of Σ such that TranslRel(Σ) reduces σ_1 to σ_2 for every translation τ in $\mathfrak{F}_\Sigma(Y)$ from σ_1 into σ_2, $\mathcal{P}[\tau, \sigma_1, \sigma_2]$ from [12, Sch. 1]. $\square$

The scheme *LambdaTerm* deals with a non empty non void many sorted signature Σ and a non-empty many sorted set $\mathcal{X}$ indexed by the carrier of Σ and including Σ-terms over $\mathcal{X}$ algebras T_1, T_2 over Σ with all variables and inheriting operations and a unary functor $\mathcal{F}$ yielding an element of T_2 and states that

(Sch. 5) There exists a many sorted function f from T_1 into T_2 such that for every element τ of T_1, $f(\tau) = \mathcal{F}(\tau)$

provided

- for every element τ of T_1, the sort of τ = the sort of $\mathcal{F}(\tau)$.

Now we state the propositions:

(126) There exists an endomorphism g of T such that

(i) (the canonical homomorphism of T) $\circ\, h =$ $g \circ$ (the canonical homomorphism of T), and

(ii) for every element τ of T, $g(\tau) =$ (the canonical homomorphism of T)($h({}^{@}\tau)$).

The theorem is a consequence of (29).

(127) (The canonical homomorphism of T)($h(\tau)$) = (the canonical homomorphism of T)($h({}^{@}$((the canonical homomorphism of T)(τ)))). The theorem is a consequence of (126) and (29).

6. Context vs. Endomorphism

Let us consider Σ. Let $\mathcal{B}$ be a non empty finite sequence of elements of the carrier of Σ and i be an element of $\operatorname{dom} \mathcal{B}$. Note that the functor $\mathcal{B}(i)$ yields a sort symbol of Σ. Let us consider X. Let $\mathcal{B}$ be a finite sequence of elements of the carrier of Σ and V be a finite sequence of elements of $\bigcup X$. We say that V is $\mathcal{B}$-sorting if and only if

(Def. 36) (i) $\operatorname{dom} V = \operatorname{dom} \mathcal{B}$, and

(ii) for every i such that $i \in \operatorname{dom} \mathcal{B}$ holds $V(i) \in X(\mathcal{B}(i))$.

Let us observe that there exists a finite sequence of elements of $\bigcup X$ which is $\mathcal{B}$-sorting.

Let $\mathcal{B}$ be a non empty finite sequence of elements of the carrier of Σ. One can check that every finite sequence of elements of $\bigcup X$ which is $\mathcal{B}$-sorting is also non empty.

Let V be a $\mathcal{B}$-sorting finite sequence of elements of $\bigcup X$ and i be an element of $\operatorname{dom}\mathcal{B}$. Note that the functor $V(i)$ yields an element of $X(\mathcal{B}(i))$. Let $\mathcal{B}$ be a finite sequence of elements of the carrier of Σ and D be a finite sequence of elements of $\mathfrak{F}_\Sigma(X)$. We say that D is $\mathcal{B}$-sorting if and only if

(Def. 37) (i) $\operatorname{dom} D = \operatorname{dom}\mathcal{B}$, and

(ii) for every i such that $i \in \operatorname{dom}\mathcal{B}$ holds $D(i) \in$ (the sorts of $\mathfrak{F}_\Sigma(X))(\mathcal{B}(i))$.

Note that there exists a finite sequence of elements of $\mathfrak{F}_\Sigma(X)$ which is $\mathcal{B}$-sorting.

Let $\mathcal{B}$ be a non empty finite sequence of elements of the carrier of Σ. One can verify that every finite sequence of elements of $\mathfrak{F}_\Sigma(X)$ which is $\mathcal{B}$-sorting is also non empty.

Let D be a $\mathcal{B}$-sorting finite sequence of elements of $\mathfrak{F}_\Sigma(X)$ and i be an element of $\operatorname{dom}\mathcal{B}$. Let us note that the functor $D(i)$ yields an element of (the sorts of $\mathfrak{F}_\Sigma(X))(\mathcal{B}(i))$. Let V be a $\mathcal{B}$-sorting finite sequence of elements of $\bigcup X$ and F be a finite sequence of elements of $\mathfrak{F}_\Sigma(X)$. We say that F is V-context sequence if and only if

(Def. 38) (i) $\operatorname{dom} F = \operatorname{dom}\mathcal{B}$, and

(ii) for every element i of $\operatorname{dom}\mathcal{B}$, $F(i)$ is a context of $V(i)$.

Let us observe that every finite sequence of elements of $\mathfrak{F}_\Sigma(X)$ which is V-context sequence is also non empty.

The scheme *FinSeqLambda* deals with a non empty finite sequence $\mathcal{B}$ and a unary functor $\mathcal{F}$ yielding an object and states that

(Sch. 6) There exists a non empty finite sequence p such that $\operatorname{dom} p = \operatorname{dom}\mathcal{B}$ and for every element i of $\operatorname{dom}\mathcal{B}$, $p(i) = \mathcal{F}(i)$.

The scheme *FinSeqRecLambda* deals with a non empty finite sequence $\mathcal{B}$ and an object $\mathfrak{A}$ and a binary functor $\mathcal{F}$ yielding a set and states that

(Sch. 7) There exists a non empty finite sequence p such that $\operatorname{dom} p = \operatorname{dom}\mathcal{B}$ and $p(1) = \mathfrak{A}$ and for every elements i, j of $\operatorname{dom}\mathcal{B}$ such that $j = i + 1$ holds $p(j) = \mathcal{F}(i, p(i))$.

The scheme *FinSeqRec2Lambda* deals with a non empty finite sequence $\mathcal{B}$ and a decorated tree $\mathfrak{A}$ and a binary functor $\mathcal{F}$ yielding a decorated tree and states that

(Sch. 8) There exists a non empty decorated tree yielding finite sequence p such that $\operatorname{dom} p = \operatorname{dom}\mathcal{B}$ and $p(1) = \mathfrak{A}$ and for every elements i, j of $\operatorname{dom}\mathcal{B}$

such that $j = i + 1$ for every decorated tree d such that $d = p(i)$ holds $p(j) = \mathcal{F}(i, d)$.

Let us consider Σ and X. Let $\mathcal{B}$ be a non empty finite sequence of elements of the carrier of Σ and V be a $\mathcal{B}$-sorting finite sequence of elements of $\bigcup X$. One can check that there exists a finite sequence of elements of $\mathfrak{F}_\Sigma(X)$ which is V-context sequence.

Let F be a V-context sequence finite sequence of elements of $\mathfrak{F}_\Sigma(X)$ and i be an element of dom $\mathcal{B}$. One can verify that the functor $F(i)$ yields a context of $V(i)$. Let V_1, V_2 be $\mathcal{B}$-sorting finite sequences of elements of $\bigcup X$. We say that V_2 is V_1-omitting if and only if

(Def. 39) rng V_1 misses rng V_2.

Let D be a $\mathcal{B}$-sorting finite sequence of elements of $\mathfrak{F}_\Sigma(X)$ and F be a V_2-context sequence finite sequence of elements of $\mathfrak{F}_\Sigma(X)$. We say that F is (V_1, V_2, D)-consequent context sequence if and only if

(Def. 40) Let us consider elements i, j of dom $\mathcal{B}$. If $i+1 = j$, then $F(j)[V_1(j)\text{-term}] = F(i)[D(i)]$.

Let V be a $\mathcal{B}$-sorting finite sequence of elements of $\bigcup X$. We say that V is D-omitting if and only if

(Def. 41) If $\tau \in \operatorname{rng} D$, then vf τ misses rng V.

Now we state the proposition:

(128) Let us consider a non empty finite sequence $\mathcal{B}$ of elements of the carrier of Σa $\mathcal{B}$-sorting finite sequence D of elements of $\mathfrak{F}_\Sigma(X)$a $\mathcal{B}$-sorting finite sequence V of elements of $\bigcup X$. Suppose V is D-omitting. Let us consider elements b_1, b_2 of dom $\mathcal{B}$. Then $D(b_1)$ is $(V(b_2))$-omitting. The theorem is a consequence of (69).

Let us consider Σ and Y. Let $\mathcal{B}$ be a non empty finite sequence of elements of the carrier of Σ, V be a $\mathcal{B}$-sorting finite sequence of elements of $\bigcup Y$, and D be a $\mathcal{B}$-sorting finite sequence of elements of $\mathfrak{F}_\Sigma(Y)$. Let us observe that there exists a $\mathcal{B}$-sorting finite sequence of elements of $\bigcup Y$ which is one-to-one, V-omitting, and D-omitting.

Let us consider X and τ.

A vf-sequence of τ is a finite sequence and is defined by

(Def. 42) There exists a one-to-one finite sequence f such that

(i) rng f = $\{\xi$, where ξ is an element of dom τ : there exists σ and there exists x such that $\tau(\xi) = \langle x, \sigma\rangle\}$, and

(ii) dom it = dom f, and

(iii) for every i such that $i \in \operatorname{dom} it$ holds $it(i) = \tau(f(i))$.

Let f be a finite sequence. Let us observe that pr1(f) is finite sequence-like and pr2(f) is finite sequence-like.

Now we state the propositions:

(129) Let us consider a vf-sequence f of τ. Then $\mathrm{pr2}(f)$ is a finite sequence of elements of the carrier of Σ.

(130) Let us consider a vf-sequence f of τ and a finite sequence $\mathcal{B}$ of elements of the carrier of Σ. Suppose $\mathcal{B} = \mathrm{pr2}(f)$. Then $\mathrm{pr1}(f)$ is a $\mathcal{B}$-sorting finite sequence of elements of $\bigcup X$.

Let f be a non empty finite sequence. One can verify that $1(\in \mathrm{dom}\, f)$ reduces to 1 and $(\mathrm{len}\, f)(\in \mathrm{dom}\, f)$ reduces to $\mathrm{len}\, f$.

Now we state the propositions:

(131) Let us consider an element ξ of $\mathrm{dom}\,\tau$. Suppose $\tau(\xi) = \langle x, \sigma\rangle$. Suppose the sort of $\tau_1 = \sigma$. Then τ with-replacement(ξ, τ_1) is an element of $\mathfrak{F}_\Sigma(X)$ from the sort of τ. Proof: Define $\mathcal{P}$[element of $\mathfrak{F}_\Sigma(X)$] $\equiv$ for every element ξ of $\mathrm{dom}\,\$_1$ for every x_1 and τ such that $\$_1(\xi) = \langle x_1, \sigma\rangle$ and $\tau = \$_1$ holds $\$_1$ with-replacement(ξ, τ_1) is an element of $\mathfrak{F}_\Sigma(X)$ from the sort of τ. $\mathcal{P}[x_{11}\text{-term}]$ by [20, (3)], [17, (29)]. For every o and p such that for every τ such that $\tau \in \mathrm{rng}\, p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[o\text{-term}\, p]$ by [20, (10)], [13, (12), (13)], [52, (25)]. $\mathcal{P}[\tau]$ from *TermInd*. $\square$

(132) Suppose X is nontrivial. Let us consider an element ξ of $\mathrm{dom}\,\mathcal{C}$. Suppose $\mathcal{C}(\xi) = \langle x, \sigma\rangle$. If the sort of $\tau = \sigma$, then $\mathcal{C}[\tau] = \mathcal{C}$ with-replacement(ξ, τ). Proof: Define $\mathcal{P}$[element of $\mathfrak{F}_\Sigma(X)$] $\equiv$ for every context $\mathcal{C}$ of x such that $\mathcal{C} = \$_1$ for every element ξ of $\mathrm{dom}\,\mathcal{C}$ such that $\mathcal{C}(\xi) = \langle x, \sigma\rangle$ holds $\mathcal{C}[\tau] = \mathcal{C}$ with-replacement(ξ, τ). $\mathcal{P}[x\text{-term}]$ by [17, (29)], [20, (3)], (84). For every operation symbol o of Σ and for every element w of $\mathrm{Args}(o, \mathfrak{F}_\Sigma(X))$ such that w is x-context including once only holds if $\mathcal{P}$[the x-context in w], then for every context $\mathcal{C}$ of x such that $\mathcal{C} = o\text{-term}\, w$ holds $\mathcal{P}[\mathcal{C}]$ by [20, (10)], [19, (38)], [13, (12), (13)]. $\mathcal{P}[\mathcal{C}]$ from *ContextInd*. $\square$

(133) Let us consider finite sequences ξ_1, ξ_2. Suppose

(i) $\xi_1 \neq \xi_2$, and

(ii) $\xi_1, \xi_2 \in \mathrm{dom}\,\tau$.

