Contents

Formaliz. Math. 20 (**2**)

FORMALIZED MATHEMATICS
Vol. 20, No. 2, Pages 97–104, 2012
DOI: 10.2478/v10037-012-0013-1

VERSITA
versita.com/fm/

Fundamental Group of n-sphere for $n \geq 2$

Marco Riccardi
Via del Pero 102
54038 Montignoso
Italy

Artur Korniłowicz[1]
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

Summary. Triviality of fundamental groups of spheres of dimension greater than 1 is proven, [17].

MML identifier: TOPALG_6, version: 7.12.02 4.176.1140

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

1. Preliminaries

In this paper T, U are non empty topological spaces, t is a point of T, and n is a natural number.

Let S be a topological space and let T be a non empty topological space. Note that every function from S into T which is constant is also continuous.

The following two propositions are true:

(1) $\mathrm{L}_{01}(0, 1, 0, 1) = \mathrm{id}_{[0,\,1]_{\mathrm{T}}}$.

(2) For all real numbers r_1, r_2, r_3, r_4, r_5, r_6 such that $r_1 < r_2$ and $r_3 \leq r_4$ and $r_5 < r_6$ holds $\mathrm{L}_{01}(r_1, r_2, r_3, r_4) \cdot \mathrm{L}_{01}(r_5, r_6, r_1, r_2) = \mathrm{L}_{01}(r_5, r_6, r_3, r_4)$.

Let n be a positive natural number. Observe that $\mathcal{E}^n_{\mathrm{T}}$ is infinite and every non empty topological space which is n-locally Euclidean is also infinite.

The following propositions are true:

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

ISSN 1426–2630(p), 1898-9934(e)

(3) For every point p of $\mathcal{E}^n_{\mathrm{T}}$ such that $p \in \mathrm{Sphere}((0_{\mathcal{E}^n_{\mathrm{T}}}), 1)$ holds $-p \in \mathrm{Sphere}((0_{\mathcal{E}^n_{\mathrm{T}}}), 1) \setminus \{p\}$.

(4) Let T be a non empty topological structure, t_1, t_2 be points of T, and p be a path from t_1 to t_2. Then $\inf \mathrm{dom}\, p = 0$ and $\sup \mathrm{dom}\, p = 1$.

(5) For all constant loops C_1, C_2 of t holds C_1, C_2 are homotopic.

(6) Let S be a non empty subspace of T, t_1, t_2 be points of T, s_1, s_2 be points of S, A, B be paths from t_1 to t_2, and C, D be paths from s_1 to s_2. Suppose s_1, s_2 are connected and t_1, t_2 are connected and $A = C$ and $B = D$ and C, D are homotopic. Then A, B are homotopic.

(7) Let S be a non empty subspace of T, t_1, t_2 be points of T, s_1, s_2 be points of S, A, B be paths from t_1 to t_2, and C, D be paths from s_1 to s_2. Suppose s_1, s_2 are connected and t_1, t_2 are connected and $A = C$ and $B = D$ and $[C]_{\mathrm{EqRel}(S,s_1,s_2)} = [D]_{\mathrm{EqRel}(S,s_1,s_2)}$. Then $[A]_{\mathrm{EqRel}(T,t_1,t_2)} = [B]_{\mathrm{EqRel}(T,t_1,t_2)}$.

(8) Let T be a trivial non empty topological space, t be a point of T, and L be a loop of t. Then the carrier of $\pi_1(T,t) = \{[L]_{\mathrm{EqRel}(T,t)}\}$.

(9) For every point p of $\mathcal{E}^n_{\mathrm{T}}$ and for every subset S of $\mathcal{E}^n_{\mathrm{T}}$ such that $n \geq 2$ and $S = \Omega_{\mathcal{E}^n_{\mathrm{T}}} \setminus \{p\}$ holds $\mathcal{E}^n_{\mathrm{T}} \restriction S$ is pathwise connected.

(10) Let S be a non empty subset of T. Suppose $n \geq 2$ and $S = \Omega_T \setminus \{t\}$ and $\mathcal{E}^n_{\mathrm{T}}$ and T are homeomorphic. Then $T \restriction S$ is pathwise connected.

Let n be an element of $\mathbb{N}$ and let p, q be points of $\mathcal{E}^n_{\mathrm{T}}$. Observe that $\mathrm{TPlane}(p, q)$ is convex.

2. Fundamental Groups

Let us consider T. We say that T has trivial fundamental group if and only if:

(Def. 1) For every point t of T holds $\pi_1(T,t)$ is trivial.

Let us consider T. We say that T is simply connected if and only if:

(Def. 2) T is pathwise connected and has trivial fundamental group.

One can verify that every non empty topological space which is simply connected is also pathwise connected and has trivial fundamental group and every non empty topological space which is pathwise connected and has trivial fundamental group is also simply connected.

The following proposition is true

(11) If T has trivial fundamental group, then for every point t of T and for all loops P, Q of t holds P, Q are homotopic.

Let n be a natural number. Note that $\mathcal{E}^n_{\mathrm{T}}$ has trivial fundamental group.

Let us note that every non empty topological space which is trivial also has trivial fundamental group.

The following proposition is true

(12) T is simply connected if and only if for all points t_1, t_2 of T holds t_1, t_2 are connected and for all paths P, Q from t_1 to t_2 holds $[P]_{\mathrm{EqRel}(T,t_1,t_2)} = [Q]_{\mathrm{EqRel}(T,t_1,t_2)}$.

Let T be a non empty topological space with trivial fundamental group and let t be a point of T. One can check that $\pi_1(T,t)$ is trivial.

Next we state three propositions:

(13) Let S, T be non empty topological spaces. Suppose S and T are homeomorphic. If S has trivial fundamental group, then T has trivial fundamental group.

(14) Let S, T be non empty topological spaces. Suppose S and T are homeomorphic. If S is simply connected, then T is simply connected.

(15) Let T be a non empty topological space with trivial fundamental group, t be a point of T, and P_1, P_2 be loops of t. Then P_1, P_2 are homotopic.

Let us consider T, t and let l be a loop of t. We say that l is null-homotopic if and only if:

(Def. 3) There exists a constant loop c of t such that l, c are homotopic.

Let us consider T, t. Observe that every loop of t which is constant is also null-homotopic.

Let us consider T, t. Note that there exists a loop of t which is constant.

The following proposition is true

(16) Let f be a loop of t and g be a continuous function from T into U. If f is null-homotopic, then $g \cdot f$ is null-homotopic.

Let T, U be non empty topological spaces, let t be a point of T, let f be a null-homotopic loop of t, and let g be a continuous function from T into U. Note that $g \cdot f$ is null-homotopic.

Let T be a non empty topological space with trivial fundamental group and let t be a point of T. Note that every loop of t is null-homotopic.

One can prove the following proposition

(17) If for every point t of T holds every loop of t is null-homotopic, then T has trivial fundamental group.

Let n be an element of $\mathbb{N}$ and let p, q be points of $\mathcal{E}^n_{\mathrm{T}}$. Note that $\mathrm{TPlane}(p,q)$ has trivial fundamental group.

We now state the proposition

(18) Let S be a non empty subspace of T, s be a point of S, f be a loop of t, and g be a loop of s. If $t = s$ and $f = g$ and g is null-homotopic, then f is null-homotopic.

3. Curves

In the sequel T is a topological structure and f is a partial function from $\mathbb{R}^{\mathbf{1}}$ to T.

Let us consider T, f. We say that f is parametrized curve if and only if the conditions (Def. 4) are satisfied.

(Def. 4)(i) $\operatorname{dom} f$ is an interval subset of $\mathbb{R}$, and

(ii) there exists a subspace S of $\mathbb{R}^{\mathbf{1}}$ and there exists a function g from S into T such that $f = g$ and $S = \mathbb{R}^{\mathbf{1}} \restriction \operatorname{dom} f$ and g is continuous.

Let us consider T. Observe that there exists a partial function from $\mathbb{R}^{\mathbf{1}}$ to T which is parametrized curve.

One can prove the following proposition

(19) $\emptyset$ is a parametrized curve partial function from $\mathbb{R}^{\mathbf{1}}$ to T.

Let us consider T. The functor T-Curves yields a subset of $\mathbb{R}\dot{\to}\Omega_T$ and is defined as follows:

(Def. 5) T-Curves $= \{f \in \mathbb{R}\dot{\to}\Omega_T : f$ is a parametrized curve partial function from $\mathbb{R}^{\mathbf{1}}$ to $T\}$.

Let us consider T. One can check that T-Curves is non empty.

Let us consider T. A curve of T is an element of T-Curves.

In the sequel c is a curve of T.

We now state several propositions:

(20) Every parametrized curve partial function from $\mathbb{R}^{\mathbf{1}}$ to T is a curve of T.

(21) $\emptyset$ is a curve of T.

(22) Let t_1, t_2 be points of T and p be a path from t_1 to t_2. If t_1, t_2 are connected, then p is a curve of T.

(23) c is a parametrized curve partial function from $\mathbb{R}^{\mathbf{1}}$ to T.

(24) $\operatorname{dom} c \subseteq \mathbb{R}$ and $\operatorname{rng} c \subseteq \Omega_T$.

Let us consider T, c. One can verify that $\operatorname{dom} c$ is real-membered.

Let us consider T, c. We say that c has first point if and only if:

(Def. 6) $\operatorname{dom} c$ is left-ended.

We say that c has last point if and only if:

(Def. 7) $\operatorname{dom} c$ is right-ended.

Let us consider T, c. We say that c has endpoints if and only if:

(Def. 8) c has first point and last point.

Let us consider T. One can check that every curve of T which has first point and last point also has endpoints and every curve of T which has endpoints also has first point and last point.

In the sequel T denotes a non empty topological structure.

Let us consider T. Note that there exists a curve of T which has endpoints.

Let us consider T and let c be a curve of T with first point. Note that $\operatorname{dom} c$ is non empty and $\inf \operatorname{dom} c$ is real.

Let us consider T and let c be a curve of T with last point. Note that $\operatorname{dom} c$ is non empty and $\sup \operatorname{dom} c$ is real.

Let us consider T. Observe that every curve of T which has first point is also non empty and every curve of T which has last point is also non empty.

Let us consider T and let c be a curve of T with first point. The first point of c yielding a point of T is defined by:

(Def. 9) The first point of $c = c(\inf \operatorname{dom} c)$.

Let us consider T and let c be a curve of T with last point. The last point of c yielding a point of T is defined by:

(Def. 10) The last point of $c = c(\sup \operatorname{dom} c)$.

The following propositions are true:

(25) Let t_1, t_2 be points of T and p be a path from t_1 to t_2. If t_1, t_2 are connected, then p is a curve of T with endpoints.

(26) For every curve c of T and for all real numbers r_1, r_2 holds $c{\restriction}[r_1, r_2]$ is a curve of T.

(27) For every curve c of T with endpoints holds $\operatorname{dom} c = [\inf \operatorname{dom} c, \sup \operatorname{dom} c]$.

(28) Let c be a curve of T with endpoints. Suppose $\operatorname{dom} c = [0, 1]$. Then c is a path from the first point of c to the last point of c.

(29) Let c be a curve of T with endpoints. Then $c \cdot \mathrm{L}_{01}(0, 1, \inf \operatorname{dom} c, \sup \operatorname{dom} c)$ is a path from the first point of c to the last point of c.

(30) Let c be a curve of T with endpoints and t_1, t_2 be points of T. Suppose $c \cdot \mathrm{L}_{01}(0, 1, \inf \operatorname{dom} c, \sup \operatorname{dom} c)$ is a path from t_1 to t_2 and t_1, t_2 are connected. Then $t_1 =$ the first point of c and $t_2 =$ the last point of c.

(31) For every curve c of T with endpoints holds the first point of $c \in \operatorname{rng} c$ and the last point of $c \in \operatorname{rng} c$.

(32) Let r_1, r_2 be real numbers, t_1, t_2 be points of T, and p_1 be a path from t_1 to t_2. Suppose t_1, t_2 are connected and $r_1 < r_2$. Then $p_1 \cdot \mathrm{L}_{01}(r_1, r_2, 0, 1)$ is a curve of T with endpoints.

(33) For every curve c of T with endpoints holds the first point of c, the last point of c are connected.

Let T be a non empty topological structure and let c_1, c_2 be curves of T with endpoints. We say that c_1, c_2 are homotopic if and only if the condition (Def. 11) is satisfied.

(Def. 11) There exist points a, b of T and there exist paths p_1, p_2 from a to b such that $p_1 = c_1 \cdot \mathrm{L}_{01}(0, 1, \inf \operatorname{dom} c_1, \sup \operatorname{dom} c_1)$ and $p_2 = c_2 \cdot \mathrm{L}_{01}(0, 1, \inf \operatorname{dom} c_2, \sup \operatorname{dom} c_2)$ and p_1, p_2 are homotopic.

Let us note that the predicate c_1, c_2 are homotopic is symmetric.

Let T be a non empty topological space and let c_1, c_2 be curves of T with endpoints. Let us notice that the predicate c_1, c_2 are homotopic is reflexive and symmetric.

The following three propositions are true:

(34) Let T be a non empty topological structure, c_1, c_2 be curves of T with endpoints, a, b be points of T, and p_1, p_2 be paths from a to b. Suppose $c_1 = p_1$ and $c_2 = p_2$ and a, b are connected. Then c_1, c_2 are homotopic if and only if p_1, p_2 are homotopic.

(35) Let c_1, c_2 be curves of T with endpoints. Suppose c_1, c_2 are homotopic. Then the first point of c_1 = the first point of c_2 and the last point of c_1 = the last point of c_2.

(36) Let T be a non empty topological space, c_1, c_2 be curves of T with endpoints, and S be a subset of $\mathbb{R}^{\mathbf{1}}$. Suppose $\operatorname{dom} c_1 = \operatorname{dom} c_2$ and $S = \operatorname{dom} c_1$. Then c_1, c_2 are homotopic if and only if there exists a function f from $(\mathbb{R}^{\mathbf{1}} \restriction S) \times \mathbb{I}$ into T and there exist points a, b of T such that f is continuous and for every point t of $\mathbb{R}^{\mathbf{1}} \restriction S$ holds $f(t, 0) = c_1(t)$ and $f(t, 1) = c_2(t)$ and for every point t of $\mathbb{I}$ holds $f(\inf S, t) = a$ and $f(\sup S, t) = b$.

Let T be a topological structure and let c_1, c_2 be curves of T. The functor $c_1 + c_2$ yielding a curve of T is defined as follows:

(Def. 12) $c_1 + c_2 = \begin{cases} c_1 \cup c_2, \text{ if } c_1 \cup c_2 \text{ is a curve of } T, \\ \emptyset, \text{ otherwise.} \end{cases}$

One can prove the following three propositions:

(37) Let c be a curve of T with endpoints and r be a real number. Then there exist elements c_1, c_2 of T-Curves such that $c = c_1 + c_2$ and $c_1 = c \restriction [\inf \operatorname{dom} c, r]$ and $c_2 = c \restriction [r, \sup \operatorname{dom} c]$.

(38) Let T be a non empty topological space and c_1, c_2 be curves of T with endpoints. Suppose $\sup \operatorname{dom} c_1 = \inf \operatorname{dom} c_2$ and the last point of c_1 = the first point of c_2. Then $c_1 + c_2$ has endpoints and $\operatorname{dom}(c_1 + c_2) = [\inf \operatorname{dom} c_1, \sup \operatorname{dom} c_2]$ and $(c_1 + c_2)(\inf \operatorname{dom} c_1)$ = the first point of c_1 and $(c_1 + c_2)(\sup \operatorname{dom} c_2)$ = the last point of c_2.

(39) Let T be a non empty topological space and c_1, c_2, c_3, c_4, c_5, c_6 be curves of T with endpoints. Suppose that c_1, c_2 are homotopic and $\operatorname{dom} c_1 = \operatorname{dom} c_2$ and c_3, c_4 are homotopic and $\operatorname{dom} c_3 = \operatorname{dom} c_4$ and $c_5 = c_1 + c_3$ and $c_6 = c_2 + c_4$ and the last point of c_1 = the first point of c_3 and $\sup \operatorname{dom} c_1 = \inf \operatorname{dom} c_3$. Then c_5, c_6 are homotopic.

Let T be a topological structure and let f be a finite sequence of elements of T-Curves. The functor $(\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}$ yielding a finite sequence of elements of T-Curves is defined as follows:

(Def. 13) $\operatorname{len} f = \operatorname{len}((\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}})$ and $f(1) = (\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}(1)$ and for every natural number i such that $1 \leq i < \operatorname{len} f$ holds $(\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}(i +$

$1) = ((\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa\in\mathbb{N}})_i + f_{i+1}$.

Let T be a topological structure and let f be a finite sequence of elements of T-Curves. The functor $\sum f$ yields a curve of T and is defined as follows:

(Def. 14) $\sum f = \begin{cases} (\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa\in\mathbb{N}}(\operatorname{len} f), \text{ if } \operatorname{len} f > 0, \\ \emptyset, \text{ otherwise.} \end{cases}$

Next we state several propositions:

(40) For every curve c of T holds $\sum\langle c\rangle = c$.

(41) For every curve c of T and for every finite sequence f of elements of T-Curves holds $\sum(f \frown \langle c\rangle) = \sum f + c$.

(42) Let X be a set and f be a finite sequence of elements of T-Curves. Suppose that for every natural number i such that $1 \leq i \leq \operatorname{len} f$ holds $\operatorname{rng}(f_i) \subseteq X$. Then $\operatorname{rng}\sum f \subseteq X$.

(43) Let T be a non empty topological space and f be a finite sequence of elements of T-Curves. Suppose that

(i) $\operatorname{len} f > 0$,

(ii) for every natural number i such that $1 \leq i < \operatorname{len} f$ holds $f_i(\sup\operatorname{dom}(f_i)) = f_{i+1}(\inf\operatorname{dom}(f_{i+1}))$ and $\sup\operatorname{dom}(f_i) = \inf\operatorname{dom}(f_{i+1})$, and

(iii) for every natural number i such that $1 \leq i \leq \operatorname{len} f$ holds f_i has endpoints.

Then there exists a curve c of T with endpoints such that $\sum f = c$ and $\operatorname{dom} c = [\inf\operatorname{dom}(f_1), \sup\operatorname{dom}(f_{\operatorname{len} f})]$ and the first point of $c = f_1(\inf\operatorname{dom}(f_1))$ and the last point of $c = f_{\operatorname{len} f}(\sup\operatorname{dom}(f_{\operatorname{len} f}))$.

(44) Let T be a non empty topological space, f_1, f_2 be finite sequences of elements of T-Curves, and c_1, c_2 be curves of T with endpoints. Suppose that $\operatorname{len} f_1 > 0$ and $\operatorname{len} f_1 = \operatorname{len} f_2$ and $\sum f_1 = c_1$ and $\sum f_2 = c_2$ and for every natural number i such that $1 \leq i < \operatorname{len} f_1$ holds $(f_1)_i(\sup\operatorname{dom}((f_1)_i)) = (f_1)_{i+1}(\inf\operatorname{dom}((f_1)_{i+1}))$ and $\sup\operatorname{dom}((f_1)_i) = \inf\operatorname{dom}((f_1)_{i+1})$ and for every natural number i such that $1 \leq i < \operatorname{len} f_2$ holds $(f_2)_i(\sup\operatorname{dom}((f_2)_i)) = (f_2)_{i+1}(\inf\operatorname{dom}((f_2)_{i+1}))$ and $\sup\operatorname{dom}((f_2)_i) = \inf\operatorname{dom}((f_2)_{i+1})$ and for every natural number i such that $1 \leq i \leq \operatorname{len} f_1$ there exist curves c_3, c_4 of T with endpoints such that $c_3 = (f_1)_i$ and $c_4 = (f_2)_i$ and c_3, c_4 are homotopic and $\operatorname{dom} c_3 = \operatorname{dom} c_4$. Then c_1, c_2 are homotopic.

(45) Let c be a curve of T with endpoints and h be a finite sequence of elements of $\mathbb{R}$. Suppose $\operatorname{len} h \geq 2$ and $h(1) = \inf\operatorname{dom} c$ and $h(\operatorname{len} h) = \sup\operatorname{dom} c$ and h is increasing. Then there exists a finite sequence f of elements of T-Curves such that $\operatorname{len} f = \operatorname{len} h - 1$ and $c = \sum f$ and for every natural number i such that $1 \leq i \leq \operatorname{len} f$ holds $f_i = c\restriction[h_i, h_{i+1}]$.

(46) If $n \geq 2$, then $\mathbb{S}^n$ has trivial fundamental group.