Let us consider sort symbols σ_1, σ_2 of Σ, an element x_1 of $X(\sigma_1)$, and an element x_2 of $X(\sigma_2)$. Suppose $\tau(\xi_1) = \langle x_1, \sigma_1\rangle$. Then $\xi_1 \not\preceq \xi_2$. The theorem is a consequence of (36).

Let us consider τ, τ_1, and an element ξ of $\mathrm{dom}\,\tau$. Now we state the propositions:

(134) If $\tau_1 = \tau$ with-replacement$(\xi, x\text{-term})$ and τ is x-omitting, then τ_1 is a context of x. Proof: $\mathrm{Coim}(\tau_1, \langle x, \sigma\rangle) = \{\xi\}$ by [17, (1), (29)], [20, (3)], [22, (87)]. $\square$

(135) If $\tau(\xi) = \langle x, \sigma\rangle$, then $\mathrm{dom}\,\tau \subseteq \mathrm{dom}(\tau$ with-replacement$(\xi, \tau_1))$. The theorem is a consequence of (89).

Now we state the propositions:

(136) Let us consider an element ξ of $\operatorname{dom}\tau$. Suppose $\tau(\xi) = \langle x, \sigma \rangle$. Then $\operatorname{dom}\tau = \operatorname{dom}(\tau \text{ with-replacement}(\xi, x_1\text{-term}))$. Proof: $\operatorname{dom}\tau \subseteq \operatorname{dom}$ $(\tau \text{ with-replacement}(\xi, x_1\text{-term}))$. $\operatorname{dom}(\tau \text{ with-replacement}(\xi, x_1\text{-term})) \subseteq$ $\operatorname{dom}\tau$ by [17, (29)], [20, (3)]. □

(137) Let us consider trees τ, τ_1 and an element ξ of τ. Then $(\tau \text{ with-replacement}(\xi, \tau_1)) \restriction \xi = \tau_1$. The theorem is a consequence of (1).

(138) Let us consider decorated trees τ, τ_1 and a node ξ of τ. Then $(\tau \text{ with-replacement}(\xi, \tau_1)) \restriction \xi = \tau_1$. The theorem is a consequence of (137).

Let us consider a node ξ of τ. Now we state the propositions:

(139) If $\tau_1 = \tau \restriction \xi$, then $h(\tau) \restriction \xi = h(\tau_1)$. Proof: Define $\mathcal{P}[\text{element of } \mathfrak{F}_\Sigma(X)] \equiv$ for every node ξ of $\$_1$ for every τ_1 such that $\tau_1 = \$_1 \restriction \xi$ holds $h(\$_1) \restriction \xi = h(\tau_1)$ and $\xi \in \operatorname{dom}(h(\$_1))$. $\mathcal{P}[x\text{-term}]$ by [17, (29)], [20, (3)], [21, (1)], [17, (22)]. For every o and p such that for every τ such that $\tau \in \operatorname{rng} p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[o\text{-term}\, p]$ by [20, (11)], [21, (1)], [17, (22)], [21, (3)]. $\mathcal{P}[\tau]$ from *TermInd*. □

(140) If $\tau(\xi) = \langle x, \sigma \rangle$, then $\tau \restriction \xi = x\text{-term}$. The theorem is a consequence of (36).

Now we state the propositions:

(141) Let us consider trees τ, τ_1 and elements ξ, ν of τ. Suppose

(i) $\xi \not\subseteq \nu$, and

(ii) $\nu \not\subseteq \xi$.

Then $(\tau \text{ with-replacement}(\xi, \tau_1)) \restriction \nu = \tau \restriction \nu$. The theorem is a consequence of (2) and (5).

(142) Let us consider decorated trees τ, τ_1 and nodes ξ, ν of τ. Suppose

(i) $\xi \not\subseteq \nu$, and

(ii) $\nu \not\subseteq \xi$.

Then $(\tau \text{ with-replacement}(\xi, \tau_1)) \restriction \nu = \tau \restriction \nu$. The theorem is a consequence of (141) and (5).

(143) If $\tau \subseteq \tau_1$, then $\tau = \tau_1$. Proof: Define $\mathcal{P}[\text{element of } \mathfrak{F}_\Sigma(X)] \equiv$ for every τ_1 such that $\$_1 \subseteq \tau_1$ holds $\$_1 = \tau_1$. $\mathcal{P}[x\text{-term}]$ by [17, (22)], [30, (2)], [20, (3)], (36). For every o and p such that for every τ such that $\tau \in \operatorname{rng} p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[o\text{-term}\, p]$ by [17, (22)], [30, (2)], (36), [20, (3)]. $\mathcal{P}[\tau]$ from *TermInd*. □

(144) Let us consider an endomorphism h of $\mathfrak{F}_\Sigma(X)$. Then

(i) $\operatorname{dom}\tau \subseteq \operatorname{dom}(h(\tau))$, and

(ii) for every I such that $I = \{\xi$, where ξ is an element of $\operatorname{dom}\tau$: there exists σ and there exists x such that $\tau(\xi) = \langle x, \sigma\rangle\}$ holds $\tau\restriction(\operatorname{dom}\tau\setminus I) = h(\tau)\restriction(\operatorname{dom}\tau\setminus I)$.

PROOF: Define $\mathcal{P}$[element of $\mathfrak{F}_\Sigma(X)$] $\equiv$ $\operatorname{dom}\$_1 \subseteq \operatorname{dom}(h(\$_1))$ and for every I such that $I = \{\xi$, where ξ is an element of $\operatorname{dom}\$_1$: there exists σ and there exists x such that $\$_1(\xi) = \langle x, \sigma\rangle\}$ holds $\$_1\restriction(\operatorname{dom}\$_1\setminus I) = h(\$_1)\restriction(\operatorname{dom}\$_1\setminus I)$. $\mathcal{P}[x\text{-term}]$ by [17, (22)], [20, (3)], [17, (29)]. For every o and p such that for every τ such that $\tau \in \operatorname{rng} p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[o\text{-term}\, p]$ by (34), [10, (13)], [20, (11)], [17, (22)]. $\mathcal{P}[\tau]$ from *TermInd*. □

(145) Suppose $I = \{\xi$, where ξ is an element of $\operatorname{dom}\tau$: there exists σ and there exists x such that $\tau(\xi) = \langle x, \sigma\rangle\}$. Let us consider a node ξ of $h(\tau)$. Then

(i) $\xi \in \operatorname{dom}\tau\setminus I$, or

(ii) there exists an element ν of $\operatorname{dom}\tau$ such that $\nu \in I$ and there exists a node μ of $h(\tau)\restriction\nu$ such that $\xi = \nu ^\frown \mu$.

PROOF: Define $\mathcal{P}$[element of $\mathfrak{F}_\Sigma(X)$] $\equiv$ for every I such that $I = \{\xi$, where ξ is an element of $\operatorname{dom}\$_1$: there exists σ and there exists x such that $\$_1(\xi) = \langle x, \sigma\rangle\}$ for every node ξ of $h(\$_1)$, $\xi \in \operatorname{dom}\$_1\setminus I$ or there exists an element ν of $\operatorname{dom}\$_1$ such that $\nu \in I$ and there exists a node μ of $h(\$_1)\restriction\nu$ such that $\xi = \nu^\frown\mu$. $\mathcal{P}[x\text{-term}]$ by [17, (22)], [20, (3)], [21, (1)]. For every o and p such that for every τ such that $\tau \in \operatorname{rng} p$ holds $\mathcal{P}[\tau]$ holds $\mathcal{P}[o\text{-term}\, p]$ by (34), [10, (13)], [20, (11)], [17, (22)]. $\mathcal{P}[\tau]$ from *TermInd*. □

(146) Let us consider an endomorphism h of $\mathfrak{F}_\Sigma(Y)$a one-to-one finite sequence g of elements of $\operatorname{dom} v$. Suppose

(i) $\operatorname{rng} g = \{\xi$, where ξ is an element of $\operatorname{dom} v$: there exists σ and there exists y such that $v(\xi) = \langle y, \sigma\rangle\}$, and

(ii) $\operatorname{dom} v \subseteq \operatorname{dom} v_1$, and

(iii) $v\restriction(\operatorname{dom} v\setminus\operatorname{rng} g) = v_1\restriction(\operatorname{dom} v\setminus\operatorname{rng} g)$, and

(iv) for every i such that $i \in \operatorname{dom} g$ holds $h(v)\restriction(g_i$ **qua** node of $v) = v_1\restriction(g_i$ **qua** node of $v)$.

Then $h(v) = v_1$. PROOF: $h(v)\restriction(\operatorname{dom} v\setminus\operatorname{rng} g) = v_1\restriction(\operatorname{dom} v\setminus\operatorname{rng} g)$. $h(v) \subseteq v_1$ by [27, (1)], (145), [27, (49)], (144). □

(147) Let us consider an endomorphism h of $\mathfrak{F}_\Sigma(Y)$ and a vf-sequence f of v. Suppose $f \neq \emptyset$. Then there exists a non empty finite sequence $\mathcal{B}$ of elements of the carrier of Σ and there exists a $\mathcal{B}$-sorting finite sequence V_1 of elements of $\bigcup Y$ such that $\operatorname{dom}\mathcal{B} = \operatorname{dom} f$ and $\mathcal{B} = \operatorname{pr2}(f)$ and $V_1 = \operatorname{pr1}(f)$ and there exists a $\mathcal{B}$-sorting finite sequence D of elements

of $\mathfrak{F}_\Sigma(Y)$ and there exists a V_1-omitting D-omitting $\mathcal{B}$-sorting finite sequence V_2 of elements of $\bigcup Y$ such that for every element i of $\operatorname{dom}\mathcal{B}$, $D(i) = h(V_1(i)\text{-term})$ and there exists a V_2-context sequence finite sequence F of elements of $\mathfrak{F}_\Sigma(Y)$ such that F is (V_1, V_2, D)-consequent context sequence and $F(1(\in \operatorname{dom}\mathcal{B}))[V_1(1(\in \operatorname{dom}\mathcal{B}))\text{-term}] = v$ and $h(v) = F((\operatorname{len}\mathcal{B})(\in \operatorname{dom}\mathcal{B}))[D((\operatorname{len}\mathcal{B})(\in \operatorname{dom}\mathcal{B}))]$. PROOF: Reconsider $\mathcal{B} = \operatorname{pr2}(f)$ as a non empty finite sequence of elements of the carrier of Σ. Consider g being a one-to-one finite sequence such that $\operatorname{rng} g = \{\xi$, where ξ is an element of $\operatorname{dom} v$: there exists σ and there exists y such that $v(\xi) = \langle y, \sigma\rangle\}$ and $\operatorname{dom} f = \operatorname{dom} g$ and for every i such that $i \in \operatorname{dom} f$ holds $f(i) = v(g(i))$. $\operatorname{rng} g \subseteq \operatorname{dom} v$. Reconsider $V_1 = \operatorname{pr1}(f)$ as a $\mathcal{B}$-sorting finite sequence of elements of $\bigcup Y$. Define $\mathcal{F}(\text{element of } \operatorname{dom}\mathcal{B}) = h(V_1(\$_1)\text{-term})$. Consider D being a non empty finite sequence such that $\operatorname{dom} D = \operatorname{dom}\mathcal{B}$ and for every element i of $\operatorname{dom}\mathcal{B}$, $D(i) = \mathcal{F}(i)$ from *FinSeqLambda*. D is a finite sequence of elements of $\mathfrak{F}_\Sigma(Y)$. D is $\mathcal{B}$-sorting. Set $V_2 =$ the one-to-one V_1-omitting D-omitting $\mathcal{B}$-sorting finite sequence of elements of $\bigcup Y$. Define $\mathcal{H}(\text{element of } \operatorname{dom}\mathcal{B}, \text{decorated tree}) = (\$_2 \text{ with-replacement}(((g_{\$_1} \textbf{ qua } \text{element of } \operatorname{dom} v) \textbf{ qua } \text{finite sequence of elements of } \mathbb{N}), D(\$_1))) \text{ with-replacement}(((g_{\$_1+1} \textbf{ qua } \text{element of } \operatorname{dom} v) \textbf{ qua } \text{finite sequence of elements of } \mathbb{N}), \text{the root tree of } \langle V_2(\$_1+1), \mathcal{B}(\$_1+1)\rangle)$. Consider F being a non empty decorated tree yielding finite sequence such that $\operatorname{dom} F = \operatorname{dom}\mathcal{B}$ and $F(1) = v \text{ with-replacement}(((g_1 \textbf{ qua } \text{element of } \operatorname{dom} v) \textbf{ qua } \text{finite sequence of elements of } \mathbb{N}), \text{the root tree of } \langle V_2(1), \mathcal{B}(1)\rangle)$ and for every elements i, j of $\operatorname{dom}\mathcal{B}$ such that $j = i+1$ for every decorated tree d such that $d = F(i)$ holds $F(j) = \mathcal{H}(i, d)$ from *FinSeqRec2Lambda*. $\operatorname{rng} F \subseteq \bigcup(\text{the sorts of } \mathfrak{F}_\Sigma(Y))$ by (131), [22, (87)], [20, (3)], (133). Define $\mathcal{Q}[\text{natural number}] \equiv$ for every element b of $\operatorname{dom}\mathcal{B}$ such that $\$_1 = b$ holds $F(b)$ is a context of $V_2(b)$ and $\operatorname{dom} v \subseteq \operatorname{dom}(F(b))$ and $F(b)(g_b) = \langle V_2(b), \mathcal{B}(b)\rangle$ and for every element b_1 of $\operatorname{dom}\mathcal{B}$ such that $b_1 > b$ holds F_b is $(V_2(b_1))$-omitting and $F(b)(g_{b_1}) = \langle V_1(b_1), \mathcal{B}(b_1)\rangle$. $\mathcal{Q}[1]$ by [27, (102)], (134), (135), [22, (87)]. For every i such that $1 \leqslant i$ and $\mathcal{Q}[i]$ holds $\mathcal{Q}[i+1]$ by [52, (25)], [13, (13)], [27, (102)], (132). For every i such that $i \geqslant 1$ holds $\mathcal{Q}[i]$ from [13, Sch. 8]. F is V_2-context sequence by [52, (25)]. F is (V_1, V_2, D)-consequent context sequence by [52, (25)], [13, (12), (13)], (132). Set $b = 1(\in \operatorname{dom}\mathcal{B})$. Reconsider $\nu = g_b$, $\xi = g_{\operatorname{len}\mathcal{B}}$ as a node of v. Consider μ being a node of v such that $\nu = \mu$ and there exists σ and there exists y such that $v(\mu) = \langle y, \sigma\rangle$. $\operatorname{dom}(F(b)) = \operatorname{dom} v$. Reconsider $\tau = V_1(b)\text{-term}$ as an element of $\mathfrak{F}_\Sigma(Y)$. Consider μ being a finite sequence of elements of $\mathbb{N}$ such that $\mu \in \operatorname{dom}(V_2(b)\text{-term})$ and $\nu = \nu \frown \mu$ and $F(b)(\nu) = V_2(b)\text{-term}(\mu)$. $F(b)[\tau] = F(b) \text{ with-replacement}(\nu, \tau)$. Define $\Sigma[\text{natural number}] \equiv$ for every elements b, b_1 of $\operatorname{dom}\mathcal{B}$ such that $\$_1 = b$ and $b_1 \leqslant b$ holds $(F(b)[D(b)])\restriction(g_{b_1} \textbf{ qua } \text{node of } v) = h(v)\restriction(g_{b_1} \textbf{ qua } \text{node of}$

v) and $(F(b)[D(b)])\restriction(\operatorname{dom} v \setminus \operatorname{rng} g) = v\restriction(\operatorname{dom} v \setminus \operatorname{rng} g)$. $\Sigma[1]$ by [52, (25)], (132), (138), (140). For every i such that $i \geqslant 1$ and $\Sigma[i]$ holds $\Sigma[i+1]$ by [52, (25)], [13, (13)], (132), (135). Set $b = (\operatorname{len} \mathcal{B})(\in \operatorname{dom} \mathcal{B})$. Set $v_1 = F(b)[D(b)]$. For every i such that $i \geqslant 1$ holds $\Sigma[i]$ from [13, Sch. 8]. $v_1 = F(b)\,\text{with-replacement}((g_b\ \textbf{qua}\ \text{node of } v), D(b))$. $\operatorname{dom}(F(b)) \subseteq \operatorname{dom} v_1$. $\square$

References

[1] Grzegorz Bancerek. Towards the construction of a model of Mizar concepts. *Formalized Mathematics*, 16(**2**):207–230, 2008. doi:10.2478/v10037-008-0027-x.

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

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

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

[5] Grzegorz Bancerek. On powers of cardinals. *Formalized Mathematics*, 3(**1**):89–93, 1992.

[6] Grzegorz Bancerek. Algebra of morphisms. *Formalized Mathematics*, 6(**2**):303–310, 1997.

[7] Grzegorz Bancerek. Tarski's classes and ranks. *Formalized Mathematics*, 1(**3**):563–567, 1990.

[8] Grzegorz Bancerek. Cartesian product of functions. *Formalized Mathematics*, 2(**4**):547–552, 1991.

[9] Grzegorz Bancerek. Institution of many sorted algebras. Part I: Signature reduct of an algebra. *Formalized Mathematics*, 6(**2**):279–287, 1997.

[10] Grzegorz Bancerek. Free term algebras. *Formalized Mathematics*, 20(**3**):239–256, 2012. doi:10.2478/v10037-012-0029-6.

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

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

[15] Grzegorz Bancerek. Veblen hierarchy. *Formalized Mathematics*, 19(**2**):83–92, 2011. doi:10.2478/v10037-011-0014-5.

[16] Grzegorz Bancerek. Reduction relations. *Formalized Mathematics*, 5(**4**):469–478, 1996.

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

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

[19] Grzegorz Bancerek. Sets and functions of trees and joining operations of trees. *Formalized Mathematics*, 3(**2**):195–204, 1992.

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

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

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

[23] Grzegorz Bancerek and Artur Korniłowicz. Yet another construction of free algebra. *Formalized Mathematics*, 9(**4**):779–785, 2001.

[24] Grzegorz Bancerek and Piotr Rudnicki. On defining functions on trees. *Formalized Mathematics*, 4(**1**):91–101, 1993.

[25] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

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

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

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

[29] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.

[30] Czesław Byliński. Graphs of functions. *Formalized Mathematics*, 1(**1**):169–173, 1990.

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

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

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

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

[35] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**): 573–577, 1997.

[36] Małgorzata Korolkiewicz. Homomorphisms of many sorted algebras. *Formalized Mathematics*, 5(**1**):61–65, 1996.

[37] Małgorzata Korolkiewicz. Many sorted quotient algebra. *Formalized Mathematics*, 5(**1**): 79–84, 1996.

[38] Jarosław Kotowicz. Convergent real sequences. Upper and lower bound of sets of real numbers. *Formalized Mathematics*, 1(**3**):477–481, 1990.

[39] Yatsuka Nakamura. Determinant of some matrices of field elements. *Formalized Mathematics*, 14(**1**):1–5, 2006. doi:10.2478/v10037-006-0001-4.

[40] Hiroyuki Okazaki, Yuichi Futa, and Yasunari Shidama. Constructing binary Huffman tree. *Formalized Mathematics*, 21(**2**):133–143, 2013. doi:10.2478/forma-2013-0015.

[41] Beata Perkowska. Free many sorted universal algebra. *Formalized Mathematics*, 5(**1**): 67–74, 1996.

[42] Karol Pąk. Abstract simplicial complexes. *Formalized Mathematics*, 18(**1**):95–106, 2010. doi:10.2478/v10037-010-0013-y.

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

[44] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1 (**3**):495–500, 1990.

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

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

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

[48] Andrzej Trybulec. A scheme for extensions of homomorphisms of many sorted algebras. *Formalized Mathematics*, 5(**2**):205–209, 1996.

[49] Andrzej Trybulec. Many sorted algebras. *Formalized Mathematics*, 5(**1**):37–42, 1996.

[50] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.

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

[52] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

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

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

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

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

Received June 13, 2014

Special Issue: 25 years of the Mizar Mathematical Library

FORMALIZED MATHEMATICS
Vol. **22**, No. **2**, Pages 157–166, **2014**
DOI: 10.2478/forma-2014-0016

DE GRUYTER OPEN
degruyter.com/view/j/forma

Cauchy Mean Theorem

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

Summary. The purpose of this paper was to prove formally, using the Mizar language, Arithmetic Mean/Geometric Mean theorem known maybe better under the name of AM-GM inequality or Cauchy mean theorem. It states that the arithmetic mean of a list of a non-negative real numbers is greater than or equal to the geometric mean of the same list.

The formalization was tempting for at least two reasons: one of them, perhaps the strongest, was that the proof of this theorem seemed to be relatively easy to formalize (e.g. the weaker variant of this was proven in [13]). Also Jensen's inequality is already present in the Mizar Mathematical Library. We were impressed by the beauty and elegance of the simple proof by induction and so we decided to follow this specific way.

The proof follows similar lines as that written in Isabelle [18]; the comparison of both could be really interesting as it seems that in both systems the number of lines needed to prove this are really close.

This theorem is item `#38` from the "Formalizing 100 Theorems" list maintained by Freek Wiedijk at `http://www.cs.ru.nl/F.Wiedijk/100/` .

MSC: 26A06 26A12 03B35

Keywords: geometric mean; arithmetic mean; AM-GM inequality; Cauchy mean theorem

MML identifier: `RVSUM_3`, version: `8.1.03 5.23.1210`

The notation and terminology used in this paper have been introduced in the following articles: [1], [2], [7], [5], [12], [20], [9], [6], [23], [21], [3], [17], [4], [15], [19], [14], [26], [16], [10], [22], [25], and [11].

ISSN 1426–2630(Print), 1898-9934(Online)

1. Preliminaries

Let us consider real numbers x, y, z, w. Now we state the propositions:

(1) If $|x-y| < |z-w|$, then $(x-y)^{\mathbf{2}} < (z-w)^{\mathbf{2}}$.

(2) If $|x-y| < |z-w|$ and $x+y = z+w$, then $x \cdot y > z \cdot w$. The theorem is a consequence of (1).

Let f be a real-valued finite sequence. We introduce f is positive as a synonym of f is positive yielding.

Observe that f is positive if and only if the condition (Def. 1) is satisfied.

(Def. 1) Let us consider a natural number n. If $n \in \operatorname{dom} f$, then $f(n) > 0$.

Note that there exists a real-valued finite sequence which is non empty, constant, and positive and there exists a real-valued finite sequence which is non empty, non constant, and positive.

Let f be a non empty real-valued finite sequence and n be a natural number. One can verify that $f \restriction \operatorname{Seg} n$ is real-valued.

Let f be a positive non empty real-valued finite sequence. Let us note that $f \restriction \operatorname{Seg} n$ is positive.

Let f be a finite sequence. We introduce f is homogeneous as a synonym of f is constant.

Let f be a finite sequence. We introduce f is heterogeneous as an antonym of f is homogeneous.

Let us consider real-valued finite sequences R_1, R_2. Now we state the propositions:

(3) Suppose $\operatorname{len} R_1 = \operatorname{len} R_2$ and for every natural number j such that $j \in \operatorname{Seg} \operatorname{len} R_1$ holds $R_1(j) \leqslant R_2(j)$ and there exists a natural number j such that $j \in \operatorname{Seg} \operatorname{len} R_1$ and $R_1(j) < R_2(j)$. Then $\sum R_1 < \sum R_2$.

(4) If R_1 and R_2 are fiberwise equipotent, then $\prod R_1 = \prod R_2$. Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequences f, g of elements of $\mathbb{R}$ such that f and g are fiberwise equipotent and $\operatorname{len} f = \$_1$ holds $\prod f = \prod g$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [2, (75)], [3, (13)], [24, (25)], [8, (10), (4), (5)]. $\mathcal{P}[0]$ by [16, (3)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

2. Arithmetic Mean and Geometric Mean

Let f be a real-valued finite sequence. The functor $\operatorname{Mean} f$ yielding a real number is defined by the term

(Def. 2) $\frac{\sum f}{\operatorname{len} f}$.

Let f be a positive real-valued finite sequence. The functor $\operatorname{GMean} f$ yielding a real number is defined by the term

(Def. 3) $\sqrt[\operatorname{len} f]{\prod f}$.

Let us consider a real-valued finite sequence f. Now we state the propositions:

(5) $\sum f = \operatorname{len} f \cdot \operatorname{Mean} f$.

(6) $\operatorname{Mean}(f \frown \langle \operatorname{Mean} f \rangle) = \operatorname{Mean} f$. The theorem is a consequence of (5).

Let f be a non empty constant real-valued finite sequence. Observe that the value of f is real.

Let us consider a non empty constant real-valued finite sequence f. Now we state the propositions:

(7) $\sum f = (\text{the value of } f) \cdot \operatorname{len} f$.

(8) $\prod f = (\text{the value of } f)^{\operatorname{len} f}$.

(9) $\operatorname{Mean} f =$ the value of f. The theorem is a consequence of (7).

Let us consider a non empty constant positive real-valued finite sequence f. Now we state the propositions:

(10) The value of $f > 0$.

(11) $\operatorname{GMean} f =$ the value of f. The theorem is a consequence of (10) and (8).