(47) Let n be a non empty natural number, r be a positive real number, and x be a point of $\mathcal{E}^n_{\mathrm{T}}$. If $n \geq 3$, then $\mathrm{Tcircle}(x, r)$ has trivial fundamental group.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[7] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[9] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[10] Agata Darmochwał and Yatsuka Nakamura. Metric spaces as topological spaces – fundamental concepts. *Formalized Mathematics*, 2(**4**):605–608, 1991.
[11] Adam Grabowski. Introduction to the homotopy theory. *Formalized Mathematics*, 6(**4**):449–454, 1997.
[12] Adam Grabowski and Artur Korniłowicz. Algebraic properties of homotopies. *Formalized Mathematics*, 12(**3**):251–260, 2004.
[13] Artur Korniłowicz. The fundamental group of convex subspaces of $\mathcal{E}^n_{\mathrm{T}}$. *Formalized Mathematics*, 12(**3**):295–299, 2004.
[14] Artur Korniłowicz. On the isomorphism of fundamental groups. *Formalized Mathematics*, 12(**3**):391–396, 2004.
[15] Artur Korniłowicz and Yasunari Shidama. Intersections of intervals and balls in $\mathcal{E}^n_{\mathrm{T}}$. *Formalized Mathematics*, 12(**3**):301–306, 2004.
[16] Artur Korniłowicz, Yasunari Shidama, and Adam Grabowski. The fundamental group. *Formalized Mathematics*, 12(**3**):261–268, 2004.
[17] John M. Lee. *Introduction to Topological Manifolds*. Springer-Verlag, New York Berlin Heidelberg, 2000.
[18] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[19] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.
[20] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.
[21] Marco Riccardi. The definition of topological manifolds. *Formalized Mathematics*, 19(**1**):41–44, 2011, doi: 10.2478/v10037-011-0007-4.
[22] Marco Riccardi. Planes and spheres as topological manifolds. Stereographic projection. *Formalized Mathematics*, 20(**1**):41–45, 2012, doi: 10.2478/v10037-012-0006-0.
[23] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[24] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[25] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received September 20, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 2, Pages 105–112, 2012
DOI: 10.2478/v10037-012-0014-0

VERSITA
versita.com/fm/

The Borsuk-Ulam Theorem

Artur Korniłowicz[1]
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

Marco Riccardi
Via del Pero 102
54038 Montignoso
Italy

Summary. The Borsuk-Ulam theorem about antipodals is proven, [18, pp. 32–33].

MML identifier: BORSUK_7, version: 7.12.02 4.176.1140

The notation and terminology used here have been introduced in the following papers: [33], [36], [15], [16], [2], [5], [28], [35], [13], [26], [20], [30], [4], [34], [6], [7], [8], [38], [27], [1], [3], [9], [29], [31], [19], [41], [42], [39], [11], [43], [37], [40], [25], [32], [14], [23], [24], [22], [12], [21], [17], and [10].

1. Preliminaries

For simplicity, we adopt the following rules: a, b, x, y, z, X, Y, Z denote sets, n denotes a natural number, i denotes an integer, r, r_1, r_2, r_3, s denote real numbers, c, c_1, c_2 denote complex numbers, and p denotes a point of $\mathcal{E}^n_{\mathrm{T}}$.

Let us observe that every element of $\mathbb{IQ}$ is irrational.

Next we state a number of propositions:

(1) If $0 \leq r$ and $0 \leq s$ and $r^{\mathbf{2}} = s^{\mathbf{2}}$, then $r = s$.

(2) If $\operatorname{frac} r \geq \operatorname{frac} s$, then $\operatorname{frac}(r - s) = \operatorname{frac} r - \operatorname{frac} s$.

(3) If $\operatorname{frac} r < \operatorname{frac} s$, then $\operatorname{frac}(r - s) = (\operatorname{frac} r - \operatorname{frac} s) + 1$.

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

ISSN 1426–2630(p), 1898-9934(e)

(4) There exists i such that $\operatorname{frac}(r-s) = (\operatorname{frac} r - \operatorname{frac} s) + i$ but $i = 0$ or $i = 1$.

(5) If $\sin r = 0$, then $r = 2 \cdot \pi \cdot \lfloor \frac{r}{2 \cdot \pi} \rfloor$ or $r = \pi + 2 \cdot \pi \cdot \lfloor \frac{r}{2 \cdot \pi} \rfloor$.

(6) If $\cos r = 0$, then $r = \frac{\pi}{2} + 2 \cdot \pi \cdot \lfloor \frac{r}{2 \cdot \pi} \rfloor$ or $r = \frac{3 \cdot \pi}{2} + 2 \cdot \pi \cdot \lfloor \frac{r}{2 \cdot \pi} \rfloor$.

(7) If $\sin r = 0$, then there exists i such that $r = \pi \cdot i$.

(8) If $\cos r = 0$, then there exists i such that $r = \frac{\pi}{2} + \pi \cdot i$.

(9) If $\sin r = \sin s$, then there exists i such that $r = s + 2 \cdot \pi \cdot i$ or $r = (\pi - s) + 2 \cdot \pi \cdot i$.

(10) If $\cos r = \cos s$, then there exists i such that $r = s + 2 \cdot \pi \cdot i$ or $r = -s + 2 \cdot \pi \cdot i$.

(11) If $\sin r = \sin s$ and $\cos r = \cos s$, then there exists i such that $r = s + 2 \cdot \pi \cdot i$.

(12) If $|c_1| = |c_2|$ and $\operatorname{Arg} c_1 = \operatorname{Arg} c_2 + 2 \cdot \pi \cdot i$, then $c_1 = c_2$.

Let f be a one-to-one complex-valued function and let us consider c. One can verify that $f + c$ is one-to-one.

Let f be a one-to-one complex-valued function and let us consider c. Note that $f - c$ is one-to-one.

One can prove the following propositions:

(13) For every complex-valued finite sequence f holds $\operatorname{len}(-f) = \operatorname{len} f$.

(14) $-\langle \underbrace{0, \ldots, 0}_{n} \rangle = \langle \underbrace{0, \ldots, 0}_{n} \rangle$.

(15) For every complex-valued function f such that $f \neq \langle \underbrace{0, \ldots, 0}_{n} \rangle$ holds $-f \neq \langle \underbrace{0, \ldots, 0}_{n} \rangle$.

(16) ${}^2\langle r_1, r_2, r_3 \rangle = \langle r_1{}^{\mathbf{2}}, r_2{}^{\mathbf{2}}, r_3{}^{\mathbf{2}} \rangle$.

(17) $\sum^2 \langle r_1, r_2, r_3 \rangle = r_1{}^{\mathbf{2}} + r_2{}^{\mathbf{2}} + r_3{}^{\mathbf{2}}$.

(18) For every complex-valued finite sequence f holds $(c \cdot f)^{\mathbf{2}} = c^{\mathbf{2}} \cdot f^{\mathbf{2}}$.

(19) For every complex-valued finite sequence f holds $(f/c)^{\mathbf{2}} = f^{\mathbf{2}}/c^{\mathbf{2}}$.

(20) For every real-valued finite sequence f such that $\sum f \neq 0$ holds $\sum(f/\sum f) = 1$.

Let a, b, c, x, y, z be sets. The functor $[a \mapsto x, b \mapsto y, c \mapsto z]$ is defined by:

(Def. 1) $[a \mapsto x, b \mapsto y, c \mapsto z] = [a \longmapsto x, b \longmapsto y] + \cdot (c \mathbin{\dot{\longmapsto}} z)$.

Let a, b, c, x, y, z be sets. One can check that $[a \mapsto x, b \mapsto y, c \mapsto z]$ is function-like and relation-like.

The following propositions are true:

(21) $\operatorname{dom}([a \mapsto x, b \mapsto y, c \mapsto z]) = \{a, b, c\}$.

(22) $\operatorname{rng}([a \mapsto x, b \mapsto y, c \mapsto z]) \subseteq \{x, y, z\}$.

(23) $[a \mapsto x, a \mapsto y, a \mapsto z] = a \mathbin{\dot{\longmapsto}} z$.

(24) $[a \mapsto x, a \mapsto y, b \mapsto z] = [a \longmapsto y, b \longmapsto z]$.

(25) If $a \neq b$, then $[a \mapsto x, b \mapsto y, a \mapsto z] = [a \longmapsto z, b \longmapsto y]$.

(26) $[a \mapsto x, b \mapsto y, b \mapsto z] = [a \longmapsto x, b \longmapsto z]$.

(27) If $a \neq b$ and $a \neq c$, then $([a \mapsto x, b \mapsto y, c \mapsto z])(a) = x$.

(28) If a, b, c are mutually different, then $([a \mapsto x, b \mapsto y, c \mapsto z])(a) = x$ and $([a \mapsto x, b \mapsto y, c \mapsto z])(b) = y$ and $([a \mapsto x, b \mapsto y, c \mapsto z])(c) = z$.

(29) For every function f such that $\operatorname{dom} f = \{a, b, c\}$ and $f(a) = x$ and $f(b) = y$ and $f(c) = z$ holds $f = [a \mapsto x, b \mapsto y, c \mapsto z]$.

(30) $\langle a, b, c\rangle = [1 \mapsto a, 2 \mapsto b, 3 \mapsto c]$.

(31) If a, b, c are mutually different, then $\prod([a \mapsto \{x\}, b \mapsto \{y\}, c \mapsto \{z\}]) = \{[a \mapsto x, b \mapsto y, c \mapsto z]\}$.

(32) For all sets A, B, C, D, E, F such that $A \subseteq B$ and $C \subseteq D$ and $E \subseteq F$ holds $\prod([a \mapsto A, b \mapsto C, c \mapsto E]) \subseteq \prod([a \mapsto B, b \mapsto D, c \mapsto F])$.

(33) If a, b, c are mutually different and $x \in X$ and $y \in Y$ and $z \in Z$, then $[a \mapsto x, b \mapsto y, c \mapsto z] \in \prod([a \mapsto X, b \mapsto Y, c \mapsto Z])$.

Let f be a function. We say that f is odd if and only if:

(Def. 2) For all complex-valued functions x, y such that x, $-x \in \operatorname{dom} f$ and $y = f(x)$ holds $f(-x) = -y$.

Let us mention that $\emptyset$ is odd.

Let us observe that there exists a function which is odd and complex-functions-valued.

The following propositions are true:

(34) For every point p of $\mathcal{E}^3_{\mathrm{T}}$ holds ${}^2p = \langle (p_{\mathbf{1}})^{\mathbf{2}}, (p_{\mathbf{2}})^{\mathbf{2}}, (p_{\mathbf{3}})^{\mathbf{2}}\rangle$.

(35) For every point p of $\mathcal{E}^3_{\mathrm{T}}$ holds $\sum {}^2p = (p_{\mathbf{1}})^{\mathbf{2}} + (p_{\mathbf{2}})^{\mathbf{2}} + (p_{\mathbf{3}})^{\mathbf{2}}$.

The following two propositions are true:

(36) For every subset S of $\mathbb{R}^{\mathbf{1}}$ such that $S = \mathbb{Q}$ holds $\mathbb{Q} \cap \,]-\infty, r[$ is an open subset of $\mathbb{R}^{\mathbf{1}} \restriction S$.

(37) For every subset S of $\mathbb{R}^{\mathbf{1}}$ such that $S = \mathbb{Q}$ holds $\mathbb{Q} \cap \,]r, +\infty[$ is an open subset of $\mathbb{R}^{\mathbf{1}} \restriction S$.

Let X be a connected non empty topological space, let Y be a non empty topological space, and let f be a continuous function from X into Y. Note that $\operatorname{Im} f$ is connected.

Next we state two propositions:

(38) Let S be a subset of $\mathbb{R}^{\mathbf{1}}$. Suppose $S = \mathbb{Q}$. Let T be a connected topological space and f be a function from T into $\mathbb{R}^{\mathbf{1}} \restriction S$. If f is continuous, then f is constant.

(39) Let a, b be real numbers, f be a continuous function from $[a, b]_{\mathrm{T}}$ into $\mathbb{R}^{\mathbf{1}}$, and g be a partial function from $\mathbb{R}$ to $\mathbb{R}$. If $a \leq b$ and $f = g$, then g is continuous.

Let s be a point of $\mathbb{R}^{\mathbf{1}}$ and let r be a real number. Then $s + r$ is a point of $\mathbb{R}^{\mathbf{1}}$.

Let s be a point of $\mathbb{R}^{\mathbf{1}}$ and let r be a real number. Then $s - r$ is a point of $\mathbb{R}^{\mathbf{1}}$.

Let X be a set, let f be a function from X into $\mathbb{R}^{\mathbf{1}}$, and let us consider r. Then $f + r$ is a function from X into $\mathbb{R}^{\mathbf{1}}$.

Let X be a set, let f be a function from X into $\mathbb{R}^{\mathbf{1}}$, and let us consider r. Then $f - r$ is a function from X into $\mathbb{R}^{\mathbf{1}}$.

Let s, t be points of $\mathbb{R}^{\mathbf{1}}$, let f be a path from s to t, and let r be a real number. Then $f + r$ is a path from $s + r$ to $t + r$. Then $f - r$ is a path from $s - r$ to $t - r$.

The point c[100] of TopUnitCircle 3 is defined by:

(Def. 3) $\mathrm{c}[100] = [1, 0, 0]$.

The point c[−100] of TopUnitCircle 3 is defined by:

(Def. 4) $\mathrm{c}[-100] = [-1, 0, 0]$.

Next we state several propositions:

(40) $-\mathrm{c}[100] = \mathrm{c}[-100]$.

(41) $-\mathrm{c}[-100] = \mathrm{c}[100]$.

(42) $\mathrm{c}[100] - \mathrm{c}[-100] = [2, 0, 0]$.

(43) For every point p of $\mathcal{E}^2_{\mathrm{T}}$ holds $p_{\mathbf{1}} = |p| \cdot \cos \operatorname{Arg} p$ and $p_{\mathbf{2}} = |p| \cdot \sin \operatorname{Arg} p$.

(44) For every point p of $\mathcal{E}^2_{\mathrm{T}}$ holds $p = \mathrm{cpx2euc}(|p| \cdot \cos \operatorname{Arg} p + |p| \cdot \sin \operatorname{Arg} p \cdot i)$.

(45) For all points p_1, p_2 of $\mathcal{E}^2_{\mathrm{T}}$ such that $|p_1| = |p_2|$ and $\operatorname{Arg} p_1 = \operatorname{Arg} p_2 + 2 \cdot \pi \cdot i$ holds $p_1 = p_2$.

One can prove the following propositions:

(46) For every point p of $\mathcal{E}^2_{\mathrm{T}}$ such that $p = \mathrm{CircleMap}(r)$ holds $\operatorname{Arg} p = 2 \cdot \pi \cdot \operatorname{frac} r$.

(47) Let p_1, p_2 be points of $\mathcal{E}^3_{\mathrm{T}}$ and u_1, u_2 be points of $\mathcal{E}^3$. If $u_1 = p_1$ and $u_2 = p_2$, then $\rho^3(u_1, u_2) = \sqrt{((p_1)_{\mathbf{1}} - (p_2)_{\mathbf{1}})^{\mathbf{2}} + ((p_1)_{\mathbf{2}} - (p_2)_{\mathbf{2}})^{\mathbf{2}} + ((p_1)_{\mathbf{3}} - (p_2)_{\mathbf{3}})^{\mathbf{2}}}$.

(48) Let p be a point of $\mathcal{E}^3_{\mathrm{T}}$ and e be a point of $\mathcal{E}^3$. If $p = e$ and $p_{\mathbf{3}} = 0$, then $\prod([1 \mapsto]p_{\mathbf{1}} - \frac{r}{\sqrt{2}}, p_{\mathbf{1}} + \frac{r}{\sqrt{2}}[, 2 \mapsto]p_{\mathbf{2}} - \frac{r}{\sqrt{2}}, p_{\mathbf{2}} + \frac{r}{\sqrt{2}}[, 3 \mapsto \{0\}]) \subseteq \operatorname{Ball}(e, r)$.

(49) For every real number s holds $c \circlearrowleft s = c \circlearrowleft s + 2 \cdot \pi \cdot i$.

(50) For every real number s holds $\operatorname{Rotate} s = \operatorname{Rotate}(s + 2 \cdot \pi \cdot i)$.

(51) For every real number s and for every point p of $\mathcal{E}^2_{\mathrm{T}}$ holds $|(\operatorname{Rotate} s)(p)| = |p|$.

(52) For every real number s and for every point p of $\mathcal{E}^2_{\mathrm{T}}$ holds $\operatorname{Arg}(\operatorname{Rotate} s)(p) = \operatorname{Arg}(\mathrm{euc2cpx}(p) \circlearrowleft s)$.

(53) For every real number s and for every point p of $\mathcal{E}^2_{\mathrm{T}}$ such that $p \neq 0_{\mathcal{E}^2_{\mathrm{T}}}$ there exists i such that $\operatorname{Arg}(\operatorname{Rotate} s)(p) = s + \operatorname{Arg} p + 2 \cdot \pi \cdot i$.

(54) For every real number s holds $(\operatorname{Rotate} s)(0_{\mathcal{E}^2_{\mathrm{T}}}) = 0_{\mathcal{E}^2_{\mathrm{T}}}$.

(55) For every real number s and for every point p of $\mathcal{E}^2_{\mathrm{T}}$ such that $(\mathrm{Rotate}\, s)(p) = 0_{\mathcal{E}^2_{\mathrm{T}}}$ holds $p = 0_{\mathcal{E}^2_{\mathrm{T}}}$.

(56) For every real number s and for every point p of $\mathcal{E}^2_{\mathrm{T}}$ holds $(\mathrm{Rotate}\, s)((\mathrm{Rotate}(-s))(p)) = p$.

(57) For every real number s holds $\mathrm{Rotate}\, s \cdot \mathrm{Rotate}(-s) = \mathrm{id}_{\mathcal{E}^2_{\mathrm{T}}}$.

(58) For every real number s and for every point p of $\mathcal{E}^2_{\mathrm{T}}$ holds $p \in \mathrm{Sphere}((0_{\mathcal{E}^2_{\mathrm{T}}}), r)$ iff $(\mathrm{Rotate}\, s)(p) \in \mathrm{Sphere}((0_{\mathcal{E}^2_{\mathrm{T}}}), r)$.

(59) For every non negative real number r and for every real number s holds $(\mathrm{Rotate}\, s)^\circ \mathrm{Sphere}((0_{\mathcal{E}^2_{\mathrm{T}}}), r) = \mathrm{Sphere}((0_{\mathcal{E}^2_{\mathrm{T}}}), r)$.

Let r be a non negative real number and let s be a real number. The functor $\mathrm{RotateCircle}(r, s)$ yields a function from $\mathrm{Tcircle}(0_{\mathcal{E}^2_{\mathrm{T}}}, r)$ into $\mathrm{Tcircle}(0_{\mathcal{E}^2_{\mathrm{T}}}, r)$ and is defined by:

(Def. 5) $\mathrm{RotateCircle}(r, s) = \mathrm{Rotate}\, s \restriction \mathrm{Tcircle}(0_{\mathcal{E}^2_{\mathrm{T}}}, r)$.

Let r be a non negative real number and let s be a real number. Note that $\mathrm{RotateCircle}(r, s)$ is homeomorphism.

One can prove the following proposition

(60) For every point p of $\mathcal{E}^2_{\mathrm{T}}$ such that $p = \mathrm{CircleMap}(r_2)$ holds $(\mathrm{RotateCircle}(1, (-\mathrm{Arg}\, p)))(\mathrm{CircleMap}(r_1)) = \mathrm{CircleMap}(r_1 - r_2)$.

2. On the Antipodals

Let n be a non empty natural number, let p be a point of $\mathcal{E}^n_{\mathrm{T}}$, and let r be a non negative real number. The functor $\mathrm{CircleIso}(p, r)$ yields a function from $\mathrm{TopUnitCircle}\, n$ into $\mathrm{Tcircle}(p, r)$ and is defined as follows:

(Def. 6) For every point a of $\mathrm{TopUnitCircle}\, n$ and for every point b of $\mathcal{E}^n_{\mathrm{T}}$ such that $a = b$ holds $(\mathrm{CircleIso}(p, r))(a) = r \cdot b + p$.

Let n be a non empty natural number, let p be a point of $\mathcal{E}^n_{\mathrm{T}}$, and let r be a positive real number. Note that $\mathrm{CircleIso}(p, r)$ is homeomorphism.

The function SphereMap from $\mathbb{R}^1$ into $\mathrm{TopUnitCircle}\, 3$ is defined by:

(Def. 7) For every real number x holds $(\mathrm{SphereMap})(x) = [\cos(2 \cdot \pi \cdot x), \sin(2 \cdot \pi \cdot x), 0]$.

We now state the proposition

(61) $(\mathrm{SphereMap})(i) = \mathrm{c}[100]$.

Let us note that SphereMap is continuous.

Let r be a real number. The functor $\mathrm{eLoop}\, r$ yields a function from $\mathbb{I}$ into $\mathrm{TopUnitCircle}\, 3$ and is defined as follows:

(Def. 8) For every point x of $\mathbb{I}$ holds $(\mathrm{eLoop}\, r)(x) = [\cos(2 \cdot \pi \cdot r \cdot x), \sin(2 \cdot \pi \cdot r \cdot x), 0]$.

We now state the proposition

(62) $\mathrm{eLoop}\, r = \mathrm{SphereMap} \cdot \mathrm{ExtendInt}\, r$.

Let us consider i. Then eLoop i is a loop of c[100].

One can check that eLoop i is null-homotopic as a loop of c[100].

One can prove the following proposition

(63) If $p \neq 0_{\mathcal{E}^n_{\mathrm{T}}}$, then $|p/|p|| = 1$.

Let n be a natural number and let p be a point of $\mathcal{E}^n_{\mathrm{T}}$. Let us assume that $p \neq 0_{\mathcal{E}^n_{\mathrm{T}}}$. The functor $(R^n \to S^1)\, p$ yields a point of Tcircle$(0_{\mathcal{E}^n_{\mathrm{T}}}, 1)$ and is defined by:

(Def. 9) $(R^n \to S^1)\, p = p/|p|$.

Let n be a non zero natural number and let f be a function from Tcircle$(0_{\mathcal{E}^{n+1}_{\mathrm{T}}}, 1)$ into $\mathcal{E}^n_{\mathrm{T}}$. The functor $(S^{n+1} \to S^n)\, f$ yielding a function from TopUnitCircle$(n+1)$ into TopUnitCircle n is defined as follows:

(Def. 10) For all points x, y of Tcircle$(0_{\mathcal{E}^{n+1}_{\mathrm{T}}}, 1)$ such that $y = -x$ holds $((S^{n+1} \to S^n)\, f)(x) = (R^n \to S^1)(f(x) - f(y))$.

Let x_0, y_0 be points of TopUnitCircle 2, let x_1 be a set, and let f be a path from x_0 to y_0. Let us assume that $x_1 \in \mathrm{CircleMap}^{-1}(\{x_0\})$. The functor liftPath$(f, x_1)$ yielding a function from $\mathbb{I}$ into $\mathbb{R}^{\mathbf{1}}$ is defined by the conditions (Def. 11).

(Def. 11)(i) $(\mathrm{liftPath}(f, x_1))(0) = x_1$,

(ii) $f = \mathrm{CircleMap} \cdot \mathrm{liftPath}(f, x_1)$,

(iii) liftPath(f, x_1) is continuous, and

(iv) for every function f_1 from $\mathbb{I}$ into $\mathbb{R}^{\mathbf{1}}$ such that f_1 is continuous and $f = \mathrm{CircleMap} \cdot f_1$ and $f_1(0) = x_1$ holds liftPath$(f, x_1) = f_1$.

Let n be a natural number, let p, x, y be points of $\mathcal{E}^n_{\mathrm{T}}$, and let r be a real number. We say that x and y are antipodals of p and r if and only if:

(Def. 12) x is a point of Tcircle(p, r) and y is a point of Tcircle(p, r) and $p \in \mathcal{L}(x, y)$.

Let n be a natural number, let p, x, y be points of $\mathcal{E}^n_{\mathrm{T}}$, let r be a real number, and let f be a function. We say that x and y are antipodals of p, r and f if and only if:

(Def. 13) x and y are antipodals of p and r and x, $y \in \mathrm{dom}\, f$ and $f(x) = f(y)$.

Let m, n be natural numbers, let p be a point of $\mathcal{E}^m_{\mathrm{T}}$, let r be a real number, and let f be a function from Tcircle(p, r) into $\mathcal{E}^n_{\mathrm{T}}$. We say that f has antipodals if and only if:

(Def. 14) There exist points x, y of $\mathcal{E}^m_{\mathrm{T}}$ such that x and y are antipodals of p, r and f.

Let m, n be natural numbers, let p be a point of $\mathcal{E}^m_{\mathrm{T}}$, let r be a real number, and let f be a function from Tcircle(p, r) into $\mathcal{E}^n_{\mathrm{T}}$. We introduce f is without antipodals as an antonym of f has antipodals.

One can prove the following propositions:

(64) Let n be a non empty natural number, r be a non negative real number, and x be a point of $\mathcal{E}^n_{\mathrm{T}}$. Suppose x is a point of $\mathrm{Tcircle}(0_{\mathcal{E}^n_{\mathrm{T}}}, r)$. Then x and $-x$ are antipodals of $0_{\mathcal{E}^n_{\mathrm{T}}}$ and r.

(65) Let n be a non empty natural number, p, x, y, x_2, y_1 be points of $\mathcal{E}^n_{\mathrm{T}}$, and r be a positive real number. Suppose x and y are antipodals of $0_{\mathcal{E}^n_{\mathrm{T}}}$ and 1 and $x_2 = (\mathrm{CircleIso}(p, r))(x)$ and $y_1 = (\mathrm{CircleIso}(p, r))(y)$. Then x_2 and y_1 are antipodals of p and r.

(66) Let f be a function from $\mathrm{Tcircle}(0_{\mathcal{E}^{n+1}_{\mathrm{T}}}, 1)$ into $\mathcal{E}^n_{\mathrm{T}}$ and x be a point of $\mathrm{Tcircle}(0_{\mathcal{E}^{n+1}_{\mathrm{T}}}, 1)$. If f is without antipodals, then $f(x) - f(-x) \neq 0_{\mathcal{E}^n_{\mathrm{T}}}$.

(67) For every function f from $\mathrm{Tcircle}(0_{\mathcal{E}^{n+1}_{\mathrm{T}}}, 1)$ into $\mathcal{E}^n_{\mathrm{T}}$ such that f is without antipodals holds $(S^{n+1} \to S^n)\, f$ is odd.

(68) Let f be a function from $\mathrm{Tcircle}(0_{\mathcal{E}^{n+1}_{\mathrm{T}}}, 1)$ into $\mathcal{E}^n_{\mathrm{T}}$ and g, B_1 be functions from $\mathrm{Tcircle}(0_{\mathcal{E}^{n+1}_{\mathrm{T}}}, 1)$ into $\mathcal{E}^n_{\mathrm{T}}$. If $g = f \circ -$ and $B_1 = f - g$ and f is without antipodals, then $(S^{n+1} \to S^n)\, f = B_1/(n\,\mathrm{NormF} \cdot B_1)$.

Let us consider n, let r be a negative real number, and let p be a point of $\mathcal{E}^{n+1}_{\mathrm{T}}$. Observe that every function from $\mathrm{Tcircle}(p, r)$ into $\mathcal{E}^n_{\mathrm{T}}$ is without antipodals.

Let r be a non negative real number and let p be a point of $\mathcal{E}^3_{\mathrm{T}}$. Note that every function from $\mathrm{Tcircle}(p, r)$ into $\mathcal{E}^2_{\mathrm{T}}$ which is continuous also has antipodals.[2]

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.
[3] Grzegorz Bancerek. 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. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 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 modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.
[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[11] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[12] Agata Darmochwał. Families of subsets, subspaces and mappings in topological spaces. *Formalized Mathematics*, 1(**2**):257–261, 1990.
[13] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[14] Agata Darmochwał and Yatsuka Nakamura. Metric spaces as topological spaces – fundamental concepts. *Formalized Mathematics*, 2(**4**):605–608, 1991.

[2] The Borsuk-Ulam Theorem

[15] Adam Grabowski. Introduction to the homotopy theory. *Formalized Mathematics*, 6(**4**):449–454, 1997.
[16] Adam Grabowski. On the subcontinua of a real line. *Formalized Mathematics*, 11(**3**):313–322, 2003.
[17] Jarosław Gryko. Injective spaces. *Formalized Mathematics*, 7(**1**):57–62, 1998.
[18] Allen Hatcher. *Algebraic Topology*. Cambridge University Press, 2002.
[19] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[20] Kanchun, Hiroshi Yamazaki, and Yatsuka Nakamura. Cross products and tripple vector products in 3-dimensional Euclidean space. *Formalized Mathematics*, 11(**4**):381–383, 2003.
[21] Artur Korniłowicz. Arithmetic operations on functions from sets into functional sets. *Formalized Mathematics*, 17(**1**):43–60, 2009, doi:10.2478/v10037-009-0005-y.
[22] Artur Korniłowicz. On the continuity of some functions. *Formalized Mathematics*, 18(**3**):175–183, 2010, doi: 10.2478/v10037-010-0020-z.
[23] Artur Korniłowicz and Yasunari Shidama. Intersections of intervals and balls in $\mathcal{E}^n_{\mathrm{T}}$. *Formalized Mathematics*, 12(**3**):301–306, 2004.
[24] Artur Korniłowicz and Yasunari Shidama. Some properties of circles on the plane. *Formalized Mathematics*, 13(**1**):117–124, 2005.
[25] Artur Korniłowicz, Yasunari Shidama, and Adam Grabowski. The fundamental group. *Formalized Mathematics*, 12(**3**):261–268, 2004.
[26] Akihiro Kubo and Yatsuka Nakamura. Angle and triangle in Euclidian topological space. *Formalized Mathematics*, 11(**3**):281–287, 2003.
[27] Adam Naumowicz and Grzegorz Bancerek. Homeomorphisms of Jordan curves. *Formalized Mathematics*, 13(**4**):477–480, 2005.
[28] Beata Padlewska. Connected spaces. *Formalized Mathematics*, 1(**1**):239–244, 1990.
[29] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[30] Konrad Raczkowski and Paweł Sadowski. Real function continuity. *Formalized Mathematics*, 1(**4**):787–791, 1990.
[31] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.
[32] Marco Riccardi and Artur Korniłowicz. Fundamental group of n-sphere for $n \geq 2$. *Formalized Mathematics*, 20(**2**):97–104, 2012, doi: 10.2478/v10037-012-0013-1.
[33] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.
[34] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[35] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[36] Andrzej Trybulec. A Borsuk theorem on homotopy types. *Formalized Mathematics*, 2(**4**):535–545, 1991.
[37] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[38] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[39] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[40] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[41] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[42] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[43] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

Received September 20, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 2, Pages 113–124, 2012
DOI: 10.2478/v10037-012-0015-z

VERSITA
versita.com/fm/

Higher-Order Partial Differentiation[1]

Noboru Endou
Nagano National College of Technology
Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we shall extend the formalization of [10] to discuss higher-order partial differentiation of real valued functions. The linearity of this operator is also proved (refer to [10], [12] and [13] for partial differentiation).

MML identifier: PDIFF_9, version: 7.12.02 4.181.1147

The terminology and notation used here have been introduced in the following articles: [3], [8], [2], [4], [5], [15], [21], [17], [16], [20], [1], [6], [10], [12], [13], [18], [11], [9], [23], [7], [19], [14], and [22].

1. Preliminaries

We use the following convention: m, n denote non empty elements of $\mathbb{N}$, i, j denote elements of $\mathbb{N}$, and Z denotes a set.

One can prove the following propositions:

(1) Let S, T be real normed spaces, f be a point of the real norm space of bounded linear operators from S into T, and r be a real number. Suppose $0 \leq r$ and for every point x of S such that $\|x\| \leq 1$ holds $\|f(x)\| \leq r \cdot \|x\|$. Then $\|f\| \leq r$.

(2) Let S be a real normed space and f be a partial function from S to $\mathbb{R}$. Then f is continuous on Z if and only if the following conditions are satisfied:

[1] This work was supported by JSPS KAKENHI 22300285 and 23500029.

ISSN 1426–2630(p), 1898-9934(e)

(i) $Z \subseteq \operatorname{dom} f$, and

(ii) for every sequence s_1 of S such that $\operatorname{rng} s_1 \subseteq Z$ and s_1 is convergent and $\lim s_1 \in Z$ holds $f_* s_1$ is convergent and $f_{\lim s_1} = \lim(f_* s_1)$.

(3) For every partial function f from $\mathcal{R}^i$ to $\mathbb{R}$ holds $\operatorname{dom}\langle f\rangle = \operatorname{dom} f$.

(4) For every partial function f from $\mathcal{R}^i$ to $\mathbb{R}$ such that $Z \subseteq \operatorname{dom} f$ holds $\operatorname{dom}(\langle f\rangle \restriction Z) = Z$.

(5) For every partial function f from $\mathcal{R}^i$ to $\mathbb{R}$ holds $\langle f \restriction Z\rangle = \langle f\rangle \restriction Z$.

(6) Let f be a partial function from $\mathcal{R}^i$ to $\mathbb{R}$ and x be an element of $\mathcal{R}^i$. If $x \in \operatorname{dom} f$, then $\langle f\rangle(x) = \langle f(x)\rangle$ and $\langle f\rangle_x = \langle f_x\rangle$.

(7) For all partial functions f, g from $\mathcal{R}^i$ to $\mathbb{R}$ holds $\langle f + g\rangle = \langle f\rangle + \langle g\rangle$ and $\langle f - g\rangle = \langle f\rangle - \langle g\rangle$.

(8) For every partial function f from $\mathcal{R}^i$ to $\mathbb{R}$ and for every real number r holds $\langle r \cdot f\rangle = r \cdot \langle f\rangle$.

(9) Let f be a partial function from $\mathcal{R}^i$ to $\mathbb{R}$ and g be a partial function from $\mathcal{R}^i$ to $\mathcal{R}^1$. If $\langle f\rangle = g$, then $|f| = |g|$.

(10) For every subset X of $\mathcal{R}^m$ and for every subset Y of $\langle \mathcal{E}^m, \|\cdot\|\rangle$ such that $X = Y$ holds X is open iff Y is open.

(11) For every element q of $\mathbb{R}$ such that $1 \leq i \leq j$ holds $|(\operatorname{reproj}(i, \langle \underbrace{0, \ldots, 0}_{j}\rangle))(q)| = |q|$.

(12) For every element x of $\mathcal{R}^j$ holds $x = (\operatorname{reproj}(i, x))((\operatorname{proj}(i, j))(x))$.

2. Continuity and Differentiability

The following two propositions are true:

(13) Let X be a subset of $\mathcal{R}^m$ and f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$. If f is differentiable on X, then X is open.

(14) Let X be a subset of $\mathcal{R}^m$ and f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$. Suppose X is open. Then f is differentiable on X if and only if the following conditions are satisfied:

(i) $X \subseteq \operatorname{dom} f$, and

(ii) for every element x of $\mathcal{R}^m$ such that $x \in X$ holds f is differentiable in x.

Let m, n be non empty elements of $\mathbb{N}$, let Z be a set, and let f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$. Let us assume that $Z \subseteq \operatorname{dom} f$. The functor $f'_{\restriction Z}$ yields a partial function from $\mathcal{R}^m$ to $(\mathcal{R}^n)^{\mathcal{R}^m}$ and is defined by:

(Def. 1) $\operatorname{dom}(f'_{\restriction Z}) = Z$ and for every element x of $\mathcal{R}^m$ such that $x \in Z$ holds $(f'_{\restriction Z})_x = f'(x)$.

We now state a number of propositions:

(15) Let X be a subset of $\mathcal{R}^m$ and f, g be partial functions from $\mathcal{R}^m$ to $\mathcal{R}^n$. Suppose f is differentiable on X and g is differentiable on X. Then $f+g$ is differentiable on X and for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $((f+g)'_{\restriction X})_x = f'(x) + g'(x)$.

(16) Let X be a subset of $\mathcal{R}^m$ and f, g be partial functions from $\mathcal{R}^m$ to $\mathcal{R}^n$. Suppose f is differentiable on X and g is differentiable on X. Then $f-g$ is differentiable on X and for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $((f-g)'_{\restriction X})_x = f'(x) - g'(x)$.

(17) Let X be a subset of $\mathcal{R}^m$, f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$, and r be a real number. Suppose f is differentiable on X. Then $r \cdot f$ is differentiable on X and for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $((r \cdot f)'_{\restriction X})_x = r \cdot f'(x)$.

(18) Let f be a point of the real norm space of bounded linear operators from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ into $\langle \mathcal{E}^j, \|\cdot\| \rangle$. Then there exists a point p of $\langle \mathcal{E}^j, \|\cdot\| \rangle$ such that

(i) $p = f(\langle 1 \rangle)$,

(ii) for every real number r and for every point x of $\langle \mathcal{E}^1, \|\cdot\| \rangle$ such that $x = \langle r \rangle$ holds $f(x) = r \cdot p$, and

(iii) for every point x of $\langle \mathcal{E}^1, \|\cdot\| \rangle$ holds $\|f(x)\| = \|p\| \cdot \|x\|$.

(19) Let f be a point of the real norm space of bounded linear operators from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ into $\langle \mathcal{E}^j, \|\cdot\| \rangle$. Then there exists a point p of $\langle \mathcal{E}^j, \|\cdot\| \rangle$ such that $p = f(\langle 1 \rangle)$ and $\|p\| = \|f\|$.

(20) Let f be a point of the real norm space of bounded linear operators from $\langle \mathcal{E}^1, \|\cdot\| \rangle$ into $\langle \mathcal{E}^j, \|\cdot\| \rangle$ and x be a point of $\langle \mathcal{E}^1, \|\cdot\| \rangle$. Then $\|f(x)\| = \|f\| \cdot \|x\|$.

(21) Let f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$, g be a partial function from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, X be a subset of $\mathcal{R}^m$, and Y be a subset of $\langle \mathcal{E}^m, \|\cdot\| \rangle$. Suppose $1 \leq i \leq m$ and X is open and $g = f$ and $X = Y$ and f is partially differentiable on X w.r.t. i. Let x be an element of $\mathcal{R}^m$ and y be a point of $\langle \mathcal{E}^m, \|\cdot\| \rangle$. If $x \in X$ and $x = y$, then $\operatorname{partdiff}(f, x, i) = (\operatorname{partdiff}(g, y, i))(\langle 1 \rangle)$.

(22) Let f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$, g be a partial function from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, X be a subset of $\mathcal{R}^m$, and Y be a subset of $\langle \mathcal{E}^m, \|\cdot\| \rangle$. Suppose $1 \leq i \leq m$ and X is open and $g = f$ and $X = Y$ and f is partially differentiable on X w.r.t. i. Let x_0, x_1 be elements of $\mathcal{R}^m$ and y_0, y_1 be points of $\langle \mathcal{E}^m, \|\cdot\| \rangle$. If $x_0 = y_0$ and $x_1 = y_1$ and x_0, $x_1 \in X$, then $|(f \restriction^i X)_{x_1} - (f \restriction^i X)_{x_0}| = \|(g \restriction^i Y)_{y_1} - (g \restriction^i Y)_{y_0}\|$.

(23) Let f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$, g be a partial function from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, X be a subset of $\mathcal{R}^m$, and Y be a subset of $\langle \mathcal{E}^m, \|\cdot\| \rangle$. Suppose $1 \leq i \leq m$ and X is open and $g = f$ and $X = Y$. Then the following statements are equivalent

(i) f is partially differentiable on X w.r.t. i and $f \restriction^i X$ is continuous on X,

(ii) g is partially differentiable on Y w.r.t. i and $g\restriction^i Y$ is continuous on Y.

(24) Let f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$, g be a partial function from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, X be a subset of $\mathcal{R}^m$, and Y be a subset of $\langle \mathcal{E}^m, \|\cdot\| \rangle$. Suppose $X = Y$ and X is open and $f = g$. Then for every i such that $1 \leq i \leq m$ holds f is partially differentiable on X w.r.t. i and $f\restriction^i X$ is continuous on X if and only if g is differentiable on Y and $g'_{\restriction Y}$ is continuous on Y.

(25) Let f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$, g be a partial function from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, X be a subset of $\mathcal{R}^m$, and Y be a subset of $\langle \mathcal{E}^m, \|\cdot\| \rangle$. Suppose X is open and $X \subseteq \operatorname{dom} f$ and $g = f$ and $X = Y$. Then g is differentiable on Y and $g'_{\restriction Y}$ is continuous on Y if and only if the following conditions are satisfied:

(i) f is differentiable on X, and

(ii) for every element x_0 of $\mathcal{R}^m$ and for every real number r such that $x_0 \in X$ and $0 < r$ there exists a real number s such that $0 < s$ and for every element x_1 of $\mathcal{R}^m$ such that $x_1 \in X$ and $|x_1 - x_0| < s$ and for every element v of $\mathcal{R}^m$ holds $|f'(x_1)(v) - f'(x_0)(v)| \leq r \cdot |v|$.

(26) Let X be a subset of $\mathcal{R}^m$ and f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$. Suppose X is open and $X \subseteq \operatorname{dom} f$. Then the following statements are equivalent

(i) for every element i of $\mathbb{N}$ such that $1 \leq i \leq m$ holds f is partially differentiable on X w.r.t. i and $f\restriction^i X$ is continuous on X,

(ii) f is differentiable on X and for every element x_0 of $\mathcal{R}^m$ and for every real number r such that $x_0 \in X$ and $0 < r$ there exists a real number s such that $0 < s$ and for every element x_1 of $\mathcal{R}^m$ such that $x_1 \in X$ and $|x_1 - x_0| < s$ and for every element v of $\mathcal{R}^m$ holds $|f'(x_1)(v) - f'(x_0)(v)| \leq r \cdot |v|$.

(27) Let f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$ and g be a partial function from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$. If $f = g$ and f is differentiable on Z, then $f'_{\restriction Z} = g'_{\restriction Z}$.