Let f be a non empty positive real-valued finite sequence. Observe that $\operatorname{Mean} f$ is positive.

Let us note that $\prod f$ is positive.

Let f be a positive non empty real-valued finite sequence. Note that $\operatorname{GMean} f$ is positive.

3. Heterogeneity of a Finite Sequence

Let f be a real-valued finite sequence. The functor $\operatorname{HetSet} f$ yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 4) $\{n$, where n is a natural number : $n \in \operatorname{dom} f$ and $f(n) \neq \operatorname{Mean} f\}$.

One can verify that $\operatorname{HetSet} f$ is finite.

Let f be a positive non empty real-valued finite sequence. Let us observe that $\operatorname{HetSet} f$ is upper bounded lower bounded and real-membered.

Let f be a real-valued finite sequence. The functor $\operatorname{Het} f$ yielding a natural number is defined by the term

(Def. 5) $\overline{\overline{\operatorname{HetSet} f}}$.

Now we state the propositions:

(12) Let us consider a real-valued finite sequence f. If $\operatorname{Het} f = 0$, then f is homogeneous.

(13) Let us consider a non empty real-valued finite sequence f. If $\operatorname{Het} f \neq 0$, then f is heterogeneous. The theorem is a consequence of (9).

Let f be a heterogeneous positive non empty real-valued finite sequence. Note that HetSet f is non empty.

Now we state the proposition:

(14) Let us consider a non empty homogeneous positive real-valued finite sequence f. Then Mean f = GMean f. The theorem is a consequence of (9) and (11).

Let f_1, f_2 be real-valued finite sequences. We say that f_1 and f_2 are γ-equivalent if and only if

(Def. 6) (i) len f_1 = len f_2, and

(ii) Mean f_1 = Mean f_2.

One can check that the predicate is reflexive and symmetric.

Now we state the proposition:

(15) Let us consider real-valued finite sequences f_1, f_2. Suppose

(i) dom f_1 = dom f_2, and

(ii) $\sum f_1 = \sum f_2$.

Then f_1 and f_2 are γ-equivalent.

Let f be a real-valued finite sequence. The functors: MeanLess f and MeanMore f yielding subsets of $\mathbb{N}$ are defined by terms,

(Def. 7) $\{n$, where n is a natural number : $n \in \operatorname{dom} f$ and $f(n) < \operatorname{Mean} f\}$,

(Def. 8) $\{n$, where n is a natural number : $n \in \operatorname{dom} f$ and $f(n) > \operatorname{Mean} f\}$,

respectively.

Let us consider a real-valued finite sequence f. Now we state the propositions:

(16) HetSet $f \subseteq \operatorname{dom} f$.

(17) MeanLess $f \subseteq \operatorname{dom} f$.

(18) MeanMore $f \subseteq \operatorname{dom} f$.

(19) HetSet f = MeanLess $f \cup$ MeanMore f.

Let f be a heterogeneous real-valued finite sequence. One can verify that MeanLess f is non empty and MeanMore f is non empty.

Let f be a homogeneous real-valued finite sequence.

Let us note that MeanLess f is empty and MeanMore f is empty.

Let us consider a heterogeneous non empty real-valued finite sequence f. Now we state the propositions:

(20) MeanLess f misses MeanMore f.

(21) Het $f \geqslant 2$. The theorem is a consequence of (19) and (20).

4. Auxiliary Replacement Function

Let f be a function, i, j be natural numbers, and a, b be objects. The functor Replace(f, i, j, a, b) yielding a function is defined by the term

(Def. 9) $(f +\cdot (i, a)) +\cdot (j, b)$.

Now we state the proposition:

(22) Let us consider a finite sequence f, natural numbers i, j, and objects a, b. Then $\mathrm{dom}\,\mathrm{Replace}(f, i, j, a, b) = \mathrm{dom}\, f$.

Let f be a real-valued finite sequence, i, j be natural numbers, and a, b be real numbers. Let us observe that Replace(f, i, j, a, b) is real-valued and finite sequence-like.

Now we state the propositions:

(23) Let us consider a real-valued finite sequence w, a real number r, and a natural number i. Suppose $i \in \mathrm{dom}\, w$. Then $w +\cdot (i, r) = ((w{\restriction}(i -' 1)) \frown \langle r\rangle) \frown w_{\downharpoonright i}$.

(24) Let us consider a real-valued finite sequence f, a natural number i, and a real number a. If $i \in \mathrm{dom}\, f$, then $\sum(f +\cdot (i, a)) = \sum f - f(i) + a$. The theorem is a consequence of (23).

(25) Let us consider a positive real-valued finite sequence f, a natural number i, and a real number a. Suppose $i \in \mathrm{dom}\, f$. Then $\prod(f +\cdot (i, a)) = \frac{\prod f \cdot a}{f(i)}$. The theorem is a consequence of (23).

(26) Let us consider a real-valued finite sequence f, natural numbers i, j, and real numbers a, b. Suppose

 (i) i, $j \in \mathrm{dom}\, f$, and

 (ii) $i \neq j$.

Then $\sum \mathrm{Replace}(f, i, j, a, b) = \sum f - f(i) - f(j) + a + b$. The theorem is a consequence of (24).

(27) Let us consider a positive real-valued finite sequence f, natural numbers i, j, and positive real numbers a, b. Suppose

 (i) i, $j \in \mathrm{dom}\, f$, and

 (ii) $i \neq j$.

Then $\prod \mathrm{Replace}(f, i, j, a, b) = \frac{\prod f \cdot a \cdot b}{f(i) \cdot f(j)}$. Proof: For every natural number n such that $n \in \mathrm{dom}(f +\cdot (i, a))$ holds $(f +\cdot (i, a))(n) > 0$ by [6, (30), (31), (32)]. $\prod \mathrm{Replace}(f, i, j, a, b) = \frac{\prod (f +\cdot (i,a)) \cdot b}{(f +\cdot (i,a))(j)}$. $\square$

(28) Let us consider a real-valued finite sequence f and natural numbers i, j. Suppose

 (i) i, $j \in \mathrm{dom}\, f$, and

(ii) $i \neq j$.

Then f and $\mathrm{Replace}(f, i, j, \mathrm{Mean}\, f, (f(i)+f(j)-\mathrm{Mean}\, f))$ are γ-equivalent. The theorem is a consequence of (22) and (26).

(29) Let us consider a real-valued finite sequence f, natural numbers i, j, k, and real numbers a, b. Suppose

(i) i, j, $k \in \mathrm{dom}\, f$, and

(ii) $i \neq j$, and

(iii) $k \neq i$, and

(iv) $k \neq j$.

Then $(\mathrm{Replace}(f, i, j, a, b))(k) = f(k)$.

Let us consider a finite sequence f, natural numbers i, j, and objects a, b. Let us assume that i, $j \in \mathrm{dom}\, f$ and $i \neq j$. Now we state the propositions:

(30) $(\mathrm{Replace}(f, i, j, a, b))(j) = b$.

(31) $(\mathrm{Replace}(f, i, j, a, b))(i) = a$.

Now we state the propositions:

(32) Let us consider a real-valued finite sequence f and natural numbers i, j. Suppose

(i) i, $j \in \mathrm{dom}\, f$, and

(ii) $i \neq j$, and

(iii) $f(i) \neq \mathrm{Mean}\, f$, and

(iv) $f(j) \neq \mathrm{Mean}\, f$.

Then $\mathrm{Het}\, f > \mathrm{Het}\, \mathrm{Replace}(f, i, j, \mathrm{Mean}\, f, (f(i) + f(j) - \mathrm{Mean}\, f))$. The theorem is a consequence of (28), (31), (22), and (29).

(33) Let us consider positive non empty real-valued finite sequences f, g. Suppose

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

(ii) $\prod f < \prod g$.

Then $\mathrm{GMean}\, f < \mathrm{GMean}\, g$.

(34) Let us consider a positive heterogeneous non empty real-valued finite sequence f. Then there exist natural numbers i, j such that

(i) i, $j \in \mathrm{dom}\, f$, and

(ii) $i \neq j$, and

(iii) $f(i) < \mathrm{Mean}\, f < f(j)$.

Let us consider a positive heterogeneous non empty real-valued finite sequence f and natural numbers i, j. Now we state the propositions:

(35) If $i, j \in \mathrm{dom}\, f$ and $i \neq j$ and $f(i) > \mathrm{Mean}\, f$, then $\mathrm{Replace}(f, i, j, \mathrm{Mean}\, f, (f(i) + f(j) - \mathrm{Mean}\, f))$ is positive. The theorem is a consequence of (22), (31), (30), and (29).

(36) If $i, j \in \mathrm{dom}\, f$ and $i \neq j$ and $f(j) > \mathrm{Mean}\, f$, then $\mathrm{Replace}(f, i, j, \mathrm{Mean}\, f, (f(i) + f(j) - \mathrm{Mean}\, f))$ is positive. The theorem is a consequence of (22), (31), (30), and (29).

Now we state the propositions:

(37) Let us consider a positive heterogeneous non empty real-valued finite sequence f. Then there exist natural numbers i, j such that

- (i) i, $j \in \mathrm{dom}\, f$, and
- (ii) $i \neq j$, and
- (iii) there exists a positive non empty real-valued finite sequence g such that $g = \mathrm{Replace}(f, i, j, \mathrm{Mean}\, f, (f(i)+f(j)-\mathrm{Mean}\, f))$ and $\mathrm{GMean}\, f < \mathrm{GMean}\, g$.

The theorem is a consequence of (34), (22), (35), (27), and (33).

(38) Let us consider a heterogeneous non empty real-valued finite sequence f and natural numbers i, j. Suppose

- (i) $i =$ the element of $\mathrm{MeanLess}\, f$, and
- (ii) $j =$ the element of $\mathrm{MeanMore}\, f$.

Then

- (iii) i, $j \in \mathrm{dom}\, f$, and
- (iv) $i \neq j$, and
- (v) $f(i) < \mathrm{Mean}\, f$, and
- (vi) $f(j) > \mathrm{Mean}\, f$.

(39) Let us consider a heterogeneous positive non empty real-valued finite sequence f and objects i, j. Suppose

- (i) $i \in \mathrm{MeanLess}\, f$, and
- (ii) $j \in \mathrm{MeanMore}\, f$.

Then

- (iii) i, $j \in \mathrm{dom}\, f$, and
- (iv) $i \neq j$, and
- (v) $f(i) < \mathrm{Mean}\, f$, and
- (vi) $f(j) > \mathrm{Mean}\, f$.

Let us consider a positive heterogeneous non empty real-valued finite sequence f and natural numbers i, j. Now we state the propositions:

(40) Suppose $i, j \in \operatorname{dom} f$ and $i \neq j$ and $i \in \operatorname{MeanMore} f$ and $j \in \operatorname{MeanLess} f$. Then there exists a positive non empty real-valued finite sequence g such that

(i) $g = \operatorname{Replace}(f, i, j, \operatorname{Mean} f, (f(i) + f(j) - \operatorname{Mean} f))$, and

(ii) $\operatorname{GMean} f < \operatorname{GMean} g$.

The theorem is a consequence of (39), (22), (35), (27), and (33).

(41) Suppose $i, j \in \operatorname{dom} f$ and $i \neq j$ and $j \in \operatorname{MeanMore} f$ and $i \in \operatorname{MeanLess} f$. Then there exists a positive non empty real-valued finite sequence g such that

(i) $g = \operatorname{Replace}(f, i, j, \operatorname{Mean} f, (f(i) + f(j) - \operatorname{Mean} f))$, and

(ii) $\operatorname{GMean} f < \operatorname{GMean} g$.

The theorem is a consequence of (39), (22), (36), (27), and (33).

5. Homogenization of a Finite Sequence

Let f be a heterogeneous positive non empty real-valued finite sequence. The functor $\operatorname{Homogen} f$ yielding a real-valued finite sequence is defined by

(Def. 10) There exist natural numbers i, j such that

(i) $i =$ the element of $\operatorname{MeanLess} f$, and

(ii) $j =$ the element of $\operatorname{MeanMore} f$, and

(iii) $it = \operatorname{Replace}(f, i, j, \operatorname{Mean} f, (f(i) + f(j) - \operatorname{Mean} f))$.

Now we state the proposition:

(42) Let us consider a heterogeneous positive non empty real-valued finite sequence f. Then $\operatorname{dom} \operatorname{Homogen} f = \operatorname{dom} f$. The theorem is a consequence of (22).

Let f be a heterogeneous positive non empty real-valued finite sequence. Note that $\operatorname{Homogen} f$ is non empty.

Observe that $\operatorname{Homogen} f$ is positive.