(28) Let f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$, g be a partial function from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ to $\langle \mathcal{E}^n, \|\cdot\| \rangle$, X be a subset of $\mathcal{R}^m$, and Y be a subset of $\langle \mathcal{E}^m, \|\cdot\| \rangle$. Suppose $X = Y$ and X is open and $f = g$. Then for every element i of $\mathbb{N}$ such that $1 \leq i \leq m$ holds f is partially differentiable on X w.r.t. i and $f\restriction^i X$ is continuous on X if and only if f is differentiable on X and $g'_{\restriction Y}$ is continuous on Y.

(29) Let f, g be partial functions from $\mathcal{R}^m$ to $\mathcal{R}^n$ and x be an element of $\mathcal{R}^m$. Suppose f is continuous in x and g is continuous in x. Then $f + g$ is continuous in x and $f - g$ is continuous in x.

(30) Let f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$, x be an element of $\mathcal{R}^m$, and r be a real number. If f is continuous in x, then $r \cdot f$ is continuous in x.

(31) Let f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$ and x be an element of $\mathcal{R}^m$. If f is continuous in x, then $-f$ is continuous in x.

(32) Let f be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^n$ and x be an element of $\mathcal{R}^m$. If f is continuous in x, then $|f|$ is continuous in x.

(33) Let Z be a set and f, g be partial functions from $\mathcal{R}^m$ to $\mathcal{R}^n$. Suppose f is continuous on Z and g is continuous on Z. Then $f+g$ is continuous on Z and $f-g$ is continuous on Z.

(34) Let r be a real number and f, g be partial functions from $\mathcal{R}^m$ to $\mathcal{R}^n$. If f is continuous on Z, then $r \cdot f$ is continuous on Z.

(35) For all partial functions f, g from $\mathcal{R}^m$ to $\mathcal{R}^n$ such that f is continuous on Z holds $-f$ is continuous on Z.

(36) Let f be a partial function from $\mathcal{R}^i$ to $\mathbb{R}$ and x_0 be an element of $\mathcal{R}^i$. Then f is continuous in x_0 if and only if the following conditions are satisfied:

(i) $x_0 \in \operatorname{dom} f$, and

(ii) for every real number r such that $0 < r$ there exists a real number s such that $0 < s$ and for every element x of $\mathcal{R}^i$ such that $x \in \operatorname{dom} f$ and $|x - x_0| < s$ holds $|f_x - f_{x_0}| < r$.

(37) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ and x_0 be an element of $\mathcal{R}^m$. Then f is continuous in x_0 if and only if $\langle f \rangle$ is continuous in x_0.

(38) Let f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$ and x_0 be an element of $\mathcal{R}^m$. Suppose f is continuous in x_0 and g is continuous in x_0. Then $f+g$ is continuous in x_0 and $f-g$ is continuous in x_0.

(39) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$, x_0 be an element of $\mathcal{R}^m$, and r be a real number. If f is continuous in x_0, then $r \cdot f$ is continuous in x_0.

(40) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ and x_0 be an element of $\mathcal{R}^m$. If f is continuous in x_0, then $|f|$ is continuous in x_0.

(41) Let f, g be partial functions from $\mathcal{R}^i$ to $\mathbb{R}$ and x be an element of $\mathcal{R}^i$. If f is continuous in x and g is continuous in x, then $f \cdot g$ is continuous in x.

Let m be a non empty element of $\mathbb{N}$, let Z be a set, and let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. We say that f is continuous on Z if and only if:

(Def. 2) For every element x_0 of $\mathcal{R}^m$ such that $x_0 \in Z$ holds $f \restriction Z$ is continuous in x_0.

We now state a number of propositions:

(42) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ and g be a partial function from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ to $\mathbb{R}$. Suppose $f = g$. Then $Z \subseteq \operatorname{dom} f$ and f is continuous on Z if and only if g is continuous on Z.

(43) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ and g be a partial function from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ to $\mathbb{R}$. Suppose $f = g$ and $Z \subseteq \operatorname{dom} f$. Then f is continuous on Z

if and only if for every sequence s of $\langle \mathcal{E}^m, \|\cdot\| \rangle$ such that $\operatorname{rng} s \subseteq Z$ and s is convergent and $\lim s \in Z$ holds $g_* s$ is convergent and $g_{\lim s} = \lim(g_* s)$.

(44) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ and g be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^1$. Suppose $\langle f \rangle = g$. Then $Z \subseteq \operatorname{dom} f$ and f is continuous on Z if and only if g is continuous on Z.

(45) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose $Z \subseteq \operatorname{dom} f$. Then f is continuous on Z if and only if for every element x_0 of $\mathcal{R}^m$ and for every real number r such that $x_0 \in Z$ and $0 < r$ there exists a real number s such that $0 < s$ and for every element x_1 of $\mathcal{R}^m$ such that $x_1 \in Z$ and $|x_1 - x_0| < s$ holds $|f_{x_1} - f_{x_0}| < r$.

(46) Let f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose f is continuous on Z and g is continuous on Z and $Z \subseteq \operatorname{dom} f$ and $Z \subseteq \operatorname{dom} g$. Then $f + g$ is continuous on Z and $f - g$ is continuous on Z.

(47) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ and r be a real number. If $Z \subseteq \operatorname{dom} f$ and f is continuous on Z, then $r \cdot f$ is continuous on Z.

(48) Let f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose f is continuous on Z and g is continuous on Z and $Z \subseteq \operatorname{dom} f$ and $Z \subseteq \operatorname{dom} g$. Then $f \cdot g$ is continuous on Z.

(49) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ and g be a partial function from $\langle \mathcal{E}^m, \|\cdot\| \rangle$ to $\mathbb{R}$. Suppose $f = g$. Then $Z \subseteq \operatorname{dom} f$ and f is continuous on Z if and only if g is continuous on Z.

(50) For all partial functions f, g from $\mathcal{R}^m$ to $\mathcal{R}^n$ such that f is continuous on Z holds $|f|$ is continuous on Z.

(51) Let f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$ and x be an element of $\mathcal{R}^m$. Suppose f is differentiable in x and g is differentiable in x. Then $f + g$ is differentiable in x and $(f+g)'(x) = f'(x) + g'(x)$ and $f - g$ is differentiable in x and $(f - g)'(x) = f'(x) - g'(x)$.

(52) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$, r be a real number, and x be an element of $\mathcal{R}^m$. Suppose f is differentiable in x. Then $r \cdot f$ is differentiable in x and $(r \cdot f)'(x) = r \cdot f'(x)$.

Let Z be a set, let m be a non empty element of $\mathbb{N}$, and let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. We say that f is differentiable on Z if and only if:

(Def. 3) For every element x of $\mathcal{R}^m$ such that $x \in Z$ holds $f \restriction Z$ is differentiable in x.

Next we state three propositions:

(53) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ and g be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^1$. Suppose $\langle f \rangle = g$. Then $Z \subseteq \operatorname{dom} f$ and f is differentiable on Z if and only if g is differentiable on Z.

(54) Let X be a subset of $\mathcal{R}^m$ and f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose $X \subseteq \operatorname{dom} f$ and X is open. Then f is differentiable on X if and

only if for every element x of $\mathcal{R}^m$ such that $x \in X$ holds f is differentiable in x.

(55) Let X be a subset of $\mathcal{R}^m$ and f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. If $X \subseteq \operatorname{dom} f$ and f is differentiable on X, then X is open.

Let m be a non empty element of $\mathbb{N}$, let Z be a set, and let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. Let us assume that $Z \subseteq \operatorname{dom} f$. The functor $f'_{\restriction Z}$ yields a partial function from $\mathcal{R}^m$ to $\mathbb{R}^{\mathcal{R}^m}$ and is defined by:

(Def. 4) $\operatorname{dom}(f'_{\restriction Z}) = Z$ and for every element x of $\mathcal{R}^m$ such that $x \in Z$ holds $(f'_{\restriction Z})_x = f'(x)$.

One can prove the following four propositions:

(56) Let X be a subset of $\mathcal{R}^m$, f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$, and g be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^1$. Suppose $\langle f \rangle = g$ and $X \subseteq \operatorname{dom} f$ and f is differentiable on X. Then g is differentiable on X and for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $(f'_{\restriction X})_x = \operatorname{proj}(1,1) \cdot (g'_{\restriction X})_x$.

(57) Let X be a subset of $\mathcal{R}^m$ and f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose $X \subseteq \operatorname{dom} f$ and $X \subseteq \operatorname{dom} g$ and f is differentiable on X and g is differentiable on X. Then $f + g$ is differentiable on X and for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $((f+g)'_{\restriction X})_x = (f'_{\restriction X})_x + (g'_{\restriction X})_x$.

(58) Let X be a subset of $\mathcal{R}^m$ and f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose $X \subseteq \operatorname{dom} f$ and $X \subseteq \operatorname{dom} g$ and f is differentiable on X and g is differentiable on X. Then $f - g$ is differentiable on X and for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $((f-g)'_{\restriction X})_x = (f'_{\restriction X})_x - (g'_{\restriction X})_x$.

(59) Let X be a subset of $\mathcal{R}^m$, f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$, and r be a real number. Suppose $X \subseteq \operatorname{dom} f$ and f is differentiable on X. Then $r \cdot f$ is differentiable on X and for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $((r \cdot f)'_{\restriction X})_x = r \cdot (f'_{\restriction X})_x$.

Let m be a non empty element of $\mathbb{N}$, let Z be a set, let i be an element of $\mathbb{N}$, and let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. We say that f is partially differentiable on Z w.r.t. i if and only if:

(Def. 5) $Z \subseteq \operatorname{dom} f$ and for every element x of $\mathcal{R}^m$ such that $x \in Z$ holds $f \restriction Z$ is partially differentiable in x w.r.t. i.

Let m be a non empty element of $\mathbb{N}$, let Z be a set, let i be an element of $\mathbb{N}$, and let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. Let us assume that f is partially differentiable on Z w.r.t. i. The functor $f \restriction^i Z$ yields a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ and is defined as follows:

(Def. 6) $\operatorname{dom}(f \restriction^i Z) = Z$ and for every element x of $\mathcal{R}^m$ such that $x \in Z$ holds $(f \restriction^i Z)_x = \operatorname{partdiff}(f, x, i)$.

Next we state several propositions:

(60) Let X be a subset of $\mathcal{R}^m$ and f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose X is open and $1 \leq i \leq m$. Then f is partially differentiable on X

w.r.t. i if and only if $X \subseteq \operatorname{dom} f$ and for every element x of $\mathcal{R}^m$ such that $x \in X$ holds f is partially differentiable in x w.r.t. i.

(61) Let X be a subset of $\mathcal{R}^m$, f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$, and g be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^1$. Suppose $\langle f \rangle = g$ and X is open and $1 \leq i \leq m$. Then f is partially differentiable on X w.r.t. i if and only if g is partially differentiable on X w.r.t. i.

(62) Let X be a subset of $\mathcal{R}^m$, f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$, and g be a partial function from $\mathcal{R}^m$ to $\mathcal{R}^1$. Suppose $\langle f \rangle = g$ and X is open and $1 \leq i \leq m$ and f is partially differentiable on X w.r.t. i. Then $f\restriction^i X$ is continuous on X if and only if $g\restriction^i X$ is continuous on X.

(63) Let X be a subset of $\mathcal{R}^m$ and f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose X is open and $X \subseteq \operatorname{dom} f$. Then the following statements are equivalent

(i) for every element i of $\mathbb{N}$ such that $1 \leq i \leq m$ holds f is partially differentiable on X w.r.t. i and $f\restriction^i X$ is continuous on X,

(ii) f is differentiable on X and for every element x_0 of $\mathcal{R}^m$ and for every real number r such that $x_0 \in X$ and $0 < r$ there exists a real number s such that $0 < s$ and for every element x_1 of $\mathcal{R}^m$ such that $x_1 \in X$ and $|x_1 - x_0| < s$ and for every element v of $\mathcal{R}^m$ holds $|f'(x_1)(v) - f'(x_0)(v)| \leq r \cdot |v|$.

(64) Let f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$ and x be an element of $\mathcal{R}^m$. Suppose f is partially differentiable in x w.r.t. i and g is partially differentiable in x w.r.t. i. Then $f \cdot g$ is partially differentiable in x w.r.t. i and $\operatorname{partdiff}(f \cdot g, x, i) = \operatorname{partdiff}(f, x, i) \cdot g(x) + f(x) \cdot \operatorname{partdiff}(g, x, i)$.

(65) Let X be a subset of $\mathcal{R}^m$ and f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose that

(i) X is open,

(ii) $1 \leq i$,

(iii) $i \leq m$,

(iv) f is partially differentiable on X w.r.t. i, and

(v) g is partially differentiable on X w.r.t. i.

Then

(vi) $f + g$ is partially differentiable on X w.r.t. i,

(vii) $(f + g)\restriction^i X = (f\restriction^i X) + (g\restriction^i X)$, and

(viii) for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $((f + g)\restriction^i X)_x = \operatorname{partdiff}(f, x, i) + \operatorname{partdiff}(g, x, i)$.

(66) Let X be a subset of $\mathcal{R}^m$ and f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose that

(i) X is open,

(ii) $1 \leq i$,

(iii) $i \leq m$,

(iv) f is partially differentiable on X w.r.t. i, and
(v) g is partially differentiable on X w.r.t. i.

Then

(vi) $f - g$ is partially differentiable on X w.r.t. i,
(vii) $(f - g)\restriction^i X = (f\restriction^i X) - (g\restriction^i X)$, and
(viii) for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $((f - g)\restriction^i X)_x = \operatorname{partdiff}(f, x, i) - \operatorname{partdiff}(g, x, i)$.

(67) Let X be a subset of $\mathcal{R}^m$, r be a real number, and f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose X is open and $1 \leq i \leq m$ and f is partially differentiable on X w.r.t. i. Then

(i) $r \cdot f$ is partially differentiable on X w.r.t. i,
(ii) $r \cdot f\restriction^i X = r \cdot (f\restriction^i X)$, and
(iii) for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $(r \cdot f\restriction^i X)_x = r \cdot \operatorname{partdiff}(f, x, i)$.

(68) Let X be a subset of $\mathcal{R}^m$ and f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose that

(i) X is open,
(ii) $1 \leq i$,
(iii) $i \leq m$,
(iv) f is partially differentiable on X w.r.t. i, and
(v) g is partially differentiable on X w.r.t. i.

Then

(vi) $f \cdot g$ is partially differentiable on X w.r.t. i,
(vii) $f \cdot g\restriction^i X = (f\restriction^i X) \cdot g + f \cdot (g\restriction^i X)$, and
(viii) for every element x of $\mathcal{R}^m$ such that $x \in X$ holds $(f \cdot g\restriction^i X)_x = \operatorname{partdiff}(f, x, i) \cdot g(x) + f(x) \cdot \operatorname{partdiff}(g, x, i)$.

3. Higher-Order Partial Differentiation

Let m be a non empty element of $\mathbb{N}$, let Z be a set, let I be a finite sequence of elements of $\mathbb{N}$, and let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. The functor $\operatorname{PartDiffSeq}(f, Z, I)$ yielding a sequence of partial functions from $\mathcal{R}^m$ into $\mathbb{R}$ is defined by:

(Def. 7) $(\operatorname{PartDiffSeq}(f, Z, I))(0) = f$ and for every natural number i holds $(\operatorname{PartDiffSeq}(f, Z, I))(i + 1) = (\operatorname{PartDiffSeq}(f, Z, I))(i)\restriction^{I_{i+1}} Z$.

Let m be a non empty element of $\mathbb{N}$, let Z be a set, let I be a finite sequence of elements of $\mathbb{N}$, and let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. We say that f is partially differentiable on Z w.r.t. I if and only if:

(Def. 8) For every element i of $\mathbb{N}$ such that $i \leq \operatorname{len} I - 1$ holds $(\operatorname{PartDiffSeq}(f, Z, I))(i)$ is partially differentiable on Z w.r.t. I_{i+1}.

Let m be a non empty element of $\mathbb{N}$, let Z be a set, let I be a finite sequence of elements of $\mathbb{N}$, and let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. The functor $f\restriction^I Z$ yielding a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ is defined by:

(Def. 9) $f\restriction^I Z = (\mathrm{PartDiffSeq}(f, Z, I))(\mathrm{len}\, I)$.

The following propositions are true:

(69) Let X be a subset of $\mathcal{R}^m$, I be a non empty finite sequence of elements of $\mathbb{N}$, and f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose that
- (i) X is open,
- (ii) $\mathrm{rng}\, I \subseteq \mathrm{Seg}\, m$,
- (iii) f is partially differentiable on X w.r.t. I, and
- (iv) g is partially differentiable on X w.r.t. I.

Let given i. Suppose $i \leq \mathrm{len}\, I - 1$. Then $(\mathrm{PartDiffSeq}(f + g, X, I))(i)$ is partially differentiable on X w.r.t. I_{i+1} and $(\mathrm{PartDiffSeq}(f+g, X, I))(i) = (\mathrm{PartDiffSeq}(f, X, I))(i) + (\mathrm{PartDiffSeq}(g, X, I))(i)$.

(70) Let X be a subset of $\mathcal{R}^m$, I be a non empty finite sequence of elements of $\mathbb{N}$, and f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose that
- (i) X is open,
- (ii) $\mathrm{rng}\, I \subseteq \mathrm{Seg}\, m$,
- (iii) f is partially differentiable on X w.r.t. I, and
- (iv) g is partially differentiable on X w.r.t. I.

Then $f + g$ is partially differentiable on X w.r.t. I and $(f + g)\restriction^I X = (f\restriction^I X) + (g\restriction^I X)$.

(71) Let X be a subset of $\mathcal{R}^m$, I be a non empty finite sequence of elements of $\mathbb{N}$, and f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose that
- (i) X is open,
- (ii) $\mathrm{rng}\, I \subseteq \mathrm{Seg}\, m$,
- (iii) f is partially differentiable on X w.r.t. I, and
- (iv) g is partially differentiable on X w.r.t. I.

Let given i. Suppose $i \leq \mathrm{len}\, I - 1$. Then $(\mathrm{PartDiffSeq}(f - g, X, I))(i)$ is partially differentiable on X w.r.t. I_{i+1} and $(\mathrm{PartDiffSeq}(f-g, X, I))(i) = (\mathrm{PartDiffSeq}(f, X, I))(i) - (\mathrm{PartDiffSeq}(g, X, I))(i)$.

(72) Let X be a subset of $\mathcal{R}^m$, I be a non empty finite sequence of elements of $\mathbb{N}$, and f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose that
- (i) X is open,
- (ii) $\mathrm{rng}\, I \subseteq \mathrm{Seg}\, m$,
- (iii) f is partially differentiable on X w.r.t. I, and
- (iv) g is partially differentiable on X w.r.t. I.

Then $f - g$ is partially differentiable on X w.r.t. I and $(f - g)\restriction^I X = (f\restriction^I X) - (g\restriction^I X)$.

(73) Let X be a subset of $\mathcal{R}^m$, r be a real number, I be a non empty finite sequence of elements of $\mathbb{N}$, and f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$.

Suppose X is open and $\operatorname{rng} I \subseteq \operatorname{Seg} m$ and f is partially differentiable on X w.r.t. I. Let given i. Suppose $i \leq \operatorname{len} I - 1$. Then $(\text{PartDiffSeq}(r \cdot f, X, I))(i)$ is partially differentiable on X w.r.t. I_{i+1} and $(\text{PartDiffSeq}(r \cdot f, X, I))(i) = r \cdot (\text{PartDiffSeq}(f, X, I))(i)$.

(74) Let X be a subset of $\mathcal{R}^m$, r be a real number, I be a non empty finite sequence of elements of $\mathbb{N}$, and f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose X is open and $\operatorname{rng} I \subseteq \operatorname{Seg} m$ and f is partially differentiable on X w.r.t. I. Then $r \cdot f$ is partially differentiable on X w.r.t. I and $r \cdot f\restriction^I X = r \cdot (f\restriction^I X)$.

Let m be a non empty element of $\mathbb{N}$, let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$, let k be an element of $\mathbb{N}$, and let Z be a set. We say that f is partial differentiable up to order k and Z if and only if the condition (Def. 10) is satisfied.

(Def. 10) Let I be a non empty finite sequence of elements of $\mathbb{N}$. If $\operatorname{len} I \leq k$ and $\operatorname{rng} I \subseteq \operatorname{Seg} m$, then f is partially differentiable on Z w.r.t. I.

The following proposition is true

(75) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ and I, G be non empty finite sequences of elements of $\mathbb{N}$. Then f is partially differentiable on Z w.r.t. $G \frown I$ if and only if f is partially differentiable on Z w.r.t. G and $f\restriction^G Z$ is partially differentiable on Z w.r.t. I.

One can prove the following propositions:

(76) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. Then f is partially differentiable on Z w.r.t. $\langle i \rangle$ if and only if f is partially differentiable on Z w.r.t. i.