Let us consider a heterogeneous positive non empty real-valued finite sequence f. Now we state the propositions:

(43) $\operatorname{Het} \operatorname{Homogen} f < \operatorname{Het} f$. The theorem is a consequence of (38) and (32).

(44) $\operatorname{Homogen} f$ and f are γ-equivalent. The theorem is a consequence of (38) and (28).

(45) $\operatorname{GMean} \operatorname{Homogen} f > \operatorname{GMean} f$. The theorem is a consequence of (39) and (41).

6. Cauchy Mean Theorem

Now we state the proposition:

(46) Let us consider a heterogeneous positive non empty real-valued finite sequence f. Then there exists a non empty homogeneous positive real-valued finite sequence g such that

(i) $\mathrm{GMean}\, g > \mathrm{GMean}\, f$, and

(ii) $\mathrm{Mean}\, g = \mathrm{Mean}\, f$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ there exists a positive non empty real-valued finite sequence g such that $\mathrm{Het}\, g = \$_1$ and $\mathrm{Mean}\, f = \mathrm{Mean}\, g$ and $\mathrm{GMean}\, g > \mathrm{GMean}\, f$ and $\mathrm{Het}\, g < \mathrm{Het}\, f$. There exists a natural number k such that $\mathcal{P}[k]$. For every natural number k such that $k \neq 0$ and $\mathcal{P}[k]$ there exists a natural number n such that $n < k$ and $\mathcal{P}[n]$. $\mathcal{P}[0]$ from [3, Sch. 7]. $\square$

Now we state the proposition:

(47) Inequality of arithmetic and geometric means:
Let us consider a non empty positive real-valued finite sequence f. Then $\mathrm{GMean}\, f \leqslant \mathrm{Mean}\, f$. The theorem is a consequence of (14), (13), and (46).

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. Tarski's classes and ranks. *Formalized Mathematics*, 1(**3**):563–567, 1990.
[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 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] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.
[7] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.
[8] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[9] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[10] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 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] Fuguo Ge and Xiquan Liang. On the partial product of series and related basic inequalities. *Formalized Mathematics*, 13(**3**):413–416, 2005.
[14] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.
[15] Artur Korniłowicz. On the real valued functions. *Formalized Mathematics*, 13(**1**):181–187, 2005.
[16] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.

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

[18] Benjamin Porter. Cauchy's mean theorem and the Cauchy-Schwarz inequality. *Archive of Formal Proofs*, March 2006. ISSN 2150-914x. `http://afp.sf.net/entries/Cauchy.shtml`, Formal proof development.

[19] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.

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

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

[22] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

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

[24] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

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

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

Received June 13, 2014

Special Issue: 25 years of the Mizar Mathematical Library

FORMALIZED MATHEMATICS
Vol. **22**, No. **2**, Pages 167–176, **2014**
DOI: 10.2478/forma-2014-0017

DE GRUYTER OPEN
degruyter.com/view/j/forma

Tarski Geometry Axioms

William Richter
Departament of Mathematics
Nortwestern University
Evanston, USA

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

Jesse Alama
Technical University of Vienna
Austria

Summary. This is the translation of the Mizar article containing readable Mizar proofs of some axiomatic geometry theorems formulated by the great Polish mathematician Alfred Tarski [8], and we hope to continue this work.[1]

The article is an extension and upgrading of the source code written by the first author with the help of `miz3` tool; his primary goal was to use proof checkers to help teach rigorous axiomatic geometry in high school using Hilbert's axioms.

This is largely a Mizar port of Julien Narboux's Coq pseudo-code [6]. We partially prove the theorem of [7] that Tarski's (extremely weak!) plane geometry axioms imply Hilbert's axioms. Specifically, we obtain Gupta's amazing proof which implies Hilbert's axiom `I1` that two points determine a line.

The primary Mizar coding was heavily influenced by [9] on axioms of incidence geometry. The original development was much improved using Mizar adjectives instead of predicates only, and to use this machinery in full extent, we have to construct some models of Tarski geometry. These are listed in the second section, together with appropriate registrations of clusters. Also models of Tarski's geometry related to real planes were constructed.

MSC: 51A05 51M04 03B35

Keywords: Tarski's geometry axioms; foundations of geometry; incidence geometry

MML identifier: `GTARSKI1`, version: `8.1.03 5.23.1213`

[1]The first author ported the code to HOL Light (`http://www.cl.cam.ac.uk/~jrh13/hol-light/`), which can be found in any recent subversion of HOL Light as `hol_light/RichterHilbertAxiomGeometry/TarskiAxiomGeometry_read.ml`

ISSN 1426–2630(Print), 1898-9934(Online)

The notation and terminology used in this paper have been introduced in the following articles: [2], [3], [5], [1], [11], [10], and [4].

1. Tarski's Geometry Axioms

We consider Tarski planes which extend 1-sorted structures and are systems

$$\langle \text{a carrier}, \text{a betweenness}, \text{an equidistance} \rangle$$

where the carrier is a set, the betweenness is a relation between (the carrier) $\times$ (the carrier) and the carrier, the equidistance is a relation between (the carrier) $\times$ (the carrier) and (the carrier) $\times$ (the carrier).

Let $\mathfrak{S}$ be a Tarski plane.

A point of $\mathfrak{S}$ is an element of $\mathfrak{S}$. Let A, B, C be points of $\mathfrak{S}$. We say that B lies between A and C if and only if

(Def. 1) $\langle\langle A, B\rangle, C\rangle \in$ the betweenness of $\mathfrak{S}$.

Let A, B, C, D be points of $\mathfrak{S}$. We say that $\overline{AB} \cong \overline{CD}$ if and only if

(Def. 2) $\langle\langle A, B\rangle, \langle C, D\rangle\rangle \in$ the equidistance of $\mathfrak{S}$.

Let A, B, C, X, Y, Z be points of $\mathfrak{S}$. We say that $\triangle ABC \cong \triangle XYZ$ if and only if

(Def. 3) (i) $\overline{AB} \cong \overline{XY}$, and

(ii) $\overline{AC} \cong \overline{XZ}$, and

(iii) $\overline{BC} \cong \overline{YZ}$.

Let A, B, C, D be points of $\mathfrak{S}$. We say that A, B, C, D are ordered if and only if

(Def. 4) (i) B lies between A and C, and

(ii) B lies between A and D, and

(iii) C lies between A and D, and

(iv) C lies between B and D.

We say that $\mathfrak{S}$ satisfies the axiom of congruence symmetry if and only if

(Def. 5) Let us consider points A, B of $\mathfrak{S}$. Then $\overline{AB} \cong \overline{BA}$.

We say that $\mathfrak{S}$ satisfies the axiom of congruence equivalence relation if and only if

(Def. 6) Let us consider points A, B, P, Q, R, S of $\mathfrak{S}$. Suppose

(i) $\overline{AB} \cong \overline{PQ}$, and

(ii) $\overline{AB} \cong \overline{RS}$.

Then $\overline{PQ} \cong \overline{RS}$.

We say that $\mathfrak{S}$ satisfies the axiom of congruence identity if and only if

(Def. 7) Let us consider points A, B, C of $\mathfrak{S}$. If $\overline{AB} \cong \overline{CC}$, then $A = B$.

We say that $\mathfrak{S}$ satisfies the axiom of segment construction if and only if

(Def. 8) Let us consider points A, Q, B, C of $\mathfrak{S}$. Then there exists a point X of $\mathfrak{S}$ such that

(i) A lies between Q and X, and

(ii) $\overline{AX} \cong \overline{BC}$.

We say that $\mathfrak{S}$ satisfies the axiom of SAS if and only if

(Def. 9) Let us consider points A, B, C, X, A_1, B_1, C_1, X_1 of $\mathfrak{S}$. Suppose

(i) $A \neq B$, and

(ii) $\triangle ABC \cong \triangle A_1B_1C_1$, and

(iii) B lies between A and X, and

(iv) B_1 lies between A_1 and X_1, and

(v) $\overline{BX} \cong \overline{B_1X_1}$.

Then $\overline{CX} \cong \overline{C_1X_1}$.

We say that $\mathfrak{S}$ satisfies the axiom of betweenness identity if and only if

(Def. 10) Let us consider points A, B of $\mathfrak{S}$. If B lies between A and A, then $A = B$.

We say that $\mathfrak{S}$ satisfies the axiom of Pasch if and only if

(Def. 11) Let us consider points A, B, P, Q, Z of $\mathfrak{S}$. Suppose

(i) P lies between A and Z, and

(ii) Q lies between B and Z.

Then there exists a point X of $\mathfrak{S}$ such that

(iii) X lies between P and B, and

(iv) X lies between Q and A.

We say that $\mathfrak{S}$ satisfies seven Tarski's geometry axioms if and only if

(Def. 12) $\mathfrak{S}$ satisfies the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of congruence identity, the axiom of segment construction, the axiom of SAS, the axiom of betweenness identity, and the axiom of Pasch.

2. Existence Proofs for Tarski Plane

We consider metric Tarski structures which extend metric structures and Tarski planes and are systems

$$\langle \text{a carrier}, \text{a distance}, \text{a betweenness}, \text{an equidistance} \rangle$$

where the carrier is a set, the distance is a function from (the carrier) $\times$ (the carrier) into $\mathbb{R}$, the betweenness is a relation between (the carrier) $\times$ (the carrier) and the carrier, the equidistance is a relation between (the carrier) $\times$ (the carrier) and (the carrier) $\times$ (the carrier).

Let $\mathfrak{M}$ be a metric structure.

A Tarski extension of $\mathfrak{M}$ is a metric Tarski structure and is defined by

(Def. 13) The metric structure of *it* = the metric structure of $\mathfrak{M}$.

Let $\mathfrak{M}$ be a non empty metric structure. One can check that every Tarski extension of $\mathfrak{M}$ is non empty.

Let $\mathfrak{M}$ be a non empty reflexive metric structure. Observe that every Tarski extension of $\mathfrak{M}$ is reflexive.

Let $\mathfrak{M}$ be a non empty discernible metric structure. Note that every Tarski extension of $\mathfrak{M}$ is discernible.

Let $\mathfrak{M}$ be a non empty symmetric metric structure. One can verify that every Tarski extension of $\mathfrak{M}$ is symmetric.

Let $\mathfrak{M}$ be a non empty triangle metric structure. Observe that every Tarski extension of $\mathfrak{M}$ is triangle.

Let $\mathfrak{S}$ be a metric structure and P, Q, R be elements of $\mathfrak{S}$. We say that Q is between P and R if and only if

(Def. 14) $\rho(P, R) = \rho(P, Q) + \rho(Q, R)$.

Let $\mathfrak{M}$ be a metric Tarski structure. We say that $\mathfrak{M}$ is naturally generated if and only if

(Def. 15) (i) for every points A, B, C of $\mathfrak{M}$, B lies between A and C iff B is between A and C, and

(ii) for every points A, B, C, D of $\mathfrak{M}$, $\overline{AB} \cong \overline{CD}$ iff $\rho(A, B) = \rho(C, D)$.

Now we state the proposition:

(1) Let us consider metric structures $\mathfrak{M}$, $\mathfrak{N}$, elements X, Y of $\mathfrak{M}$, and elements A, B of $\mathfrak{N}$. Suppose

(i) the metric structure of $\mathfrak{M}$ = the metric structure of $\mathfrak{N}$, and

(ii) $X = A$, and

(iii) $Y = B$.

Then $\rho(X, Y) = \rho(A, B)$.

Let $\mathfrak{N}$ be a non empty metric structure. Let us note that there exists a Tarski extension of $\mathfrak{N}$ which is naturally generated and there exists a metric space which is trivial and non empty.

The functor TrivialTarskiSpace yielding a metric Tarski structure is defined by the term

(Def. 16) The naturally generated Tarski extension of the trivial non empty metric space.

Note that TrivialTarskiSpace is trivial and non empty.

Now we state the proposition:

(2) Let us consider a trivial non empty metric space $\mathfrak{M}$ and elements A, B, C of $\mathfrak{M}$. Then A is between B and C.

Let us observe that TrivialTarskiSpace satisfies the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of congruence identity, the axiom of segment construction, the axiom of SAS, the axiom of betweenness identity, and the axiom of Pasch and TrivialTarskiSpace satisfies seven Tarski's geometry axioms and there exists a Tarski plane which is non empty and satisfies seven Tarski's geometry axioms and every Tarski plane which satisfies the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of congruence identity, the axiom of segment construction, the axiom of SAS, the axiom of betweenness identity, and the axiom of Pasch satisfies also seven Tarski's geometry axioms and every Tarski plane which satisfies seven Tarski's geometry axioms satisfies also the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of congruence identity, the axiom of segment construction, the axiom of SAS, the axiom of betweenness identity, and the axiom of Pasch.