(77) For every partial function f from $\mathcal{R}^m$ to $\mathbb{R}$ holds $f\restriction^{\langle i \rangle} Z = f\restriction^i Z$.

(78) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$ and I be a non empty finite sequence of elements of $\mathbb{N}$. Suppose f is partial differentiable up to order $i + j$ and Z and $\operatorname{rng} I \subseteq \operatorname{Seg} m$ and $\operatorname{len} I = j$. Then $f\restriction^I Z$ is partial differentiable up to order i and Z.

(79) Let f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose f is partial differentiable up to order i and Z and $j \leq i$. Then f is partial differentiable up to order j and Z.

(80) Let X be a subset of $\mathcal{R}^m$ and f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose that

(i) X is open,

(ii) f is partial differentiable up to order i and X, and

(iii) g is partial differentiable up to order i and X.

Then $f + g$ is partial differentiable up to order i and X and $f - g$ is partial differentiable up to order i and X.

(81) Let X be a subset of $\mathcal{R}^m$, f be a partial function from $\mathcal{R}^m$ to $\mathbb{R}$, and r be a real number. Suppose X is open and f is partial differentiable up to

order i and X. Then $r \cdot f$ is partial differentiable up to order i and X.

(82) Let X be a subset of $\mathcal{R}^m$. Suppose X is open. Let i be an element of $\mathbb{N}$ and f, g be partial functions from $\mathcal{R}^m$ to $\mathbb{R}$. Suppose f is partial differentiable up to order i and X and g is partial differentiable up to order i and X. Then $f \cdot g$ is partial differentiable up to order i and X.

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. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.
[4] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[7] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[8] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[9] Noboru Endou and Yasunari Shidama. Completeness of the real Euclidean space. *Formalized Mathematics*, 13(**4**):577–580, 2005.
[10] Noboru Endou, Yasunari Shidama, and Keiichi Miyajima. Partial differentiation on normed linear spaces $\mathcal{R}^n$. *Formalized Mathematics*, 15(**2**):65–72, 2007, doi:10.2478/v10037-007-0008-5.
[11] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[12] Takao Inoué, Noboru Endou, and Yasunari Shidama. Differentiation of vector-valued functions on n-dimensional real normed linear spaces. *Formalized Mathematics*, 18(**4**):207–212, 2010, doi: 10.2478/v10037-010-0025-7.
[13] Takao Inoué, Adam Naumowicz, Noboru Endou, and Yasunari Shidama. Partial differentiation of vector-valued functions on n-dimensional real normed linear spaces. *Formalized Mathematics*, 19(**1**):1–9, 2011, doi: 10.2478/v10037-011-0001-x.
[14] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[15] Keiichi Miyajima and Yasunari Shidama. Riemann integral of functions from $\mathbb{R}$ into $\mathcal{R}^n$. *Formalized Mathematics*, 17(**2**):179–185, 2009, doi: 10.2478/v10037-009-0021-y.
[16] Keiko Narita, Artur Kornilowicz, and Yasunari Shidama. More on the continuity of real functions. *Formalized Mathematics*, 19(**4**):233–239, 2011, doi: 10.2478/v10037-011-0032-3.
[17] Takaya Nishiyama, Keiji Ohkubo, and Yasunari Shidama. The continuous functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):269–275, 2004.
[18] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[19] Beata Perkowska. Functional sequence from a domain to a domain. *Formalized Mathematics*, 3(**1**):17–21, 1992.
[20] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[21] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.
[22] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[23] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received November 20, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 2, Pages 125–146, 2012
DOI: 10.2478/v10037-012-0016-y

VERSITA
versita.com/fm/

Formalization of the Data Encryption Standard[1]

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article we formalize DES (the Data Encryption Standard), that was the most widely used symmetric cryptosystem in the world. DES is a block cipher which was selected by the National Bureau of Standards as an official Federal Information Processing Standard for the United States in 1976 [15].

MML identifier: DESCIP_1, version: 7.12.02 4.181.1147

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

1. Preliminaries

Let n be a natural number and let f be an n-element finite sequence. Note that $\mathrm{Rev}(f)$ is n-element.

Let D be a non empty set, let n be a natural number, and let f be an element of D^n. Then $\mathrm{Rev}(f)$ is an element of D^n.

Let n be a natural number and let f be a finite sequence. We introduce Op-Left(f, n) as a synonym of $f{\restriction}n$. We introduce Op-Right(f, n) as a synonym of $f_{\lfloor n}$.

Let D be a non empty set, let n be a natural number, and let f be a finite sequence of elements of D. Then Op-Left(f, n) is a finite sequence of elements of D. Then Op-Right(f, n) is a finite sequence of elements of D.

[1] This work was supported by JSPS KAKENHI 21240001.

ISSN 1426–2630(p), 1898-9934(e)

Let D be a non empty set, let n be a natural number, and let s be an element of $D^{2 \cdot n}$. We introduce SP-Left s as a synonym of Op-Left(s, n). We introduce SP-Right s as a synonym of Op-Right(s, n).

Let D be a non empty set, let n be a natural number, and let s be an element of $D^{2 \cdot n}$. Then SP-Left s is an element of D^n.

One can prove the following propositions:

(1) For all non empty elements m, n of $\mathbb{N}$ and for every element s of D^n such that $m \leq n$ holds Op-Left(s, m) is an element of D^m.

(2) Let m, n, l be non empty elements of $\mathbb{N}$ and s be an element of D^n. If $m \leq n$ and $l = n - m$, then Op-Right(s, m) is an element of D^l.

Let D be a non empty set, let n be a non empty element of $\mathbb{N}$, and let s be an element of $D^{2 \cdot n}$. Then SP-Right s is an element of D^n.

Next we state the proposition

(3) For every non empty element n of $\mathbb{N}$ and for every element s of $D^{2 \cdot n}$ holds (SP-Left s) $\frown$ SP-Right $s = s$.

Let s be a finite sequence. The functor Op-LeftShift s yielding a finite sequence is defined by:

(Def. 1) Op-LeftShift $s = (s_{\downarrow 1}) \frown \langle s(1) \rangle$.

Next we state three propositions:

(4) For every finite sequence s such that $1 \leq \operatorname{len} s$ holds len Op-LeftShift $s = \operatorname{len} s$.

(5) If $1 \leq \operatorname{len} s$, then Op-LeftShift s is a finite sequence of elements of D and len Op-LeftShift $s = \operatorname{len} s$.

(6) For every non empty element n of $\mathbb{N}$ and for every element s of D^n holds Op-LeftShift s is an element of D^n.

Let s be a finite sequence. The functor Op-RightShift s yields a finite sequence and is defined by:

(Def. 2) Op-RightShift $s = (\langle s(\operatorname{len} s) \rangle \frown s) \restriction \operatorname{len} s$.

One can prove the following three propositions:

(7) For every finite sequence s holds len Op-RightShift $s = \operatorname{len} s$.

(8) If $1 \leq \operatorname{len} s$, then Op-RightShift s is a finite sequence of elements of D and len Op-RightShift $s = \operatorname{len} s$.

(9) For every non empty element n of $\mathbb{N}$ and for every element s of D^n holds Op-RightShift s is an element of D^n.

Let D be a non empty set, let s be a finite sequence of elements of D, and let n be an integer. Let us assume that $1 \leq \operatorname{len} s$. The functor Op-Shift$(s, n)$ yields a finite sequence of elements of D and is defined by:

(Def. 3) len Op-Shift$(s, n) = \operatorname{len} s$ and for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} s$ holds (Op-Shift(s, n))$(i) = s((((i - 1) + n) \bmod \operatorname{len} s) + 1)$.

The following propositions are true:

(10) For all integers n, m such that $1 \leq \operatorname{len} s$ holds Op-Shift(Op-Shift$(s, n), m) =$ Op-Shift$(s, n + m)$.

(11) If $1 \leq \operatorname{len} s$, then Op-Shift$(s, 0) = s$.

(12) If $1 \leq \operatorname{len} s$, then Op-Shift$(s, \operatorname{len} s) = s$.

(13) If $1 \leq \operatorname{len} s$, then Op-Shift$(s, -\operatorname{len} s) = s$.

(14) Let n be a non empty element of $\mathbb{N}$, m be an integer, and s be an element of D^n. Then Op-Shift(s, m) is an element of D^n.

(15) If $1 \leq \operatorname{len} s$, then Op-Shift$(s, -1) =$ Op-RightShift s.

(16) If $1 \leq \operatorname{len} s$, then Op-Shift$(s, 1) =$ Op-LeftShift s.

Let x, y be elements of $Boolean^{28}$. Then $x \frown y$ is an element of $Boolean^{56}$.

Let n be a non empty element of $\mathbb{N}$, let s be an element of $Boolean^n$, and let i be a natural number. Then $s(i)$ is an element of $Boolean$.

Let n be a non empty element of $\mathbb{N}$, let s be an element of $\mathbb{N}^n$, and let i be a natural number. Then $s(i)$ is an element of $\mathbb{N}$.

Let n be a natural number. Observe that every element of $Boolean^n$ is boolean-valued.

Let n be an element of $\mathbb{N}$ and let s, t be elements of $Boolean^n$. We introduce Op-XOR(s, t) as a synonym of $s \oplus t$.

Let n be a non empty element of $\mathbb{N}$ and let s, t be elements of $Boolean^n$. Then Op-XOR(s, t) is an element of $Boolean^n$ and it can be characterized by the condition:

(Def. 4) For every natural number i such that $i \in \operatorname{Seg} n$ holds (Op-XOR$(s, t))(i) = s(i) \oplus t(i)$.

Let us notice that the functor Op-XOR(s, t) is commutative.

Let n, k be non empty elements of $\mathbb{N}$, let R_1 be an element of $(Boolean^n)^k$, and let i be an element of $\operatorname{Seg} k$. Then $R_1(i)$ is an element of $Boolean^n$.

We now state the proposition

(17) For every non empty element n of $\mathbb{N}$ and for all elements s, t of $Boolean^n$ holds Op-XOR(Op-XOR$(s, t), t) = s$.

Let m be a non empty element of $\mathbb{N}$, let D be a non empty set, let L be a sequence of D^m, and let i be a natural number. Then $L(i)$ is an element of D^m.

Let f be a function from 64 into 16 and let i be a set. Then $f(i)$ is an element of 16.

Next we state the proposition

(18) For all natural numbers n, m such that $n + m \leq \operatorname{len} s$ holds $(s{\restriction}n) \frown (s_{\restriction n}{\restriction}m) = s{\restriction}(n + m)$.

The scheme *QuadChoiceRec* deals with non empty sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$, an element $\mathcal{E}$ of $\mathcal{A}$, an element $\mathcal{F}$ of $\mathcal{B}$, an element $\mathcal{G}$ of $\mathcal{C}$, an element $\mathcal{H}$ of $\mathcal{D}$, and a 9-ary predicate $\mathcal{P}$, and states that:

There exists a function f from $\mathbb{N}$ into $\mathcal{A}$ and there exists a function g from $\mathbb{N}$ into $\mathcal{B}$ and there exists a function h from $\mathbb{N}$ into $\mathcal{C}$ and there exists a function i from $\mathbb{N}$ into $\mathcal{D}$ such that $f(0) = \mathcal{E}$ and $g(0) = \mathcal{F}$ and $h(0) = \mathcal{G}$ and $i(0) = \mathcal{H}$ and for every element n of $\mathbb{N}$ holds $\mathcal{P}[n, f(n), g(n), h(n), i(n), f(n+1), g(n+1), h(n+1), i(n+1)]$

provided the following condition is satisfied:

- Let n be an element of $\mathbb{N}$, x be an element of $\mathcal{A}$, y be an element of $\mathcal{B}$, z be an element of $\mathcal{C}$, and w be an element of $\mathcal{D}$. Then there exists an element x_1 of $\mathcal{A}$ and there exists an element y_1 of $\mathcal{B}$ and there exists an element z_1 of $\mathcal{C}$ and there exists an element w_1 of $\mathcal{D}$ such that $\mathcal{P}[n, x, y, z, w, x_1, y_1, z_1, w_1]$.

Next we state a number of propositions:

(19) Let x be a set. Suppose $x \in \operatorname{Seg} 16$. Then $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$.

(20) Let x be a set. Suppose $x \in \operatorname{Seg} 32$. Then $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$ or $x = 17$ or $x = 18$ or $x = 19$ or $x = 20$ or $x = 21$ or $x = 22$ or $x = 23$ or $x = 24$ or $x = 25$ or $x = 26$ or $x = 27$ or $x = 28$ or $x = 29$ or $x = 30$ or $x = 31$ or $x = 32$.

(21) Let x be a set. Suppose $x \in \operatorname{Seg} 48$. Then $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$ or $x = 17$ or $x = 18$ or $x = 19$ or $x = 20$ or $x = 21$ or $x = 22$ or $x = 23$ or $x = 24$ or $x = 25$ or $x = 26$ or $x = 27$ or $x = 28$ or $x = 29$ or $x = 30$ or $x = 31$ or $x = 32$ or $x = 33$ or $x = 34$ or $x = 35$ or $x = 36$ or $x = 37$ or $x = 38$ or $x = 39$ or $x = 40$ or $x = 41$ or $x = 42$ or $x = 43$ or $x = 44$ or $x = 45$ or $x = 46$ or $x = 47$ or $x = 48$.

(22) Let x be a set. Suppose $x \in \operatorname{Seg} 56$. Then $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$ or $x = 17$ or $x = 18$ or $x = 19$ or $x = 20$ or $x = 21$ or $x = 22$ or $x = 23$ or $x = 24$ or $x = 25$ or $x = 26$ or $x = 27$ or $x = 28$ or $x = 29$ or $x = 30$ or $x = 31$ or $x = 32$ or $x = 33$ or $x = 34$ or $x = 35$ or $x = 36$ or $x = 37$ or $x = 38$ or $x = 39$ or $x = 40$ or $x = 41$ or $x = 42$ or $x = 43$ or $x = 44$ or $x = 45$ or $x = 46$ or $x = 47$ or $x = 48$ or $x = 49$ or $x = 50$ or $x = 51$ or $x = 52$ or $x = 53$ or $x = 54$ or $x = 55$ or $x = 56$.

(23) Let x be a set. Suppose $x \in \operatorname{Seg} 64$. Then $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$ or $x = 17$ or $x = 18$ or $x = 19$ or $x = 20$ or $x = 21$ or $x = 22$ or $x = 23$ or $x = 24$ or $x = 25$ or

$x = 26$ or $x = 27$ or $x = 28$ or $x = 29$ or $x = 30$ or $x = 31$ or $x = 32$ or $x = 33$ or $x = 34$ or $x = 35$ or $x = 36$ or $x = 37$ or $x = 38$ or $x = 39$ or $x = 40$ or $x = 41$ or $x = 42$ or $x = 43$ or $x = 44$ or $x = 45$ or $x = 46$ or $x = 47$ or $x = 48$ or $x = 49$ or $x = 50$ or $x = 51$ or $x = 52$ or $x = 53$ or $x = 54$ or $x = 55$ or $x = 56$ or $x = 57$ or $x = 58$ or $x = 59$ or $x = 60$ or $x = 61$ or $x = 62$ or $x = 63$ or $x = 64$.

(24) For every non empty natural number n holds $n = \{0\} \cup (\operatorname{Seg} n \setminus \{n\})$.

(25) For every non empty natural number n and for every set x such that $x \in n$ holds $x = 0$ or $x \in \operatorname{Seg} n$ and $x \neq n$.

(26) Let x be a set. Suppose $x \in 16$. Then $x = 0$ or $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$.

(27) Let x be a set. Suppose $x \in 64$. Then $x = 0$ or $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$ or $x = 17$ or $x = 18$ or $x = 19$ or $x = 20$ or $x = 21$ or $x = 22$ or $x = 23$ or $x = 24$ or $x = 25$ or $x = 26$ or $x = 27$ or $x = 28$ or $x = 29$ or $x = 30$ or $x = 31$ or $x = 32$ or $x = 33$ or $x = 34$ or $x = 35$ or $x = 36$ or $x = 37$ or $x = 38$ or $x = 39$ or $x = 40$ or $x = 41$ or $x = 42$ or $x = 43$ or $x = 44$ or $x = 45$ or $x = 46$ or $x = 47$ or $x = 48$ or $x = 49$ or $x = 50$ or $x = 51$ or $x = 52$ or $x = 53$ or $x = 54$ or $x = 55$ or $x = 56$ or $x = 57$ or $x = 58$ or $x = 59$ or $x = 60$ or $x = 61$ or $x = 62$ or $x = 63$.

(28) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 be elements of S. Then there exists a finite sequence s of elements of S such that s is 8-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$.

(29) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16} be elements of S. Then there exists a finite sequence s of elements of S such that
s is 16-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$ and $s(9) = x_9$ and $s(10) = x_{10}$ and $s(11) = x_{11}$ and $s(12) = x_{12}$ and $s(13) = x_{13}$ and $s(14) = x_{14}$ and $s(15) = x_{15}$ and $s(16) = x_{16}$.

(30) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32} be elements of S. Then there exists a finite sequence s of elements of S such that
s is 32-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$ and $s(9) = x_9$ and $s(10) = x_{10}$ and $s(11) = x_{11}$ and $s(12) = x_{12}$ and $s(13) = x_{13}$ and $s(14) = x_{14}$ and $s(15) = x_{15}$ and $s(16) = x_{16}$ and $s(17) = x_{17}$

and $s(18) = x_{18}$ and $s(19) = x_{19}$ and $s(20) = x_{20}$ and $s(21) = x_{21}$ and $s(22) = x_{22}$ and $s(23) = x_{23}$ and $s(24) = x_{24}$ and $s(25) = x_{25}$ and $s(26) = x_{26}$ and $s(27) = x_{27}$ and $s(28) = x_{28}$ and $s(29) = x_{29}$ and $s(30) = x_{30}$ and $s(31) = x_{31}$ and $s(32) = x_{32}$.

(31) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48} be elements of S. Then there exists a finite sequence s of elements of S such that

s is 48-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$ and $s(9) = x_9$ and $s(10) = x_{10}$ and $s(11) = x_{11}$ and $s(12) = x_{12}$ and $s(13) = x_{13}$ and $s(14) = x_{14}$ and $s(15) = x_{15}$ and $s(16) = x_{16}$ and $s(17) = x_{17}$ and $s(18) = x_{18}$ and $s(19) = x_{19}$ and $s(20) = x_{20}$ and $s(21) = x_{21}$ and $s(22) = x_{22}$ and $s(23) = x_{23}$ and $s(24) = x_{24}$ and $s(25) = x_{25}$ and $s(26) = x_{26}$ and $s(27) = x_{27}$ and $s(28) = x_{28}$ and $s(29) = x_{29}$ and $s(30) = x_{30}$ and $s(31) = x_{31}$ and $s(32) = x_{32}$ and $s(33) = x_{33}$ and $s(34) = x_{34}$ and $s(35) = x_{35}$ and $s(36) = x_{36}$ and $s(37) = x_{37}$ and $s(38) = x_{38}$ and $s(39) = x_{39}$ and $s(40) = x_{40}$ and $s(41) = x_{41}$ and $s(42) = x_{42}$ and $s(43) = x_{43}$ and $s(44) = x_{44}$ and $s(45) = x_{45}$ and $s(46) = x_{46}$ and $s(47) = x_{47}$ and $s(48) = x_{48}$.

(32) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48}, x_{49}, x_{50}, x_{51}, x_{52}, x_{53}, x_{54}, x_{55}, x_{56} be elements of S. Then there exists a finite sequence s of elements of S such that

s is 56-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$ and $s(9) = x_9$ and $s(10) = x_{10}$ and $s(11) = x_{11}$ and $s(12) = x_{12}$ and $s(13) = x_{13}$ and $s(14) = x_{14}$ and $s(15) = x_{15}$ and $s(16) = x_{16}$ and $s(17) = x_{17}$ and $s(18) = x_{18}$ and $s(19) = x_{19}$ and $s(20) = x_{20}$ and $s(21) = x_{21}$ and $s(22) = x_{22}$ and $s(23) = x_{23}$ and $s(24) = x_{24}$ and $s(25) = x_{25}$ and $s(26) = x_{26}$ and $s(27) = x_{27}$ and $s(28) = x_{28}$ and $s(29) = x_{29}$ and $s(30) = x_{30}$ and $s(31) = x_{31}$ and $s(32) = x_{32}$ and $s(33) = x_{33}$ and $s(34) = x_{34}$ and $s(35) = x_{35}$ and $s(36) = x_{36}$ and $s(37) = x_{37}$ and $s(38) = x_{38}$ and $s(39) = x_{39}$ and $s(40) = x_{40}$ and $s(41) = x_{41}$ and $s(42) = x_{42}$ and $s(43) = x_{43}$ and $s(44) = x_{44}$ and $s(45) = x_{45}$ and $s(46) = x_{46}$ and $s(47) = x_{47}$ and $s(48) = x_{48}$ and $s(49) = x_{49}$ and $s(50) = x_{50}$ and $s(51) = x_{51}$ and $s(52) = x_{52}$ and $s(53) = x_{53}$ and $s(54) = x_{54}$ and $s(55) = x_{55}$ and $s(56) = x_{56}$.