3. Proofs of Basic Properties

From now on $\mathfrak{S}$ denotes Tarski plane and A, B, C, D, E, F, O, P, Q, R, S, V, W, U, X, Y, Z, A', B', C', D', X', Y', Z denote points of $\mathfrak{S}$.

Now we state the propositions:

(3) $\overline{AB} \cong \overline{BA}$.

(4) If $\overline{AB} \cong \overline{PQ}$ and $\overline{AB} \cong \overline{RS}$, then $\overline{PQ} \cong \overline{RS}$.

(5) If $\overline{AB} \cong \overline{CC}$, then $A = B$.

(6) There exists X such that

(i) A lies between Q and X, and

(ii) $\overline{AX} \cong \overline{BC}$.

(7) Suppose $A \neq B$ and $\triangle ABC \cong \triangle A'B'C'$ and B lies between A and X and B' lies between A' and X' and $\overline{BX} \cong \overline{B'X'}$. Then $\overline{CX} \cong \overline{C'X'}$.

(8) If B lies between A and A, then $A = B$.

(9) If P lies between A and Z and Q lies between B and Z, then there exists X such that X lies between P and B and X lies between Q and A.

(10) $\overline{AB} \cong \overline{AB}$. The theorem is a consequence of (3) and (4).

(11) If $\overline{AB} \cong \overline{CD}$, then $\overline{CD} \cong \overline{AB}$. The theorem is a consequence of (10) and (4).

(12) If $\overline{AB} \cong \overline{PQ}$ and $\overline{PQ} \cong \overline{RS}$, then $\overline{AB} \cong \overline{RS}$. The theorem is a consequence of (11) and (4).

(13) (i) A lies between A and A, and
(ii) $\overline{AA} \cong \overline{BB}$.
The theorem is a consequence of (6) and (5).

(14) A lies between Q and A. The theorem is a consequence of (6) and (5).

(15) If $A \neq B$ and B lies between A and X and B lies between A and Y and $\overline{BX} \cong \overline{BY}$, then $X = Y$. The theorem is a consequence of (10), (5), and (7).

(16) If P lies between A and Z, then P lies between Z and A. The theorem is a consequence of (14), (9), and (8).

(17) A lies between A and Q.

(18) If B lies between A and C and A lies between B and C, then $A = B$. The theorem is a consequence of (9) and (8).

(19) If B lies between A and D and C lies between B and D, then B lies between A and C. The theorem is a consequence of (9), (8), and (16).

Let us assume that $B \neq C$ and B lies between A and C and C lies between B and D. Now we state the propositions:

(20) C lies between A and D. The theorem is a consequence of (6), (16), (19), and (15).

(21) A, B, C, D are ordered. The theorem is a consequence of (20) and (16).

Let us assume that B lies between A and D and C lies between B and D. Now we state the propositions:

(22) A, B, C, D are ordered. The theorem is a consequence of (14), (19), and (21).

(23) A, B, C, D are ordered. The theorem is a consequence of (19), (14), (17), and (21).

Now we state the propositions:

(24) If B lies between A and C and B' lies between A' and C' and $\overline{AB} \cong \overline{A'B'}$ and $\overline{BC} \cong \overline{B'C'}$, then $\overline{AC} \cong \overline{A'C'}$. The theorem is a consequence of (3), (12), (5), (11), (13), and (7).

(25) If $\overline{AB} \cong \overline{CD}$, then $\overline{BA} \cong \overline{DC}$. The theorem is a consequence of (3) and (12).

(26) If $A \neq B$ and B lies between A and X and B lies between A and Y and $\overline{AX} \cong \overline{AY}$, then $X = Y$. The theorem is a consequence of (6), (11), (5), (16), (21), and (15).

(27) If B lies between A and C and B' lies between A' and C' and $\overline{AB} \cong \overline{A'B'}$ and $\overline{AC} \cong \overline{A'C'}$, then $\overline{BC} \cong \overline{B'C'}$. The theorem is a consequence of (5), (11), (6), (24), (12), and (26).

(28) If $O \neq A$, then there exists X and there exists Y such that O lies between B and X and O lies between A and Y and $\triangle XYO \cong \triangle ABO$. The theorem is a consequence of (6), (25), (3), (11), (16), and (7).

(29) If B lies between A and C and C lies between A and D, then A, B, C, D are ordered. The theorem is a consequence of (16) and (23).

(30) If $A \neq B$ and B lies between A and C and B lies between A and D, then there exists X such that A, B, C, X are ordered and A, B, D, X are ordered. The theorem is a consequence of (6), (29), (16), (3), (12), (11), (24), and (15).

(31) If $A \neq B$ and B lies between A and C and B lies between A and D and $B \neq C$ and $B \neq D$, then B does not lie between C and D. The theorem is a consequence of (30), (21), and (18).

(32) Suppose $\triangle ABC \cong \triangle A'B'C'$ and X lies between A and C and X' lies between A' and C' and $\overline{CX} \cong \overline{C'X'}$. Then $\overline{BX} \cong \overline{B'X'}$. The theorem is a consequence of (5), (11), (8), (6), (12), (25), (7), (16), and (19).

(33) Suppose C lies between B and D' and D lies between B and C' and $\overline{CD'} \cong \overline{CD}$ and $\overline{DC'} \cong \overline{CD}$ and $\overline{D'C'} \cong \overline{CD}$. Then there exists E such that

(i) E lies between C and C', and

(ii) E lies between D and D', and

(iii) $\overline{CE} \cong \overline{C'E}$, and

(iv) $\overline{DE} \cong \overline{D'E}$.

The theorem is a consequence of (16), (9), (11), (10), (12), (32), and (3).

(34) Suppose E lies between D and D' and $\overline{CD'} \cong \overline{CD}$ and $\overline{DE} \cong \overline{D'E}$ and $C \neq D$ and $E \neq D$. Then there exists P and there exists R and there exists Q such that R lies between P and Q and C lies between R and D' and C lies between E and P and $\triangle RCP \cong \triangle RCQ$ and $\overline{RC} \cong \overline{EC}$ and $\overline{PR} \cong \overline{DE}$. The theorem is a consequence of (11), (5), (28), (12), (6), (16), (25), (7), and (10).

(35) If $A \neq B$ and B lies between A and C and $\overline{AP} \cong \overline{AQ}$ and $\overline{BP} \cong \overline{BQ}$, then $\overline{CP} \cong \overline{CQ}$. The theorem is a consequence of (10), (7), and (25).

(36) If X lies between A and C and $\overline{AP} \cong \overline{AQ}$ and $\overline{CP} \cong \overline{CQ}$, then $\overline{XP} \cong \overline{XQ}$. The theorem is a consequence of (10), (25), and (32).

(37) If $A \neq B$ and B lies between A and C and B lies between A and D, then D lies between B and C or C lies between B and D. The theorem is a consequence of (17), (14), (6), (29), (5), (11), (8), (21), (16), (3), (12), (24), (15), (25), (7), (33), (34), (35), and (36).

Let us consider $\mathfrak{S}$, A, B, and C. We say that A, B and C are collinear if and only if

(Def. 17) (i) B lies between A and C, or

(ii) C lies between B and A, or

(iii) A lies between C and B.

Let us consider X. We say that X lies on the line passing through A and B if and only if

(Def. 18) (i) $A \neq B$, and

(ii) B lies between A and X or X lies between B and A or A lies between X and B.

Let us consider Y. We say that the line passing through A and B is equal to the line passing through X and Y if and only if

(Def. 19) (i) $A \neq B$, and

(ii) $X \neq Y$, and

(iii) for every C, C lies on the line passing through A and B iff C lies on the line passing through X and Y.

Now we state the propositions:

(38) If $A \neq B$ and $A \neq X$ and X lies on the line passing through A and B and C lies on the line passing through A and B, then C lies on the line passing through A and X. The theorem is a consequence of (16), (6), (11), (5), (37), (21), (29), and (19).

(39) If $A \neq B$ and $A \neq X$ and X lies on the line passing through A and B, then the line passing through A and B is equal to the line passing through A and X. The theorem is a consequence of (38) and (16).

Let us assume that $A \neq B$. Now we state the propositions:

(40) the line passing through A and B is equal to the line passing through A and B.

(41) the line passing through A and B is equal to the line passing through B and A. The theorem is a consequence of (16).

Now we state the propositions:

(42) Suppose $A \neq B$ and $C \neq D$ and the line passing through A and B is equal to the line passing through C and D. Then the line passing through C and D is equal to the line passing through A and B.

(43) Suppose $A \neq B$ and $C \neq D$ and $E \neq F$ and the line passing through A and B is equal to the line passing through C and D and the line passing through C and D is equal to the line passing through E and F. Then the line passing through A and B is equal to the line passing through E and F.

(44) If X lies on the line passing through A and B and the line passing through A and B is equal to the line passing through C and D, then X lies on the line passing through C and D.

(45) If $A \neq B$ and $B \neq Y$ and Y lies on the line passing through A and B, then the line passing through A and B is equal to the line passing through Y and B. The theorem is a consequence of (41) and (39).

(46) Suppose $A \neq B$ and $X \neq Y$ and A lies on the line passing through X and Y and B lies on the line passing through X and Y. Then the line passing through X and Y is equal to the line passing through A and B. The theorem is a consequence of (41), (39), and (45).

4. Construction of the Euclidean Example

The functor Tarski$_0$Space yielding a metric Tarski structure is defined by the term

(Def. 20) The naturally generated Tarski extension of $\ominus$.

Note that Tarski$_0$Space is reflexive symmetric and non empty.

Let $\mathfrak{M}$ be a non empty metric structure. We say that $\mathfrak{M}$ is close-everywhere if and only if

(Def. 21) Let us consider elements A, B of $\mathfrak{M}$. Then $\rho(A, B) = 0$.

Let us note that Tarski$_0$Space is close-everywhere and Tarski$_0$Space satisfies the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of segment construction, the axiom of SAS, and the axiom of Pasch.

The functor TarskiSpace yielding a metric Tarski structure is defined by the term

(Def. 22) The naturally generated Tarski extension of the metric space of real numbers.

One can check that TarskiSpace is non empty and TarskiSpace is reflexive symmetric and discernible and every element of TarskiSpace is real and every element of the metric space of real numbers is real.

Now we state the proposition:

(47) Let us consider elements A, B, C of the metric space of real numbers. If $B \in [A, C]$, then B is between A and C. The theorem is a consequence of (3).

Let us observe that TarskiSpace satisfies the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of congruence identity, the axiom of segment construction, and the axiom of betweenness identity.

References

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

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

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

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

[5] Stanisława Kanas, Adam Lecko, and Mariusz Startek. Metric spaces. *Formalized Mathematics*, 1(**3**):607–610, 1990.

[6] Julien Narboux. Mechanical theorem proving in Tarski's geometry. In F. Botana and T. Recio, editors, *Automated Deduction in Geometry*, volume 4869, pages 139–156, 2007.

[7] Wolfram Schwabhäuser, Wanda Szmielew, and Alfred Tarski. *Metamathematische Methoden in der Geometrie*. Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1983.

[8] Alfred Tarski and Steven Givant. Tarski's system of geometry. *Bulletin of Symbolic Logic*, 5(2):175–214, 1999.

[9] Wojciech A. Trybulec. Axioms of incidence. *Formalized Mathematics*, 1(**1**):205–213, 1990.

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

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

Received June 16, 2014

Special Issue: 25 years of the Mizar Mathematical Library

FORMALIZED MATHEMATICS
Vol. 22, No. 2, Pages 177–178, 2014
DOI: 10.2478/forma-2014-0018

DE GRUYTER OPEN
degruyter.com/view/j/forma

A Note on the Seven Bridges of Königsberg Problem

Adam Naumowicz
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

Summary. In this paper we account for the formalization of the seven bridges of Königsberg puzzle. The problem originally posed and solved by Euler in 1735 is historically notable for having laid the foundations of graph theory, cf. [7]. Our formalization utilizes a simple set-theoretical graph representation with four distinct sets for the graph's vertices and another seven sets that represent the edges (bridges). The work appends the article by Nakamura and Rudnicki [10] by introducing the classic example of a graph that does not contain an Eulerian path.

This theorem is item `#54` from the "Formalizing 100 Theorems" list maintained by Freek Wiedijk at `http://www.cs.ru.nl/F.Wiedijk/100/` .

MSC: 05C45 05C62 03B35

Keywords: Eulerian paths; Eulerian cycles; Königsberg bridges problem

MML identifier: `GRAPH_3A`, version: `8.1.03 5.23.1213`

The notation and terminology used in this paper have been introduced in the following articles: [11], [2], [8], [3], [4], [9], [10], [6], [1], [13], [12], and [5].