(33) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11},

x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48}, x_{49}, x_{50}, x_{51}, x_{52}, x_{53}, x_{54}, x_{55}, x_{56}, x_{57}, x_{58}, x_{59}, x_{60}, x_{61}, x_{62}, x_{63}, x_{64} be elements of S. Then there exists a finite sequence s of elements of S such that

s is 64-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$ and $s(9) = x_9$ and $s(10) = x_{10}$ and $s(11) = x_{11}$ and $s(12) = x_{12}$ and $s(13) = x_{13}$ and $s(14) = x_{14}$ and $s(15) = x_{15}$ and $s(16) = x_{16}$ and $s(17) = x_{17}$ and $s(18) = x_{18}$ and $s(19) = x_{19}$ and $s(20) = x_{20}$ and $s(21) = x_{21}$ and $s(22) = x_{22}$ and $s(23) = x_{23}$ and $s(24) = x_{24}$ and $s(25) = x_{25}$ and $s(26) = x_{26}$ and $s(27) = x_{27}$ and $s(28) = x_{28}$ and $s(29) = x_{29}$ and $s(30) = x_{30}$ and $s(31) = x_{31}$ and $s(32) = x_{32}$ and $s(33) = x_{33}$ and $s(34) = x_{34}$ and $s(35) = x_{35}$ and $s(36) = x_{36}$ and $s(37) = x_{37}$ and $s(38) = x_{38}$ and $s(39) = x_{39}$ and $s(40) = x_{40}$ and $s(41) = x_{41}$ and $s(42) = x_{42}$ and $s(43) = x_{43}$ and $s(44) = x_{44}$ and $s(45) = x_{45}$ and $s(46) = x_{46}$ and $s(47) = x_{47}$ and $s(48) = x_{48}$ and $s(49) = x_{49}$ and $s(50) = x_{50}$ and $s(51) = x_{51}$ and $s(52) = x_{52}$ and $s(53) = x_{53}$ and $s(54) = x_{54}$ and $s(55) = x_{55}$ and $s(56) = x_{56}$ and $s(57) = x_{57}$ and $s(58) = x_{58}$ and $s(59) = x_{59}$ and $s(60) = x_{60}$ and $s(61) = x_{61}$ and $s(62) = x_{62}$ and $s(63) = x_{63}$ and $s(64) = x_{64}$.

Let n be a non empty natural number and let i be an element of n. We introduce ntoSeg i as a synonym of succ i.

Let n be a non empty natural number and let i be an element of n. Then ntoSeg i is an element of Seg n.

Let n be a non empty natural number and let f be a function from n into Seg n. We say that f is NtoSeg if and only if:

(Def. 5) For every element i of n holds $f(i) =$ ntoSeg i.

Let n be a non empty natural number. One can check that there exists a function from n into Seg n which is NtoSeg.

Let n be a non empty natural number. Observe that every function from n into Seg n is bijective and NtoSeg.

We now state two propositions:

(34) Let n be a non empty natural number, f be an NtoSeg function from n into Seg n, and i be a natural number. If $i < n$, then $f(i) = i + 1$ and $i \in \operatorname{dom} f$.

(35) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48}, x_{49}, x_{50}, x_{51}, x_{52}, x_{53}, x_{54}, x_{55}, x_{56}, x_{57}, x_{58}, x_{59}, x_{60}, x_{61}, x_{62}, x_{63}, x_{64} be elements of S. Then there exists a function f

from 64 into S such that
$f(0) = x_1$ and $f(1) = x_2$ and $f(2) = x_3$ and $f(3) = x_4$ and $f(4) = x_5$ and $f(5) = x_6$ and $f(6) = x_7$ and $f(7) = x_8$ and $f(8) = x_9$ and $f(9) = x_{10}$ and $f(10) = x_{11}$ and $f(11) = x_{12}$ and $f(12) = x_{13}$ and $f(13) = x_{14}$ and $f(14) = x_{15}$ and $f(15) = x_{16}$ and $f(16) = x_{17}$ and $f(17) = x_{18}$ and $f(18) = x_{19}$ and $f(19) = x_{20}$ and $f(20) = x_{21}$ and $f(21) = x_{22}$ and $f(22) = x_{23}$ and $f(23) = x_{24}$ and $f(24) = x_{25}$ and $f(25) = x_{26}$ and $f(26) = x_{27}$ and $f(27) = x_{28}$ and $f(28) = x_{29}$ and $f(29) = x_{30}$ and $f(30) = x_{31}$ and $f(31) = x_{32}$ and $f(32) = x_{33}$ and $f(33) = x_{34}$ and $f(34) = x_{35}$ and $f(35) = x_{36}$ and $f(36) = x_{37}$ and $f(37) = x_{38}$ and $f(38) = x_{39}$ and $f(39) = x_{40}$ and $f(40) = x_{41}$ and $f(41) = x_{42}$ and $f(42) = x_{43}$ and $f(43) = x_{44}$ and $f(44) = x_{45}$ and $f(45) = x_{46}$ and $f(46) = x_{47}$ and $f(47) = x_{48}$ and $f(48) = x_{49}$ and $f(49) = x_{50}$ and $f(50) = x_{51}$ and $f(51) = x_{52}$ and $f(52) = x_{53}$ and $f(53) = x_{54}$ and $f(54) = x_{55}$ and $f(55) = x_{56}$ and $f(56) = x_{57}$ and $f(57) = x_{58}$ and $f(58) = x_{59}$ and $f(59) = x_{60}$ and $f(60) = x_{61}$ and $f(61) = x_{62}$ and $f(62) = x_{63}$ and $f(63) = x_{64}$.

2. S-Boxes

The function DES-SBOX1 from 64 into 16 is defined by the conditions (Def. 6).

(Def. 6) (DES-SBOX1)(0) = 14 and (DES-SBOX1)(1) = 4 and (DES-SBOX1)(2) = 13 and (DES-SBOX1)(3) = 1 and (DES-SBOX1)(4) = 2 and (DES-SBOX1)(5) = 15 and (DES-SBOX1)(6) = 11 and (DES-SBOX1)(7) = 8 and (DES-SBOX1)(8) = 3 and (DES-SBOX1)(9) = 10 and (DES-SBOX1)(10) = 6 and (DES-SBOX1)(11) = 12 and (DES-SBOX1)(12) = 5 and (DES-SBOX1)(13) = 9 and (DES-SBOX1)(14) = 0 and (DES-SBOX1)(15) = 7 and (DES-SBOX1)(16) = 0 and (DES-SBOX1)(17) = 15 and (DES-SBOX1)(18) = 7 and (DES-SBOX1)(19) = 4 and (DES-SBOX1)(20) = 14 and (DES-SBOX1)(21) = 2 and (DES-SBOX1)(22) = 13 and (DES-SBOX1)(23) = 1 and (DES-SBOX1)(24) = 10 and (DES-SBOX1)(25) = 6 and (DES-SBOX1)(26) = 12 and (DES-SBOX1)(27) = 11 and (DES-SBOX1)(28) = 9 and (DES-SBOX1)(29) = 5 and (DES-SBOX1)(30) = 3 and (DES-SBOX1)(31) = 8 and (DES-SBOX1)(32) = 4 and (DES-SBOX1)(33) = 1 and (DES-SBOX1)(34) = 14 and (DES-SBOX1)(35) = 8 and (DES-SBOX1)(36) = 13 and (DES-SBOX1)(37) = 6 and (DES-SBOX1)(38) = 2 and (DES-SBOX1)(39) = 11 and (DES-SBOX1)(40) = 15 and (DES-SBOX1)(41) = 12 and (DES-SBOX1)(42) = 9 and (DES-SBOX1)(43) = 7 and

(DES-SBOX1)(44) = 3 and (DES-SBOX1)(45) = 10 and (DES-SBOX1)(46) = 5 and (DES-SBOX1)(47) = 0 and (DES-SBOX1)(48) = 15 and (DES-SBOX1)(49) = 12 and (DES-SBOX1)(50) = 8 and (DES-SBOX1)(51) = 2 and (DES-SBOX1)(52) = 4 and (DES-SBOX1)(53) = 9 and (DES-SBOX1)(54) = 1 and (DES-SBOX1)(55) = 7 and (DES-SBOX1)(56) = 5 and (DES-SBOX1)(57) = 11 and (DES-SBOX1)(58) = 3 and (DES-SBOX1)(59) = 14 and (DES-SBOX1)(60) = 10 and (DES-SBOX1)(61) = 0 and (DES-SBOX1)(62) = 6 and (DES-SBOX1)(63) = 13.

The function DES-SBOX2 from 64 into 16 is defined by the conditions (Def. 7).

(Def. 7) (DES-SBOX2)(0) = 15 and (DES-SBOX2)(1) = 1 and (DES-SBOX2)(2) = 8 and (DES-SBOX2)(3) = 14 and (DES-SBOX2)(4) = 6 and (DES-SBOX2)(5) = 11 and (DES-SBOX2)(6) = 3 and (DES-SBOX2)(7) = 4 and (DES-SBOX2)(8) = 9 and (DES-SBOX2)(9) = 7 and (DES-SBOX2)(10) = 2 and (DES-SBOX2)(11) = 13 and (DES-SBOX2)(12) = 12 and (DES-SBOX2)(13) = 0 and (DES-SBOX2)(14) = 5 and (DES-SBOX2)(15) = 10 and (DES-SBOX2)(16) = 3 and (DES-SBOX2)(17) = 13 and (DES-SBOX2)(18) = 4 and (DES-SBOX2)(19) = 7 and (DES-SBOX2)(20) = 15 and (DES-SBOX2)(21) = 2 and (DES-SBOX2)(22) = 8 and (DES-SBOX2)(23) = 14 and (DES-SBOX2)(24) = 12 and (DES-SBOX2)(25) = 0 and (DES-SBOX2)(26) = 1 and (DES-SBOX2)(27) = 10 and (DES-SBOX2)(28) = 6 and (DES-SBOX2)(29) = 9 and (DES-SBOX2)(30) = 11 and (DES-SBOX2)(31) = 5 and (DES-SBOX2)(32) = 0 and (DES-SBOX2)(33) = 14 and (DES-SBOX2)(34) = 7 and (DES-SBOX2)(35) = 11 and (DES-SBOX2)(36) = 10 and (DES-SBOX2)(37) = 4 and (DES-SBOX2)(38) = 13 and (DES-SBOX2)(39) = 1 and (DES-SBOX2)(40) = 5 and (DES-SBOX2)(41) = 8 and (DES-SBOX2)(42) = 12 and (DES-SBOX2)(43) = 6 and (DES-SBOX2)(44) = 9 and (DES-SBOX2)(45) = 3 and (DES-SBOX2)(46) = 2 and (DES-SBOX2)(47) = 15 and (DES-SBOX2)(48) = 13 and (DES-SBOX2)(49) = 8 and (DES-SBOX2)(50) = 10 and (DES-SBOX2)(51) = 1 and (DES-SBOX2)(52) = 3 and (DES-SBOX2)(53) = 15 and (DES-SBOX2)(54) = 4 and (DES-SBOX2)(55) = 2 and (DES-SBOX2)(56) = 11 and (DES-SBOX2)(57) = 6 and (DES-SBOX2)(58) = 7 and (DES-SBOX2)(59) = 12 and (DES-SBOX2)(60) = 0 and (DES-SBOX2)(61) = 5 and (DES-SBOX2)(62) = 14 and (DES-SBOX2)(63) = 9.

The function DES-SBOX3 from 64 into 16 is defined by the conditions (Def. 8).

(Def. 8) (DES-SBOX3)(0) = 10 and (DES-SBOX3)(1) = 0 and (DES-SBOX3)(2) = 9 and (DES-SBOX3)(3) = 14 and (DES-SBOX3)(4) = 6 and (DES-SBOX3)(5) = 3 and (DES-SBOX3)(6) = 15 and (DES-SBOX3)(7) = 5 and (DES-SBOX3)(8) = 1 and (DES-SBOX3)(9) = 13 and (DES-SBOX3)(10) = 12 and (DES-SBOX3)(11) = 7 and (DES-SBOX3)(12) = 11 and (DES-SBOX3)(13) = 4 and (DES-SBOX3)(14) = 2 and (DES-SBOX3)(15) = 8 and (DES-SBOX3)(16) = 13 and (DES-SBOX3)(17) = 7 and (DES-SBOX3)(18) = 0 and (DES-SBOX3)(19) = 9 and (DES-SBOX3)(20) = 3 and (DES-SBOX3)(21) = 4 and (DES-SBOX3)(22) = 6 and (DES-SBOX3)(23) = 10 and (DES-SBOX3)(24) = 2 and (DES-SBOX3)(25) = 8 and (DES-SBOX3)(26) = 5 and (DES-SBOX3)(27) = 14 and (DES-SBOX3)(28) = 12 and (DES-SBOX3)(29) = 11 and (DES-SBOX3)(30) = 15 and (DES-SBOX3)(31) = 1 and (DES-SBOX3)(32) = 13 and (DES-SBOX3)(33) = 6 and (DES-SBOX3)(34) = 4 and (DES-SBOX3)(35) = 9 and (DES-SBOX3)(36) = 8 and (DES-SBOX3)(37) = 15 and (DES-SBOX3)(38) = 3 and (DES-SBOX3)(39) = 0 and (DES-SBOX3)(40) = 11 and (DES-SBOX3)(41) = 1 and (DES-SBOX3)(42) = 2 and (DES-SBOX3)(43) = 12 and (DES-SBOX3)(44) = 5 and (DES-SBOX3)(45) = 10 and (DES-SBOX3)(46) = 14 and (DES-SBOX3)(47) = 7 and (DES-SBOX3)(48) = 1 and (DES-SBOX3)(49) = 10 and (DES-SBOX3)(50) = 13 and (DES-SBOX3)(51) = 0 and (DES-SBOX3)(52) = 6 and (DES-SBOX3)(53) = 9 and (DES-SBOX3)(54) = 8 and (DES-SBOX3)(55) = 7 and (DES-SBOX3)(56) = 4 and (DES-SBOX3)(57) = 15 and (DES-SBOX3)(58) = 14 and (DES-SBOX3)(59) = 3 and (DES-SBOX3)(60) = 11 and (DES-SBOX3)(61) = 5 and (DES-SBOX3)(62) = 2 and (DES-SBOX3)(63) = 12.

The function DES-SBOX4 from 64 into 16 is defined by the conditions (Def. 9).

(Def. 9) (DES-SBOX4)(0) = 7 and (DES-SBOX4)(1) = 13 and (DES-SBOX4)(2) = 14 and (DES-SBOX4)(3) = 3 and (DES-SBOX4)(4) = 0 and (DES-SBOX4)(5) = 6 and (DES-SBOX4)(6) = 9 and (DES-SBOX4)(7) = 10 and (DES-SBOX4)(8) = 1 and (DES-SBOX4)(9) = 2 and (DES-SBOX4)(10) = 8 and (DES-SBOX4)(11) = 5 and (DES-SBOX4)(12) = 11 and (DES-SBOX4)(13) = 12 and (DES-SBOX4)(14) = 4 and (DES-SBOX4)(15) = 15 and (DES-SBOX4)(16) = 13 and (DES-SBOX4)(17) = 8 and (DES-SBOX4)(18) = 11 and (DES-SBOX4)(19) = 5 and (DES-SBOX4)(20) = 6 and (DES-SBOX4)(21) = 15 and (DES-SBOX4)(22) = 0 and (DES-SBOX4)(23) = 3 and (DES-SBOX4)(24) = 4 and (DES-SBOX4)(25) = 7

and (DES-SBOX4)(26) = 2 and (DES-SBOX4)(27) = 12 and (DES-SBOX4)(28) = 1 and (DES-SBOX4)(29) = 10 and (DES-SBOX4)(30) = 14 and (DES-SBOX4)(31) = 9 and (DES-SBOX4)(32) = 10 and (DES-SBOX4)(33) = 6 and (DES-SBOX4)(34) = 9 and (DES-SBOX4)(35) = 0 and (DES-SBOX4)(36) = 12 and (DES-SBOX4)(37) = 11 and (DES-SBOX4)(38) = 7 and (DES-SBOX4)(39) = 13 and (DES-SBOX4)(40) = 15 and (DES-SBOX4)(41) = 1 and (DES-SBOX4)(42) = 3 and (DES-SBOX4)(43) = 14 and (DES-SBOX4)(44) = 5 and (DES-SBOX4)(45) = 2 and (DES-SBOX4)(46) = 8 and (DES-SBOX4)(47) = 4 and (DES-SBOX4)(48) = 3 and (DES-SBOX4)(49) = 15 and (DES-SBOX4)(50) = 0 and (DES-SBOX4)(51) = 6 and (DES-SBOX4)(52) = 10 and (DES-SBOX4)(53) = 1 and (DES-SBOX4)(54) = 13 and (DES-SBOX4)(55) = 8 and (DES-SBOX4)(56) = 9 and (DES-SBOX4)(57) = 4 and (DES-SBOX4)(58) = 5 and (DES-SBOX4)(59) = 11 and (DES-SBOX4)(60) = 12 and (DES-SBOX4)(61) = 7 and (DES-SBOX4)(62) = 2 and (DES-SBOX4)(63) = 14.

The function DES-SBOX5 from 64 into 16 is defined by the conditions (Def. 10).

(Def. 10) (DES-SBOX5)(0) = 2 and (DES-SBOX5)(1) = 12 and (DES-SBOX5)(2) = 4 and (DES-SBOX5)(3) = 1 and (DES-SBOX5)(4) = 7 and (DES-SBOX5)(5) = 10 and (DES-SBOX5)(6) = 11 and (DES-SBOX5)(7) = 6 and (DES-SBOX5)(8) = 8 and (DES-SBOX5)(9) = 5 and (DES-SBOX5)(10) = 3 and (DES-SBOX5)(11) = 15 and (DES-SBOX5)(12) = 13 and (DES-SBOX5)(13) = 0 and (DES-SBOX5)(14) = 14 and (DES-SBOX5)(15) = 9 and (DES-SBOX5)(16) = 14 and (DES-SBOX5)(17) = 11 and (DES-SBOX5)(18) = 2 and (DES-SBOX5)(19) = 12 and (DES-SBOX5)(20) = 4 and (DES-SBOX5)(21) = 7 and (DES-SBOX5)(22) = 13 and (DES-SBOX5)(23) = 1 and (DES-SBOX5)(24) = 5 and (DES-SBOX5)(25) = 0 and (DES-SBOX5)(26) = 15 and (DES-SBOX5)(27) = 10 and (DES-SBOX5)(28) = 3 and (DES-SBOX5)(29) = 9 and (DES-SBOX5)(30) = 8 and (DES-SBOX5)(31) = 6 and (DES-SBOX5)(32) = 4 and (DES-SBOX5)(33) = 2 and (DES-SBOX5)(34) = 1 and (DES-SBOX5)(35) = 11 and (DES-SBOX5)(36) = 10 and (DES-SBOX5)(37) = 13 and (DES-SBOX5)(38) = 7 and (DES-SBOX5)(39) = 8 and (DES-SBOX5)(40) = 15 and (DES-SBOX5)(41) = 9 and (DES-SBOX5)(42) = 12 and (DES-SBOX5)(43) = 5 and (DES-SBOX5)(44) = 6 and (DES-SBOX5)(45) = 3 and (DES-SBOX5)(46) = 0 and (DES-SBOX5)(47) = 14 and (DES-SBOX5)(48) = 11 and (DES-SBOX5)(49) = 8 and (DES-SBOX5)(50) = 12 and (DES-SBOX5)(51) =

7 and (DES-SBOX5)(52) = 1 and (DES-SBOX5)(53) = 14 and (DES-SBOX5)(54) = 2 and (DES-SBOX5)(55) = 13 and (DES-SBOX5)(56) = 6 and (DES-SBOX5)(57) = 15 and (DES-SBOX5)(58) = 0 and (DES-SBOX5)(59) = 9 and (DES-SBOX5)(60) = 10 and (DES-SBOX5)(61) = 4 and (DES-SBOX5)(62) = 5 and (DES-SBOX5)(63) = 3.

The function DES-SBOX6 from 64 into 16 is defined by the conditions (Def. 11).

(Def. 11) (DES-SBOX6)(0) = 12 and (DES-SBOX6)(1) = 1 and (DES-SBOX6)(2) = 10 and (DES-SBOX6)(3) = 15 and (DES-SBOX6)(4) = 9 and (DES-SBOX6)(5) = 2 and (DES-SBOX6)(6) = 6 and (DES-SBOX6)(7) = 8 and (DES-SBOX6)(8) = 0 and (DES-SBOX6)(9) = 13 and (DES-SBOX6)(10) = 3 and (DES-SBOX6)(11) = 4 and (DES-SBOX6)(12) = 14 and (DES-SBOX6)(13) = 7 and (DES-SBOX6)(14) = 5 and (DES-SBOX6)(15) = 11 and (DES-SBOX6)(16) = 10 and (DES-SBOX6)(17) = 15 and (DES-SBOX6)(18) = 4 and (DES-SBOX6)(19) = 2 and (DES-SBOX6)(20) = 7 and (DES-SBOX6)(21) = 12 and (DES-SBOX6)(22) = 9 and (DES-SBOX6)(23) = 5 and (DES-SBOX6)(24) = 6 and (DES-SBOX6)(25) = 1 and (DES-SBOX6)(26) = 13 and (DES-SBOX6)(27) = 14 and (DES-SBOX6)(28) = 0 and (DES-SBOX6)(29) = 11 and (DES-SBOX6)(30) = 3 and (DES-SBOX6)(31) = 8 and (DES-SBOX6)(32) = 9 and (DES-SBOX6)(33) = 14 and (DES-SBOX6)(34) = 15 and (DES-SBOX6)(35) = 5 and (DES-SBOX6)(36) = 2 and (DES-SBOX6)(37) = 8 and (DES-SBOX6)(38) = 12 and (DES-SBOX6)(39) = 3 and (DES-SBOX6)(40) = 7 and (DES-SBOX6)(41) = 0 and (DES-SBOX6)(42) = 4 and (DES-SBOX6)(43) = 10 and (DES-SBOX6)(44) = 1 and (DES-SBOX6)(45) = 13 and (DES-SBOX6)(46) = 11 and (DES-SBOX6)(47) = 6 and (DES-SBOX6)(48) = 4 and (DES-SBOX6)(49) = 3 and (DES-SBOX6)(50) = 2 and (DES-SBOX6)(51) = 12 and (DES-SBOX6)(52) = 9 and (DES-SBOX6)(53) = 5 and (DES-SBOX6)(54) = 15 and (DES-SBOX6)(55) = 10 and (DES-SBOX6)(56) = 11 and (DES-SBOX6)(57) = 14 and (DES-SBOX6)(58) = 1 and (DES-SBOX6)(59) = 7 and (DES-SBOX6)(60) = 6 and (DES-SBOX6)(61) = 0 and (DES-SBOX6)(62) = 8 and (DES-SBOX6)(63) = 13.

The function DES-SBOX7 from 64 into 16 is defined by the conditions (Def. 12).

(Def. 12) (DES-SBOX7)(0) = 4 and (DES-SBOX7)(1) = 11 and (DES-SBOX7)(2) = 2 and (DES-SBOX7)(3) = 14 and (DES-SBOX7)(4) = 15 and (DES-SBOX7)(5) = 0 and (DES-SBOX7)(6) = 8 and (DES-SBOX7)(7) =

13 and (DES-SBOX7)(8) = 3 and (DES-SBOX7)(9) = 12 and (DES-SBOX7)(10) = 9 and (DES-SBOX7)(11) = 7 and (DES-SBOX7)(12) = 5 and (DES-SBOX7)(13) = 10 and (DES-SBOX7)(14) = 6 and (DES-SBOX7)(15) = 1 and (DES-SBOX7)(16) = 13 and (DES-SBOX7)(17) = 0 and (DES-SBOX7)(18) = 11 and (DES-SBOX7)(19) = 7 and (DES-SBOX7)(20) = 4 and (DES-SBOX7)(21) = 9 and (DES-SBOX7)(22) = 1 and (DES-SBOX7)(23) = 10 and (DES-SBOX7)(24) = 14 and (DES-SBOX7)(25) = 3 and (DES-SBOX7)(26) = 5 and (DES-SBOX7)(27) = 12 and (DES-SBOX7)(28) = 2 and (DES-SBOX7)(29) = 15 and (DES-SBOX7)(30) = 8 and (DES-SBOX7)(31) = 6 and (DES-SBOX7)(32) = 1 and (DES-SBOX7)(33) = 4 and (DES-SBOX7)(34) = 11 and (DES-SBOX7)(35) = 13 and (DES-SBOX7)(36) = 12 and (DES-SBOX7)(37) = 3 and (DES-SBOX7)(38) = 7 and (DES-SBOX7)(39) = 14 and (DES-SBOX7)(40) = 10 and (DES-SBOX7)(41) = 15 and (DES-SBOX7)(42) = 6 and (DES-SBOX7)(43) = 8 and (DES-SBOX7)(44) = 0 and (DES-SBOX7)(45) = 5 and (DES-SBOX7)(46) = 9 and (DES-SBOX7)(47) = 2 and (DES-SBOX7)(48) = 6 and (DES-SBOX7)(49) = 11 and (DES-SBOX7)(50) = 13 and (DES-SBOX7)(51) = 8 and (DES-SBOX7)(52) = 1 and (DES-SBOX7)(53) = 4 and (DES-SBOX7)(54) = 10 and (DES-SBOX7)(55) = 7 and (DES-SBOX7)(56) = 9 and (DES-SBOX7)(57) = 5 and (DES-SBOX7)(58) = 0 and (DES-SBOX7)(59) = 15 and (DES-SBOX7)(60) = 14 and (DES-SBOX7)(61) = 2 and (DES-SBOX7)(62) = 3 and (DES-SBOX7)(63) = 12.

The function DES-SBOX8 from 64 into 16 is defined by the conditions (Def. 13).

(Def. 13) (DES-SBOX8)(0) = 13 and (DES-SBOX8)(1) = 2 and (DES-SBOX8)(2) = 8 and (DES-SBOX8)(3) = 4 and (DES-SBOX8)(4) = 6 and (DES-SBOX8)(5) = 15 and (DES-SBOX8)(6) = 11 and (DES-SBOX8)(7) = 1 and (DES-SBOX8)(8) = 10 and (DES-SBOX8)(9) = 9 and (DES-SBOX8)(10) = 3 and (DES-SBOX8)(11) = 14 and (DES-SBOX8)(12) = 5 and (DES-SBOX8)(13) = 0 and (DES-SBOX8)(14) = 12 and (DES-SBOX8)(15) = 7 and (DES-SBOX8)(16) = 1 and (DES-SBOX8)(17) = 15 and (DES-SBOX8)(18) = 13 and (DES-SBOX8)(19) = 8 and (DES-SBOX8)(20) = 10 and (DES-SBOX8)(21) = 3 and (DES-SBOX8)(22) = 7 and (DES-SBOX8)(23) = 4 and (DES-SBOX8)(24) = 12 and (DES-SBOX8)(25) = 5 and (DES-SBOX8)(26) = 5 and (DES-SBOX8)(27) = 11 and (DES-SBOX8)(28) = 0 and (DES-SBOX8)(29) = 14 and (DES-SBOX8)(30) = 9 and (DES-SBOX8)(31) = 2 and (DES-SBOX8)(32) = 7

and (DES-SBOX8)(33) = 11 and (DES-SBOX8)(34) = 4 and (DES-SBOX8)(35) = 1 and (DES-SBOX8)(36) = 9 and (DES-SBOX8)(37) = 12 and (DES-SBOX8)(38) = 14 and (DES-SBOX8)(39) = 2 and (DES-SBOX8)(40) = 0 and (DES-SBOX8)(41) = 6 and (DES-SBOX8)(42) = 10 and (DES-SBOX8)(43) = 13 and (DES-SBOX8)(44) = 15 and (DES-SBOX8)(45) = 3 and (DES-SBOX8)(46) = 5 and (DES-SBOX8)(47) = 8 and (DES-SBOX8)(48) = 2 and (DES-SBOX8)(49) = 1 and (DES-SBOX8)(50) = 14 and (DES-SBOX8)(51) = 7 and (DES-SBOX8)(52) = 4 and (DES-SBOX8)(53) = 10 and (DES-SBOX8)(54) = 8 and (DES-SBOX8)(55) = 13 and (DES-SBOX8)(56) = 15 and (DES-SBOX8)(57) = 12 and (DES-SBOX8)(58) = 9 and (DES-SBOX8)(59) = 0 and (DES-SBOX8)(60) = 3 and (DES-SBOX8)(61) = 5 and (DES-SBOX8)(62) = 6 and (DES-SBOX8)(63) = 11.

3. Initial Permutation

Let r be an element of $Boolean^{64}$. The functor DES-IP r yields an element of $Boolean^{64}$ and is defined by the conditions (Def. 14).

(Def. 14) (DES-IP r)(1) = $r(58)$ and (DES-IP r)(2) = $r(50)$ and (DES-IP r)(3) = $r(42)$ and (DES-IP r)(4) = $r(34)$ and (DES-IP r)(5) = $r(26)$ and (DES-IP r)(6) = $r(18)$ and (DES-IP r)(7) = $r(10)$ and (DES-IP r)(8) = $r(2)$ and (DES-IP r)(9) = $r(60)$ and (DES-IP r)(10) = $r(52)$ and (DES-IP r)(11) = $r(44)$ and (DES-IP r)(12) = $r(36)$ and (DES-IP r)(13) = $r(28)$ and (DES-IP r)(14) = $r(20)$ and (DES-IP r)(15) = $r(12)$ and (DES-IP r)(16) = $r(4)$ and (DES-IP r)(17) = $r(62)$ and (DES-IP r)(18) = $r(54)$ and (DES-IP r)(19) = $r(46)$ and (DES-IP r)(20) = $r(38)$ and (DES-IP r)(21) = $r(30)$ and (DES-IP r)(22) = $r(22)$ and (DES-IP r)(23) = $r(14)$ and (DES-IP r)(24) = $r(6)$ and (DES-IP r)(25) = $r(64)$ and (DES-IP r)(26) = $r(56)$ and (DES-IP r)(27) = $r(48)$ and (DES-IP r)(28) = $r(40)$ and (DES-IP r)(29) = $r(32)$ and (DES-IP r)(30) = $r(24)$ and (DES-IP r)(31) = $r(16)$ and (DES-IP r)(32) = $r(8)$ and (DES-IP r)(33) = $r(57)$ and (DES-IP r)(34) = $r(49)$ and (DES-IP r)(35) = $r(41)$ and (DES-IP r)(36) = $r(33)$ and (DES-IP r)(37) = $r(25)$ and (DES-IP r)(38) = $r(17)$ and (DES-IP r)(39) = $r(9)$ and (DES-IP r)(40) = $r(1)$ and (DES-IP r)(41) = $r(59)$ and (DES-IP r)(42) = $r(51)$ and (DES-IP r)(43) = $r(43)$ and (DES-IP r)(44) = $r(35)$ and (DES-IP r)(45) = $r(27)$ and (DES-IP r)(46) = $r(19)$ and (DES-IP r)(47) = $r(11)$ and (DES-IP r)(48) = $r(3)$ and (DES-IP r)(49) = $r(61)$ and (DES-IP r)(50) = $r(53)$ and (DES-IP r)(51) = $r(45)$ and (DES-IP r)(52) = $r(37)$

and $(\text{DES-IP}\, r)(53) = r(29)$ and $(\text{DES-IP}\, r)(54) = r(21)$ and $(\text{DES-IP}\, r)(55) = r(13)$ and $(\text{DES-IP}\, r)(56) = r(5)$ and $(\text{DES-IP}\, r)(57) = r(63)$ and $(\text{DES-IP}\, r)(58) = r(55)$ and $(\text{DES-IP}\, r)(59) = r(47)$ and $(\text{DES-IP}\, r)(60) = r(39)$ and $(\text{DES-IP}\, r)(61) = r(31)$ and $(\text{DES-IP}\, r)(62) = r(23)$ and $(\text{DES-IP}\, r)(63) = r(15)$ and $(\text{DES-IP}\, r)(64) = r(7)$.

The function DES-PIP from $Boolean^{64}$ into $Boolean^{64}$ is defined by:

(Def. 15) For every element i of $Boolean^{64}$ holds $(\text{DES-PIP})(i) = \text{DES-IP}\, i$.

Let r be an element of $Boolean^{64}$. The functor $\text{DES-IPINV}\, r$ yields an element of $Boolean^{64}$ and is defined by the conditions (Def. 16).

(Def. 16) $(\text{DES-IPINV}\, r)(1) = r(40)$ and $(\text{DES-IPINV}\, r)(2) = r(8)$ and $(\text{DES-IPINV}\, r)(3) = r(48)$ and $(\text{DES-IPINV}\, r)(4) = r(16)$ and $(\text{DES-IPINV}\, r)(5) = r(56)$ and $(\text{DES-IPINV}\, r)(6) = r(24)$ and $(\text{DES-IPINV}\, r)(7) = r(64)$ and $(\text{DES-IPINV}\, r)(8) = r(32)$ and $(\text{DES-IPINV}\, r)(9) = r(39)$ and $(\text{DES-IPINV}\, r)(10) = r(7)$ and $(\text{DES-IPINV}\, r)(11) = r(47)$ and $(\text{DES-IPINV}\, r)(12) = r(15)$ and $(\text{DES-IPINV}\, r)(13) = r(55)$ and $(\text{DES-IPINV}\, r)(14) = r(23)$ and $(\text{DES-IPINV}\, r)(15) = r(63)$ and $(\text{DES-IPINV}\, r)(16) = r(31)$ and $(\text{DES-IPINV}\, r)(17) = r(38)$ and $(\text{DES-IPINV}\, r)(18) = r(6)$ and $(\text{DES-IPINV}\, r)(19) = r(46)$ and $(\text{DES-IPINV}\, r)(20) = r(14)$ and $(\text{DES-IPINV}\, r)(21) = r(54)$ and $(\text{DES-IPINV}\, r)(22) = r(22)$ and $(\text{DES-IPINV}\, r)(23) = r(62)$ and $(\text{DES-IPINV}\, r)(24) = r(30)$ and $(\text{DES-IPINV}\, r)(25) = r(37)$ and $(\text{DES-IPINV}\, r)(26) = r(5)$ and $(\text{DES-IPINV}\, r)(27) = r(45)$ and $(\text{DES-IPINV}\, r)(28) = r(13)$ and $(\text{DES-IPINV}\, r)(29) = r(53)$ and $(\text{DES-IPINV}\, r)(30) = r(21)$ and $(\text{DES-IPINV}\, r)(31) = r(61)$ and $(\text{DES-IPINV}\, r)(32) = r(29)$ and $(\text{DES-IPINV}\, r)(33) = r(36)$ and $(\text{DES-IPINV}\, r)(34) = r(4)$ and $(\text{DES-IPINV}\, r)(35) = r(44)$ and $(\text{DES-IPINV}\, r)(36) = r(12)$ and $(\text{DES-IPINV}\, r)(37) = r(52)$ and $(\text{DES-IPINV}\, r)(38) = r(20)$ and $(\text{DES-IPINV}\, r)(39) = r(60)$ and $(\text{DES-IPINV}\, r)(40) = r(28)$ and $(\text{DES-IPINV}\, r)(41) = r(35)$ and $(\text{DES-IPINV}\, r)(42) = r(3)$ and $(\text{DES-IPINV}\, r)(43) = r(43)$ and $(\text{DES-IPINV}\, r)(44) = r(11)$ and $(\text{DES-IPINV}\, r)(45) = r(51)$ and $(\text{DES-IPINV}\, r)(46) = r(19)$ and $(\text{DES-IPINV}\, r)(47) = r(59)$ and $(\text{DES-IPINV}\, r)(48) = r(27)$ and $(\text{DES-IPINV}\, r)(49) = r(34)$ and $(\text{DES-IPINV}\, r)(50) = r(2)$ and $(\text{DES-IPINV}\, r)(51) = r(42)$ and $(\text{DES-IPINV}\, r)(52) = r(10)$ and $(\text{DES-IPINV}\, r)(53) = r(50)$ and $(\text{DES-IPINV}\, r)(54) = r(18)$ and $(\text{DES-IPINV}\, r)(55) = r(58)$ and $(\text{DES-IPINV}\, r)(56) = r(26)$ and $(\text{DES-IPINV}\, r)(57) = r(33)$ and $(\text{DES-IPINV}\, r)(58) = r(1)$ and $(\text{DES-IPINV}\, r)(59) = r(41)$ and $(\text{DES-IPINV}\, r)(60) = r(9)$ and $(\text{DES-IPINV}\, r)(61) = r(49)$ and $(\text{DES-IPINV}\, r)(62) = r(17)$ and

(DES-IPINV r)(63) = r(57) and (DES-IPINV r)(64) = r(25).

The function DES-PIPINV from $Boolean^{64}$ into $Boolean^{64}$ is defined by:

(Def. 17) For every element i of $Boolean^{64}$ holds (DES-PIPINV)(i) = DES-IPINV i.

Let us note that DES-PIP is bijective.

Let us note that DES-PIPINV is bijective.

The following proposition is true

(36) DES-PIPINV = (DES-PIP)$^{-1}$.

4. Feistel Function

Let r be an element of $Boolean^{32}$. The functor DES-E r yielding an element of $Boolean^{48}$ is defined by the conditions (Def. 18).

(Def. 18) (DES-E r)(1) = r(32) and (DES-E r)(2) = r(1) and (DES-E r)(3) = r(2) and (DES-E r)(4) = r(3) and (DES-E r)(5) = r(4) and (DES-E r)(6) = r(5) and (DES-E r)(7) = r(4) and (DES-E r)(8) = r(5) and (DES-E r)(9) = r(6) and (DES-E r)(10) = r(7) and (DES-E r)(11) = r(8) and (DES-E r)(12) = r(9) and (DES-E r)(13) = r(8) and (DES-E r)(14) = r(9) and (DES-E r)(15) = r(10) and (DES-E r)(16) = r(11) and (DES-E r)(17) = r(12) and (DES-E r)(18) = r(13) and (DES-E r)(19) = r(12) and (DES-E r)(20) = r(13) and (DES-E r)(21) = r(14) and (DES-E r)(22) = r(15) and (DES-E r)(23) = r(16) and (DES-E r)(24) = r(17) and (DES-E r)(25) = r(16) and (DES-E r)(26) = r(17) and (DES-E r)(27) = r(18) and (DES-E r)(28) = r(19) and (DES-E r)(29) = r(20) and (DES-E r)(30) = r(21) and (DES-E r)(31) = r(20) and (DES-E r)(32) = r(21) and (DES-E r)(33) = r(22) and (DES-E r)(34) = r(23) and (DES-E r)(35) = r(24) and (DES-E r)(36) = r(25) and (DES-E r)(37) = r(24) and (DES-E r)(38) = r(25) and (DES-E r)(39) = r(26) and (DES-E r)(40) = r(27) and (DES-E r)(41) = r(28) and (DES-E r)(42) = r(29) and (DES-E r)(43) = r(28) and (DES-E r)(44) = r(29) and (DES-E r)(45) = r(30) and (DES-E r)(46) = r(31) and (DES-E r)(47) = r(32) and (DES-E r)(48) = r(1).

Let r be an element of $Boolean^{32}$. The functor DES-P r yielding an element of $Boolean^{32}$ is defined by the conditions (Def. 19).

(Def. 19) (DES-P r)(1) = r(16) and (DES-P r)(2) = r(7) and (DES-P r)(3) = r(20) and (DES-P r)(4) = r(21) and (DES-P r)(5) = r(29) and (DES-P r)(6) = r(12) and (DES-P r)(7) = r(28) and (DES-P r)(8) = r(17) and (DES-P r)(9) = r(1) and (DES-P r)(10) = r(15) and (DES-P r)(11) = r(23) and (DES-P r)(12) = r(26) and (DES-P r)(13) = r(5) and (DES-P r)(14) = r(18) and (DES-P r)(15) = r(31) and

(DES-P r)(16) = r(10) and (DES-P r)(17) = r(2) and (DES-P r)(18) = r(8) and (DES-P r)(19) = r(24) and (DES-P r)(20) = r(14) and (DES-P r)(21) = r(32) and (DES-P r)(22) = r(27) and (DES-P r)(23) = r(3) and (DES-P r)(24) = r(9) and (DES-P r)(25) = r(19) and (DES-P r)(26) = r(13) and (DES-P r)(27) = r(30) and (DES-P r)(28) = r(6) and (DES-P r)(29) = r(22) and (DES-P r)(30) = r(11) and (DES-P r)(31) = r(4) and (DES-P r)(32) = r(25).

Let r be an element of $Boolean^{48}$. The functor DES-DIV8 r yielding an element of $(Boolean^6)^8$ is defined by the conditions (Def. 20).

(Def. 20) (DES-DIV8 r)(1) = Op-Left(r, 6) and (DES-DIV8 r)(2) = Op-Left(Op-Right(r, 6), 6) and (DES-DIV8 r)(3) = Op-Left(Op-Right(r, 12), 6) and (DES-DIV8 r)(4) = Op-Left(Op-Right(r, 18), 6) and (DES-DIV8 r)(5) = Op-Left(Op-Right(r, 24), 6) and (DES-DIV8 r)(6) = Op-Left(Op-Right(r, 30), 6) and (DES-DIV8 r)(7) = Op-Left(Op-Right(r, 36), 6) and (DES-DIV8 r)(8) = Op-Right(r, 42).