The functors: KVertices and KEdges yielding sets are defined by terms,

(Def. 1) $\{0, 1, 2, 3\}$,

(Def. 2) $\{10, 20, 30, 40, 50, 60, 70\}$,

respectively. The functors: KSource and KTarget yielding functions from KEdges into KVertices are defined by terms,

(Def. 3) $\{\langle 10, 0\rangle, \langle 20, 0\rangle, \langle 30, 0\rangle, \langle 40, 1\rangle, \langle 50, 1\rangle, \langle 60, 2\rangle, \langle 70, 2\rangle\}$,

(Def. 4) $\{\langle 10, 1\rangle, \langle 20, 2\rangle, \langle 30, 3\rangle, \langle 40, 2\rangle, \langle 50, 2\rangle, \langle 60, 3\rangle, \langle 70, 3\rangle\}$,

respectively. The functor KönigsbergBridges yielding a graph is defined by the term

ISSN 1426–2630(Print), 1898-9934(Online)

(Def. 5) $\langle$KVertices, KEdges, KSource, KTarget$\rangle$.

Let us observe that KönigsbergBridges is finite and connected.

Let us consider a vertex v of KönigsbergBridges. Now we state the propositions:

(1) If $v = 0$, then the degree of $v = 3$. PROOF: EdgesIn $v = \emptyset$ by [3, (1)]. EdgesOut $v = \{10, 20, 30\}$ by [3, (1)]. The degree of $v = 3$ by [10, (24)]. □

(2) If $v = 1$, then the degree of $v = 3$. PROOF: EdgesIn $v = \{10\}$ by [3, (1)]. EdgesOut $v = \{40, 50\}$ by [3, (1)]. The degree of $v = 3$ by [10, (24)]. □

(3) If $v = 2$, then the degree of $v = 5$. PROOF: EdgesIn $v = \{20, 40, 50\}$ by [3, (1)]. EdgesOut $v = \{60, 70\}$ by [3, (1)]. The degree of $v = 5$ by [10, (24)]. □

(4) If $v = 3$, then the degree of $v = 3$. PROOF: EdgesIn $v = \{30, 60, 70\}$ by [3, (1)]. EdgesOut $v = \emptyset$ by [3, (1)]. The degree of $v = 3$ by [10, (24)]. □

Now we state the propositions:

(5) SEVEN BRIDGES OF KÖNIGSBERG:
There exists no path p of KönigsbergBridges such that p is cyclic and Eulerian. The theorem is a consequence of (1).

(6) There exists no path p of KönigsbergBridges such that p is non cyclic and Eulerian. The theorem is a consequence of (4), (1), and (2).

References

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

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

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

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

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

[6] Czesław Byliński and Piotr Rudnicki. The correspondence between monotonic many sorted signatures and well-founded graphs. Part I. *Formalized Mathematics*, 5(**4**):577–582, 1996.

[7] Gary Chartrand. *Introductory Graph Theory*. New York: Dover, 1985.

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

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

[10] Yatsuka Nakamura and Piotr Rudnicki. Euler circuits and paths. *Formalized Mathematics*, 6(**3**):417–425, 1997.

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

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

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

Received June 16, 2014

Special Issue: 25 years of the Mizar Mathematical Library

FORMALIZED MATHEMATICS
Vol. **22**, No. **2**, Pages 179–186, **2014**
DOI: 10.2478/forma-2014-0019

DE GRUYTER
OPEN
degruyter.com/view/j/forma

Topological Manifolds[1]

Karol Pąk
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

Summary. Let us recall that a topological space M is a topological manifold if M is second-countable Hausdorff and locally Euclidean, i.e. each point has a neighborhood that is homeomorphic to an open ball of $\mathcal{E}^n$ for some n. However, if we would like to consider a topological manifold with a boundary, we have to extend this definition. Therefore, we introduce here the concept of a locally Euclidean space that covers both cases (with and without a boundary), i.e. where each point has a neighborhood that is homeomorphic to a closed ball of $\mathcal{E}^n$ for some n.

Our purpose is to prove, using the Mizar formalism, a number of properties of such locally Euclidean spaces and use them to demonstrate basic properties of a manifold. Let T be a locally Euclidean space. We prove that every interior point of T has a neighborhood homeomorphic to an open ball and that every boundary point of T has a neighborhood homeomorphic to a closed ball, where additionally this point is transformed into a point of the boundary of this ball. When T is n-dimensional, i.e. each point of T has a neighborhood that is homeomorphic to a closed ball of $\mathcal{E}^n$, we show that the interior of T is a locally Euclidean space without boundary of dimension n and the boundary of T is a locally Euclidean space without boundary of dimension $n-1$. Additionally, we show that every connected component of a compact locally Euclidean space is a locally Euclidean space of some dimension. We prove also that the Cartesian product of locally Euclidean spaces also forms a locally Euclidean space. We determine the interior and boundary of this product and show that its dimension is the sum of the dimensions of its factors. At the end, we present several consequences of these results for topological manifolds. This article is based on [14].

MSC: 57N15 03B35

Keywords: locally Euclidean spaces; interior; boundary; Cartesian product

MML identifier: `MFOLD_0`, version: `8.1.03 5.23.1213`

[1]The paper has been financed by the resources of the Polish National Science Centre granted by decision no. DEC-2012/07/N/ST6/02147.

ISSN 1426–2630(Print), 1898-9934(Online)

The notation and terminology used in this paper have been introduced in the following articles: [30], [15], [19], [1], [10], [23], [24], [28], [11], [5], [12], [6], [7], [29], [3], [4], [8], [26], [33], [25], [32], [20], [34], [13], [21], and [9].

1. Preliminaries

From now on n, m denote natural numbers.

Now we state the proposition:

(1) Let us consider a non empty topological space M, a point q of M, a real number r, and a point p of $\mathcal{E}^n_{\mathrm{T}}$. Suppose $r > 0$. Let us consider a neighbourhood U of q. Suppose $M\restriction U$ and $\mathbb{B}_r(p)$ are homeomorphic. Then there exists a neighbourhood W of q such that

(i) $W \subseteq \operatorname{Int} U$, and

(ii) $M\restriction W$ and $\operatorname{Tdisk}(p, r)$ are homeomorphic.

2. Locally Euclidean Spaces

In the sequel M, M_1, M_2 denote non empty topological spaces.

Let us consider M. We say that M is locally Euclidean if and only if

(Def. 1) Let us consider a point p of M. Then there exists a neighbourhood U of p and there exists n such that $M\restriction U$ and $\operatorname{Tdisk}(0_{\mathcal{E}^n_{\mathrm{T}}}, 1)$ are homeomorphic.

Let us consider n. We say that M is n-locally Euclidean if and only if

(Def. 2) Let us consider a point p of M. Then there exists a neighbourhood U of p such that $M\restriction U$ and $\operatorname{Tdisk}(0_{\mathcal{E}^n_{\mathrm{T}}}, 1)$ are homeomorphic.

Observe that $\operatorname{Tdisk}(0_{\mathcal{E}^n_{\mathrm{T}}}, 1)$ is n-locally Euclidean.

Note that there exists a non empty topological space which is n-locally Euclidean.

Observe that every non empty topological space which is n-locally Euclidean is also locally Euclidean.

3. Locally Euclidean Spaces With and Without a Boundary

Let M be a locally Euclidean non empty topological space. The functor $\operatorname{Int} M$ yielding a subset of M is defined by

(Def. 3) Let us consider a point p of M. Then $p \in it$ if and only if there exists a neighbourhood U of p and there exists n such that $M\restriction U$ and $\mathbb{B}_1(0_{\mathcal{E}^n_{\mathrm{T}}})$ are homeomorphic.

Observe that $\operatorname{Int} M$ is non empty and open.

The functor $\operatorname{Fr} M$ yielding a subset of M is defined by the term

(Def. 4) $(\operatorname{Int} M)^{c}$.

Now we state the proposition:

(2) Boundary Points of Locally Euclidean Spaces:
Let us consider a locally Euclidean non empty topological space M and a point p of M. Then $p \in \operatorname{Fr} M$ if and only if there exists a neighbourhood U of p and there exists a natural number n and there exists a function h from $M \restriction U$ into $\operatorname{Tdisk}(0_{\mathcal{E}^{n}_{\mathrm{T}}}, 1)$ such that h is a homeomorphism and $h(p) \in \operatorname{Sphere}(0_{\mathcal{E}^{n}_{\mathrm{T}}}, 1)$. Proof: If $p \in \operatorname{Fr} M$, then there exists a neighbourhood U of p and there exists a natural number n and there exists a function h from $M \restriction U$ into $\operatorname{Tdisk}(0_{\mathcal{E}^{n}_{\mathrm{T}}}, 1)$ such that h is a homeomorphism and $h(p) \in \operatorname{Sphere}(0_{\mathcal{E}^{n}_{\mathrm{T}}}, 1)$ by [34, (16)], [18, (25)], [6, (94)], [20, (18)]. $\square$

4. Interior and Boundary of Locally Euclidean Spaces

Let M be a locally Euclidean non empty topological space. We say that M is without boundary if and only if

(Def. 5) $\operatorname{Int} M =$ the carrier of M.

Let us consider n. Let us observe that $\mathbb{B}_1(0_{\mathcal{E}^{n}_{\mathrm{T}}})$ is n-locally Euclidean and $\mathbb{B}_1(0_{\mathcal{E}^{n}_{\mathrm{T}}})$ is without boundary.

Let n be a non zero natural number. Let us observe that $\operatorname{Tdisk}(0_{\mathcal{E}^{n}_{\mathrm{T}}}, 1)$ has boundary.

Let us consider n. One can check that there exists an n-locally Euclidean non empty topological space which is without boundary.

Let n be a non zero natural number. One can verify that there exists an n-locally Euclidean non empty topological space which is compact and has boundary.

Let M be a without boundary locally Euclidean non empty topological space. Let us observe that $\operatorname{Fr} M$ is empty.

Let M be a locally Euclidean non empty topological space with boundary. Observe that $\operatorname{Fr} M$ is non empty.

Let n be a zero natural number. Let us observe that every n-locally Euclidean non empty topological space is without boundary.

Now we state the propositions:

(3) M is a without boundary locally Euclidean non empty topological space if and only if for every point p of M, there exists a neighbourhood U of p and there exists n such that $M \restriction U$ and $\mathbb{B}_1(0_{\mathcal{E}^{n}_{\mathrm{T}}})$ are homeomorphic.

(4) Let us consider a locally Euclidean non empty topological space M with boundary, a point p of M, and n. Suppose there exists a neighbourhood U of p such that $M \restriction U$ and $\operatorname{Tdisk}(0_{\mathcal{E}^{n+1}_{\mathrm{T}}}, 1)$ are homeomorphic. Let us consider a point p_1 of $M \restriction \operatorname{Fr} M$. Suppose $p = p_1$. Then there exists a neighbourhood

U of p_1 such that $(M \restriction \operatorname{Fr} M) \restriction U$ and $\mathbb{B}_1(0_{\mathcal{E}^n_{\mathrm{T}}})$ are homeomorphic. Proof: Set $n_1 = n + 1$. Set $T_1 = \mathcal{E}^{n_1}_{\mathrm{T}}$. Consider W being a neighbourhood of p such that $M \restriction W$ and $\mathrm{Tdisk}(0_{T_1}, 1)$ are homeomorphic. Set $T_2 = \mathcal{E}^n_{\mathrm{T}}$. Set $S = \mathrm{Sphere}(0_{T_1}, 1)$. Set $F = \operatorname{Fr} M$. Set $M_4 = M \restriction F$. Consider U being a neighbourhood of p, m being a natural number, h being a function from $M \restriction U$ into $\mathrm{Tdisk}(0_{\mathcal{E}^m_{\mathrm{T}}}, 1)$ such that h is a homeomorphism and $h(p) \in \mathrm{Sphere}(0_{\mathcal{E}^m_{\mathrm{T}}}, 1)$. Reconsider $I_3 = \operatorname{Int} U$ as a subset of $M \restriction U$. Set $M_6 = M \restriction U$. Reconsider $F_1 = F \cap \operatorname{Int} U$ as a non empty subset of M_6. Consider W being a subset of T_1 such that $W \in$ the topology of T_1 and $h^\circ I_3 = W \cap \Omega_{\mathrm{Tdisk}(0_{T_1},1)}$. Reconsider $h_{14} = h(p)$ as a point of T_1. Reconsider $H_3 = h_{14}$ as a point of $\mathcal{E}^{n_1}$. Consider s being a real number such that $s > 0$ and $\mathrm{Ball}(H_3, s) \subseteq W$. Set $m = \min(\frac{s}{2}, \frac{1}{2})$. Set $V_0 = S \cap \mathrm{Ball}(h_{14}, m)$. Set $h_9 = h^{-1}(V_0)$. $h_9 \subseteq F$ by [20, (9)], (2). Reconsider $h_8 = h^\circ F_1$ as a subset of T_1. $V_0 \subseteq h_8$. $h_8 \cap \mathrm{Ball}(h_{14}, m) \subseteq V_0$ by [11, (67)], [34, (23)], [33, (123)], [31, (5)]. □

Let M be a locally Euclidean non empty topological space. Note that $M \restriction \operatorname{Int} M$ is locally Euclidean and $M \restriction \operatorname{Int} M$ is without boundary.

Let M be a locally Euclidean non empty topological space with boundary. Note that $M \restriction \operatorname{Fr} M$ is locally Euclidean and $M \restriction \operatorname{Fr} M$ is without boundary.

5. Cartesian Product of Locally Euclidean Spaces

Let N, M be locally Euclidean non empty topological spaces. Note that $N \times M$ is locally Euclidean.

Let us consider locally Euclidean non empty topological spaces N, M. Now we state the propositions:

(5) $\operatorname{Int}(N \times M) = \operatorname{Int} N \times \operatorname{Int} M$. Proof: Set $N_1 = N \times M$. Set $I_2 = \operatorname{Int} N$. Set $I_1 = \operatorname{Int} M$. $\operatorname{Int} N_1 \subseteq I_2 \times I_1$ by [9, (87)], (2), [20, (19)], [27, (19), (15)]. □

(6) $\operatorname{Fr}(N \times M) = \Omega_N \times \operatorname{Fr} M \cup \operatorname{Fr} N \times \Omega_M$. The theorem is a consequence of (5).

Let N, M be without boundary locally Euclidean non empty topological spaces. Let us observe that $N \times M$ is without boundary.

Let N be a locally Euclidean non empty topological space and M be a locally Euclidean non empty topological space with boundary. Note that $N \times M$ has boundary and $M \times N$ has boundary.

6. FIXED DIMENSION LOCALLY EUCLIDEAN SPACES

Let us consider n. Let M be an n-locally Euclidean non empty topological space. Observe that the functor $\operatorname{Int} M$ yields a subset of M and is defined by

(Def. 6) Let us consider a point p of M. Then $p \in it$ if and only if there exists a neighbourhood U of p such that $M \restriction U$ and $\mathbb{B}_1(0_{\mathcal{E}^n_{\mathrm{T}}})$ are homeomorphic.

Let us note that the functor $\operatorname{Fr} M$ yields a subset of M and is defined by

(Def. 7) Let us consider a point p of M. Then $p \in it$ if and only if there exists a neighbourhood U of p and there exists a function h from $M \restriction U$ into $\operatorname{Tdisk}(0_{\mathcal{E}^n_{\mathrm{T}}}, 1)$ such that h is a homeomorphism and $h(p) \in \operatorname{Sphere}(0_{\mathcal{E}^n_{\mathrm{T}}}, 1)$.

Now we state the propositions:

(7) If M_1 is locally Euclidean and M_1 and M_2 are homeomorphic, then M_2 is locally Euclidean.

(8) If M_1 is n-locally Euclidean and M_2 is locally Euclidean and M_1 and M_2 are homeomorphic, then M_2 is n-locally Euclidean.

Now we state the propositions:

(9) TOPOLOGICAL INVARIANCE OF DIMENSION OF LOCALLY EUCLIDEAN SPACES:
If M is n-locally Euclidean and m-locally Euclidean, then $n = m$.

(10) M is a without boundary n-locally Euclidean non empty topological space if and only if for every point p of M, there exists a neighbourhood U of p such that $M \restriction U$ and $\mathbb{B}_1(0_{\mathcal{E}^n_{\mathrm{T}}})$ are homeomorphic. PROOF: M is n-locally Euclidean by [20, (16)], [16, (9)], [17, (21)], [34, (16)]. M is without boundary. $\square$

Let n, m be elements of $\mathbb{N}$, N be an n-locally Euclidean non empty topological space, and M be an m-locally Euclidean non empty topological space.

DIMENSION OF THE CARTESIAN PRODUCT OF LOCALLY EUCLIDEAN SPACES: $N \times M$ is $(n+m)$-locally Euclidean.

Let us consider n. Let M be an n-locally Euclidean non empty topological space.

DIMENSION OF THE INTERIOR OF LOCALLY EUCLIDEAN SPACES: $M \restriction \operatorname{Int} M$ is n-locally Euclidean as a non empty topological space.

Let n be a non zero natural number and M be an n-locally Euclidean non empty topological space with boundary.

DIMENSION OF THE BOUNDARY OF LOCALLY EUCLIDEAN SPACES: $M \restriction \operatorname{Fr} M$ is $(n -' 1)$-locally Euclidean as a non empty topological space.

7. Connected Components of Locally Euclidean Spaces

Now we state the proposition:

(11) Let us consider a compact locally Euclidean non empty topological space M and a subset C of M. Suppose C is a component. Then

(i) C is open, and

(ii) there exists n such that $M \restriction C$ is an n-locally Euclidean non empty topological space.

Proof: Define $\mathcal{P}[\text{point of } M, \text{subset of } M] \equiv \$_2$ is a neighbourhood of $\$_1$ and there exists n such that $M \restriction \$_2$ and $\mathrm{Tdisk}(0_{\mathcal{E}^n_{\mathrm{T}}}, 1)$ are homeomorphic. Consider p being an object such that $p \in C$. For every point x of M, there exists an element y of 2^{α} such that $\mathcal{P}[x, y]$, where α is the carrier of M. Consider W being a function from M into $2^{(\text{the carrier of } M)}$ such that for every point x of M, $\mathcal{P}[x, W(x)]$ from [7, Sch. 3]. Reconsider $M_3 = M \restriction C$ as a non empty connected topological space. Define $\mathcal{D}[\text{object}, \text{object}] \equiv \$_2 \in C$ and for every subset A of M such that $A = W(\$_2)$ holds $\mathrm{Int}\, A = \$_1$. Set $I_5 = \{\mathrm{Int}\, U$, where U is a subset of $M : U \in \mathrm{rng}(W \restriction C)\}$. $I_5 \subseteq 2^{\alpha}$, where α is the carrier of M. Reconsider $R = I_5 \cup \{C^{\mathrm{c}}\}$ as a family of subsets of M. For every subset A of M such that $A \in R$ holds A is open by [9, (136)]. For every subset A of M such that $A \in \mathrm{rng}\, W$ holds A is connected and $\mathrm{Int}\, A$ is not empty by [33, (113)], [23, (14)]. The carrier of $M \subseteq \bigcup R$ by [33, (57)], [6, (47)], [9, (136)]. Consider R_1 being a family of subsets of M such that $R_1 \subseteq R$ and R_1 is a cover of M and R_1 is finite. Set $R_2 = R_1 \setminus \{C^{\mathrm{c}}\}$. Consider x_1 being a set such that $p \in x_1$ and $x_1 \in R_2$. For every set x, $x \in C$ iff there exists a subset Q of M such that Q is open and $Q \subseteq C$ and $x \in Q$ by [34, (16)], [22, (16)]. $\bigcup R_2 \subseteq C$ by [9, (56), (136)], [34, (16)], [6, (47)]. For every object x such that $x \in R_2$ there exists an object y such that $\mathcal{D}[x, y]$ by [9, (56), (136)], [6, (47)]. Consider c being a function such that $\mathrm{dom}\, c = R_2$ and for every object x such that $x \in R_2$ holds $\mathcal{D}[x, c(x)]$ from [2, Sch. 1]. Reconsider $c_3 = c(x_1)$ as a point of M. Consider n such that $M \restriction W(c_3)$ and $\mathrm{Tdisk}(0_{\mathcal{E}^n_{\mathrm{T}}}, 1)$ are homeomorphic. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant \overline{\overline{R_2}}$, then there exists a family R_3 of subsets of M such that $\overline{\overline{R_3}} = \$_1$ and $R_3 \subseteq R_2$ and $\bigcup(W^{\circ}(c^{\circ} R_3))$ is a connected subset of M and for every subsets A, B of M such that $A \in R_3$ and $B = W(c(A))$ holds $M \restriction B$ and $\mathrm{Tdisk}(0_{\mathcal{E}^n_{\mathrm{T}}}, 1)$ are homeomorphic. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [3, (13), (44)], [1, (68)], [9, (56), (136), (74)]. $\mathcal{P}[0]$ by [9, (2)]. For every natural number k, $\mathcal{P}[k]$ from [3, Sch. 2]. For every point p of M_3, there exists a neighbourhood U of p such that $M_3 \restriction U$ and $\mathrm{Tdisk}(0_{\mathcal{E}^n_{\mathrm{T}}}, 1)$ are homeomorphic by [34, (16)], [22, (16), (28)], [34, (22)]. □

Let us consider a compact locally Euclidean non empty topological space M. Now we state the propositions:

(12) There exists a partition P of the carrier of M such that for every subset A of M such that $A \in P$ holds A is open and a component and there exists n such that $M \restriction A$ is an n-locally Euclidean non empty topological space. Proof: Set $P = \{$the component of p, where p is a point of M : not contradiction$\}$. $P \subseteq 2^{\alpha}$, where α is the carrier of M. The carrier of $M \subseteq \bigcup P$ by [23, (38)]. For every subset A of M such that $A \in P$ holds $A \neq \emptyset$ and for every subset B of M such that $B \in P$ holds $A = B$ or A misses B by [23, (42)]. $\square$

(13) If M is connected, then there exists n such that M is n-locally Euclidean. The theorem is a consequence of (11) and (8).

8. Topological Manifold

Let us consider n. Observe that there exists a non empty topological space which is second-countable, Hausdorff, and n-locally Euclidean.

A topological manifold is a second-countable Hausdorff locally Euclidean non empty topological space. Let us consider n. Let M be a topological manifold. We introduce M is n-dimensional as a synonym of M is n-locally Euclidean.

Note that there exists a topological manifold which is n-dimensional and without boundary.

Let n be a non zero natural number. Note that there exists a topological manifold which is n-dimensional and compact and has boundary.

Let M be a topological manifold. Let us observe that every non empty subspace of M is second-countable and Hausdorff.

Let M_1, M_2 be topological manifolds. Observe that $M_1 \times M_2$ is second-countable and Hausdorff.

References

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

[2] Grzegorz Bancerek. Tarski's classes and ranks. *Formalized Mathematics*, 1(**3**):563–567, 1990.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 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] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

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

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

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

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

[11] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.

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

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

[14] Ryszard Engelking. *Teoria wymiaru.* PWN, 1981.

[15] Adam Grabowski. Properties of the product of compact topological spaces. *Formalized Mathematics*, 8(**1**):55–59, 1999.

[16] Zbigniew Karno. Separated and weakly separated subspaces of topological spaces. *Formalized Mathematics*, 2(**5**):665–674, 1991.

[17] Artur Korniłowicz. Jordan curve theorem. *Formalized Mathematics*, 13(**4**):481–491, 2005.

[18] Artur Korniłowicz. The definition and basic properties of topological groups. *Formalized Mathematics*, 7(**2**):217–225, 1998.

[19] Artur Korniłowicz and Yasunari Shidama. Brouwer fixed point theorem for disks on the plane. *Formalized Mathematics*, 13(**2**):333–336, 2005.

[20] Artur Korniłowicz and Yasunari Shidama. Intersections of intervals and balls in $\mathcal{E}^n_{\mathrm{T}}$. *Formalized Mathematics*, 12(**3**):301–306, 2004.

[21] Robert Milewski. Bases of continuous lattices. *Formalized Mathematics*, 7(**2**):285–294, 1998.

[22] Yatsuka Nakamura and Andrzej Trybulec. Components and unions of components. *Formalized Mathematics*, 5(**4**):513–517, 1996.

[23] Beata Padlewska. Connected spaces. *Formalized Mathematics*, 1(**1**):239–244, 1990.

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

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

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

[27] Karol Pąk. Tietze extension theorem for n-dimensional spaces. *Formalized Mathematics*, 22(1):11–19. doi:10.2478/forma-2014-0002.

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

[29] Marco Riccardi. The definition of topological manifolds. *Formalized Mathematics*, 19(**1**):41–44, 2011. doi:10.2478/v10037-011-0007-4.

[30] Andrzej Trybulec. A Borsuk theorem on homotopy types. *Formalized Mathematics*, 2(**4**):535–545, 1991.

[31] Andrzej Trybulec. On the geometry of a Go-Board. *Formalized Mathematics*, 5(**3**):347–352, 1996.

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

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

[34] Mirosław Wysocki and Agata Darmochwał. Subsets of topological spaces. *Formalized Mathematics*, 1(**1**):231–237, 1990.

Received June 16, 2014

Index of MML Identifiers