Next we state the proposition

(37) Let r be an element of $Boolean^{48}$. Then there exist elements s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8 of $Boolean^6$ such that s_1 = (DES-DIV8 r)(1) and s_2 = (DES-DIV8 r)(2) and s_3 = (DES-DIV8 r)(3) and s_4 = (DES-DIV8 r)(4) and s_5 = (DES-DIV8 r)(5) and s_6 = (DES-DIV8 r)(6) and s_7 = (DES-DIV8 r)(7) and s_8 = (DES-DIV8 r)(8) and $r = s_1 \frown s_2 \frown s_3 \frown s_4 \frown s_5 \frown s_6 \frown s_7 \frown s_8$.

Let t be an element of $Boolean^6$. The functor B6toN64 t yielding an element of 64 is defined by:

(Def. 21) B6toN64 $t = 32 \cdot t(1) + 16 \cdot t(6) + 8 \cdot t(2) + 4 \cdot t(3) + 2 \cdot t(4) + 1 \cdot t(5)$.

The function N16toB4 from 16 into $Boolean^4$ is defined by the conditions (Def. 22).

(Def. 22) (N16toB4)(0) = $\langle 0,0,0,0 \rangle$ and (N16toB4)(1) = $\langle 0,0,0,1 \rangle$ and (N16toB4)(2) = $\langle 0,0,1,0 \rangle$ and (N16toB4)(3) = $\langle 0,0,1,1 \rangle$ and (N16toB4)(4) = $\langle 0,1,0,0 \rangle$ and (N16toB4)(5) = $\langle 0,1,0,1 \rangle$ and (N16toB4)(6) = $\langle 0,1,1,0 \rangle$ and (N16toB4)(7) = $\langle 0,1,1,1 \rangle$ and (N16toB4)(8) = $\langle 1,0,0,0 \rangle$ and (N16toB4)(9) = $\langle 1,0,0,1 \rangle$ and (N16toB4)(10) = $\langle 1,0,1,0 \rangle$ and (N16toB4)(11) = $\langle 1,0,1,1 \rangle$ and (N16toB4)(12) = $\langle 1,1,0,0 \rangle$ and (N16toB4)(13) = $\langle 1,1,0,1 \rangle$ and (N16toB4)(14) = $\langle 1,1,1,0 \rangle$ and (N16toB4)(15) = $\langle 1,1,1,1 \rangle$.

Let R be an element of $Boolean^{32}$ and let R_2 be an element of $Boolean^{48}$. The functor DES-F(R, R_2) yields an element of $Boolean^{32}$ and is defined by the condition (Def. 23).

(Def. 23) There exist elements D_1, D_2, D_3, D_4, D_5, D_6, D_7, D_8 of $Boolean^6$ and

there exist elements x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 of $Boolean^4$ and there exists an element C_{32} of $Boolean^{32}$ such that
$D_1 = (\text{DES-DIV8 Op-XOR}(\text{DES-E}\, R, R_2))(1)$ and
$D_2 = (\text{DES-DIV8 Op-XOR}(\text{DES-E}\, R, R_2))(2)$ and
$D_3 = (\text{DES-DIV8 Op-XOR}(\text{DES-E}\, R, R_2))(3)$ and
$D_4 = (\text{DES-DIV8 Op-XOR}(\text{DES-E}\, R, R_2))(4)$ and
$D_5 = (\text{DES-DIV8 Op-XOR}(\text{DES-E}\, R, R_2))(5)$ and
$D_6 = (\text{DES-DIV8 Op-XOR}(\text{DES-E}\, R, R_2))(6)$ and
$D_7 = (\text{DES-DIV8 Op-XOR}(\text{DES-E}\, R, R_2))(7)$ and
$D_8 = (\text{DES-DIV8 Op-XOR}(\text{DES-E}\, R, R_2))(8)$ and
$\text{Op-XOR}(\text{DES-E}\, R, R_2) = D_1 \frown D_2 \frown D_3 \frown D_4 \frown D_5 \frown D_6 \frown D_7 \frown D_8$ and $x_1 = (\text{N16toB4})((\text{DES-SBOX1})(\text{B6toN64}\, D_1))$ and $x_2 = (\text{N16toB4})((\text{DES-SBOX2})(\text{B6toN64}\, D_2))$ and
$x_3 = (\text{N16toB4})((\text{DES-SBOX3})(\text{B6toN64}\, D_3))$ and
$x_4 = (\text{N16toB4})((\text{DES-SBOX4})(\text{B6toN64}\, D_4))$ and
$x_5 = (\text{N16toB4})((\text{DES-SBOX5})(\text{B6toN64}\, D_5))$ and
$x_6 = (\text{N16toB4})((\text{DES-SBOX6})(\text{B6toN64}\, D_6))$ and
$x_7 = (\text{N16toB4})((\text{DES-SBOX7})(\text{B6toN64}\, D_7))$ and
$x_8 = (\text{N16toB4})((\text{DES-SBOX8})(\text{B6toN64}\, D_8))$ and $C_{32} = x_1 \frown x_2 \frown x_3 \frown x_4 \frown x_5 \frown x_6 \frown x_7 \frown x_8$ and $\text{DES-F}(R, R_2) = \text{DES-P}\, C_{32}$.

The function DES-FFUNC from $Boolean^{32} \times Boolean^{48}$ into $Boolean^{32}$ is defined as follows:

(Def. 24) For every element z of $Boolean^{32} \times Boolean^{48}$ holds $(\text{DES-FFUNC})(z) = \text{DES-F}(z_{\mathbf{1}}, z_{\mathbf{2}})$.

5. Key Schedule

Let r be an element of $Boolean^{64}$. The functor DES-PC1 r yields an element of $Boolean^{56}$ and is defined by the conditions (Def. 25).

(Def. 25) $(\text{DES-PC1}\, r)(1) = r(57)$ and $(\text{DES-PC1}\, r)(2) = r(49)$ and $(\text{DES-PC1}\, r)(3) = r(41)$ and $(\text{DES-PC1}\, r)(4) = r(33)$ and $(\text{DES-PC1}\, r)(5) = r(25)$ and $(\text{DES-PC1}\, r)(6) = r(17)$ and $(\text{DES-PC1}\, r)(7) = r(9)$ and $(\text{DES-PC1}\, r)(8) = r(1)$ and $(\text{DES-PC1}\, r)(9) = r(58)$ and $(\text{DES-PC1}\, r)(10) = r(50)$ and $(\text{DES-PC1}\, r)(11) = r(42)$ and $(\text{DES-PC1}\, r)(12) = r(34)$ and $(\text{DES-PC1}\, r)(13) = r(26)$ and $(\text{DES-PC1}\, r)(14) = r(18)$ and $(\text{DES-PC1}\, r)(15) = r(10)$ and $(\text{DES-PC1}\, r)(16) = r(2)$ and $(\text{DES-PC1}\, r)(17) = r(59)$ and $(\text{DES-PC1}\, r)(18) = r(51)$ and $(\text{DES-PC1}\, r)(19) = r(43)$ and $(\text{DES-PC1}\, r)(20) = r(35)$ and $(\text{DES-PC1}\, r)(21) = r(27)$ and $(\text{DES-PC1}\, r)(22) = r(19)$ and $(\text{DES-PC1}\, r)(23) = r(11)$ and $(\text{DES-PC1}\, r)(24) = r(3)$ and $(\text{DES-PC1}\, r)(25) = r(60)$ and

(DES-PC1 r)(26) = $r(52)$ and (DES-PC1 r)(27) = $r(44)$ and (DES-PC1 r)(28) = $r(36)$ and (DES-PC1 r)(29) = $r(63)$ and (DES-PC1 r)(30) = $r(55)$ and (DES-PC1 r)(31) = $r(47)$ and (DES-PC1 r)(32) = $r(39)$ and (DES-PC1 r)(33) = $r(31)$ and (DES-PC1 r)(34) = $r(23)$ and (DES-PC1 r)(35) = $r(15)$ and (DES-PC1 r)(36) = $r(7)$ and (DES-PC1 r)(37) = $r(62)$ and (DES-PC1 r)(38) = $r(54)$ and (DES-PC1 r)(39) = $r(46)$ and (DES-PC1 r)(40) = $r(38)$ and (DES-PC1 r)(41) = $r(30)$ and (DES-PC1 r)(42) = $r(22)$ and (DES-PC1 r)(43) = $r(14)$ and (DES-PC1 r)(44) = $r(6)$ and (DES-PC1 r)(45) = $r(61)$ and (DES-PC1 r)(46) = $r(53)$ and (DES-PC1 r)(47) = $r(45)$ and (DES-PC1 r)(48) = $r(37)$ and (DES-PC1 r)(49) = $r(29)$ and (DES-PC1 r)(50) = $r(21)$ and (DES-PC1 r)(51) = $r(13)$ and (DES-PC1 r)(52) = $r(5)$ and (DES-PC1 r)(53) = $r(28)$ and (DES-PC1 r)(54) = $r(20)$ and (DES-PC1 r)(55) = $r(12)$ and (DES-PC1 r)(56) = $r(4)$.

Let r be an element of $Boolean^{56}$. The functor DES-PC2 r yielding an element of $Boolean^{48}$ is defined by the conditions (Def. 26).

(Def. 26) (DES-PC2 r)(1) = $r(14)$ and (DES-PC2 r)(2) = $r(17)$ and (DES-PC2 r)(3) = $r(11)$ and (DES-PC2 r)(4) = $r(24)$ and (DES-PC2 r)(5) = $r(1)$ and (DES-PC2 r)(6) = $r(5)$ and (DES-PC2 r)(7) = $r(3)$ and (DES-PC2 r)(8) = $r(28)$ and (DES-PC2 r)(9) = $r(15)$ and (DES-PC2 r)(10) = $r(6)$ and (DES-PC2 r)(11) = $r(21)$ and (DES-PC2 r)(12) = $r(10)$ and (DES-PC2 r)(13) = $r(23)$ and (DES-PC2 r)(14) = $r(19)$ and (DES-PC2 r)(15) = $r(12)$ and (DES-PC2 r)(16) = $r(4)$ and (DES-PC2 r)(17) = $r(26)$ and (DES-PC2 r)(18) = $r(8)$ and (DES-PC2 r)(19) = $r(16)$ and (DES-PC2 r)(20) = $r(7)$ and (DES-PC2 r)(21) = $r(27)$ and (DES-PC2 r)(22) = $r(20)$ and (DES-PC2 r)(23) = $r(13)$ and (DES-PC2 r)(24) = $r(2)$ and (DES-PC2 r)(25) = $r(41)$ and (DES-PC2 r)(26) = $r(52)$ and (DES-PC2 r)(27) = $r(31)$ and (DES-PC2 r)(28) = $r(37)$ and (DES-PC2 r)(29) = $r(47)$ and (DES-PC2 r)(30) = $r(55)$ and (DES-PC2 r)(31) = $r(30)$ and (DES-PC2 r)(32) = $r(40)$ and (DES-PC2 r)(33) = $r(51)$ and (DES-PC2 r)(34) = $r(45)$ and (DES-PC2 r)(35) = $r(33)$ and (DES-PC2 r)(36) = $r(48)$ and (DES-PC2 r)(37) = $r(44)$ and (DES-PC2 r)(38) = $r(49)$ and (DES-PC2 r)(39) = $r(39)$ and (DES-PC2 r)(40) = $r(56)$ and (DES-PC2 r)(41) = $r(34)$ and (DES-PC2 r)(42) = $r(53)$ and (DES-PC2 r)(43) = $r(46)$ and (DES-PC2 r)(44) = $r(42)$ and (DES-PC2 r)(45) = $r(50)$ and (DES-PC2 r)(46) = $r(36)$ and (DES-PC2 r)(47) = $r(29)$ and

(DES-PC2 r)(48) = r(32).

The finite sequence $\text{bitshift}_{\text{DES}}$ of elements of $\mathbb{N}$ is defined by the conditions (Def. 27).

(Def. 27) $\text{bitshift}_{\text{DES}}$ is 16-element and $(\text{bitshift}_{\text{DES}})(1) = 1$ and $(\text{bitshift}_{\text{DES}})(2) = 1$ and $(\text{bitshift}_{\text{DES}})(3) = 2$ and $(\text{bitshift}_{\text{DES}})(4) = 2$ and $(\text{bitshift}_{\text{DES}})(5) = 2$ and $(\text{bitshift}_{\text{DES}})(6) = 2$ and $(\text{bitshift}_{\text{DES}})(7) = 2$ and $(\text{bitshift}_{\text{DES}})(8) = 2$ and $(\text{bitshift}_{\text{DES}})(9) = 1$ and $(\text{bitshift}_{\text{DES}})(10) = 2$ and $(\text{bitshift}_{\text{DES}})(11) = 2$ and $(\text{bitshift}_{\text{DES}})(12) = 2$ and $(\text{bitshift}_{\text{DES}})(13) = 2$ and $(\text{bitshift}_{\text{DES}})(14) = 2$ and $(\text{bitshift}_{\text{DES}})(15) = 2$ and $(\text{bitshift}_{\text{DES}})(16) = 1$.

Let K_1 be an element of $\mathit{Boolean}^{64}$. The functor DES-KS K_1 yielding an element of $(\mathit{Boolean}^{48})^{16}$ is defined by the condition (Def. 28).

(Def. 28) There exist sequences C, D of $\mathit{Boolean}^{28}$ such that

(i) $C(0) = \text{Op-Left}(\text{DES-PC1}\, K_1, 28)$,

(ii) $D(0) = \text{Op-Right}(\text{DES-PC1}\, K_1, 28)$, and

(iii) for every element i of $\mathbb{N}$ such that $0 \leq i \leq 15$ holds $(\text{DES-KS}\, K_1)(i + 1) = \text{DES-PC2}(C(i + 1) \frown D(i + 1))$ and $C(i + 1) = \text{Op-Shift}(C(i), (\text{bitshift}_{\text{DES}})(i))$ and $D(i + 1) = \text{Op-Shift}(D(i), (\text{bitshift}_{\text{DES}})(i))$.

6. Encryption and Decryption

Let n, m, k be non empty elements of $\mathbb{N}$, let R_1 be an element of $(\mathit{Boolean}^m)^k$, let F be a function from $\mathit{Boolean}^n \times \mathit{Boolean}^m$ into $\mathit{Boolean}^n$, let I_1 be a permutation of $\mathit{Boolean}^{2 \cdot n}$, and let M be an element of $\mathit{Boolean}^{2 \cdot n}$. The functor DES-like-CoDec(M, F, I_1, R_1) yields an element of $\mathit{Boolean}^{2 \cdot n}$ and is defined by the condition (Def. 29).

(Def. 29) There exist sequences L, R of $\mathit{Boolean}^n$ such that

(i) $L(0) = \text{SP-Left}\, I_1(M)$,

(ii) $R(0) = \text{SP-Right}\, I_1(M)$,

(iii) for every element i of $\mathbb{N}$ such that $0 \leq i \leq k - 1$ holds $L(i + 1) = R(i)$ and $R(i + 1) = \text{Op-XOR}(L(i), F(R(i), (R_1)_{i+1}))$, and

(iv) DES-like-CoDec$(M, F, I_1, R_1) = {I_1}^{-1}(R(k) \frown L(k))$.

The following proposition is true

(38) Let n, m, k be non empty elements of $\mathbb{N}$, R_1 be an element of $(\mathit{Boolean}^m)^k$, F be a function from $\mathit{Boolean}^n \times \mathit{Boolean}^m$ into $\mathit{Boolean}^n$, I_1 be a permutation of $\mathit{Boolean}^{2 \cdot n}$, and M be an element of $\mathit{Boolean}^{2 \cdot n}$. Then DES-like-CoDec(DES-like-CoDec$(M, F, I_1, R_1), F, I_1, \text{Rev}(R_1)) = M$.

Let R_1 be an element of $(\mathit{Boolean}^{48})^{16}$, let F be a function from $\mathit{Boolean}^{32} \times \mathit{Boolean}^{48}$ into $\mathit{Boolean}^{32}$, let I_1 be a permutation of $\mathit{Boolean}^{64}$, and let M be an

element of $Boolean^{64}$. The functor DES-CoDec(M, F, I_1, R_1) yielding an element of $Boolean^{64}$ is defined by:

(Def. 30) There exists a permutation I_2 of $Boolean^{2 \cdot 32}$ and there exists an element M_1 of $Boolean^{2 \cdot 32}$ such that $I_2 = I_1$ and $M_1 = M$ and DES-CoDec(M, F, I_1, R_1) = DES-like-CoDec(M_1, F, I_2, R_1).

The following proposition is true

(39) Let R_1 be an element of $(Boolean^{48})^{16}$, F be a function from $Boolean^{32} \times Boolean^{48}$ into $Boolean^{32}$, I_1 be a permutation of $Boolean^{64}$, and M be an element of $Boolean^{64}$.

Then DES-CoDec(DES-CoDec$(M, F, I_1, R_1), F, I_1, \mathrm{Rev}(R_1)) = M$.

Let p_1, s_9 be elements of $Boolean^{64}$. The functor DES-ENC(p_1, s_9) yields an element of $Boolean^{64}$ and is defined by:

(Def. 31) DES-ENC(p_1, s_9) = DES-CoDec$(p_1,$ DES-FFUNC, DES-PIP, DES-KS $s_9)$.

Let c_1, s_9 be elements of $Boolean^{64}$. The functor DES-DEC(c_1, s_9) yields an element of $Boolean^{64}$ and is defined as follows:

(Def. 32) DES-DEC(c_1, s_9) =
DES-CoDec$(c_1,$ DES-FFUNC, DES-PIP, Rev(DES-KS $s_9))$.

The following proposition is true

(40) For all elements m_1, s_9 of $Boolean^{64}$ holds
DES-DEC(DES-ENC$(m_1, s_9), s_9) = m_1$.

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. 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. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[11] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(**2**):241–245, 1996.
[12] Shunichi Kobayashi and Kui Jia. A theory of Boolean valued functions and partitions. *Formalized Mathematics*, 7(**2**):249–254, 1998.
[13] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.
[14] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[15] U.S. Department of Commerce/National Institute of Standards and Technology. Fips pub 46-3, data encryption standard (DES). `http://csrc.nist.gov/publications/fips/-fips46-3/fips46-3.pdf`. *Federal Information Processing Standars Publication*, 1999.
[16] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[17] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[18] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[20] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.
[21] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[22] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received November 30, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 2, Pages 147–155, 2012
DOI: 10.2478/v10037-012-0017-x

VERSITA
versita.com/fm/

Semantics of MML Query[1]

Grzegorz Bancerek
Białystok Technical University
Poland

Summary. In the paper the semantics of MML Query queries is given. The formalization is done according to [4].

MML identifier: MMLQUERY, version: 7.12.02 4.181.1147

The notation and terminology used here have been introduced in the following papers: [1], [5], [11], [8], [10], [6], [2], [3], [15], [13], [14], [9], [12], and [7].

1. Elementary Queries

Let X be a set. A list of X is a subset of X. An operation of X is a binary relation on X.

Let x, y, R be sets. The predicate $x, y \in R$ is defined by:

(Def. 1) $\langle x, y \rangle \in R$.

Let x, y, R be sets. We introduce $x, y \notin R$ as an antonym of $x, y \in R$.

For simplicity, we use the following convention: X, Y, z, s denote sets, L, L_1, L_2, A denote lists of X, x denotes an element of X, O, O_2, O_3 denote operations of X, and m denotes a natural number.

The following proposition is true

(1) For all binary relations R_1, R_2 holds $R_1 \subseteq R_2$ iff for every z holds ${R_1}^\circ z \subseteq {R_2}^\circ z$.

Let us consider X, O, x. We introduce $x\ O$ as a synonym of $O^\circ x$.

Let us consider X, O, x. Then $x\ O$ is a list of X.

One can prove the following proposition

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

ISSN 1426–2630(p), 1898-9934(e)

(2) $x, y \in O$ iff $y \in x\ O$.

Let us consider X, O, L. We introduce $L|O$ as a synonym of $O^\circ L$.

Let us consider X, O, L. Then $L|O$ is a list of X and it can be characterized by the condition:

(Def. 2) $L|O = \bigcup\{x\ O : x \in L\}$.

The functor $L\&O$ yielding a list of X is defined as follows:

(Def. 3) $L\&O = \bigcap\{x\ O : x \in L\}$.

The functor $L\,\mathtt{where}\,O$ yielding a list of X is defined as follows:

(Def. 4) $L\,\mathtt{where}\,O = \{x : \bigvee_y\ (x, y \in O\ \wedge\ x \in L)\}$.

Let O_2 be an operation of X. The functor $L\,\mathtt{where}\,O = O_2$ yielding a list of X is defined as follows:

(Def. 5) $L\,\mathtt{where}\,O = O_2 = \{x : \overline{\overline{x\ O}} = \overline{\overline{x\ O_2}}\ \wedge\ x \in L\}$.

The functor $L\,\mathtt{where}\,O \leq O_2$ yielding a list of X is defined by:

(Def. 6) $L\,\mathtt{where}\,O \leq O_2 = \{x : \overline{\overline{x\ O}} \subseteq \overline{\overline{x\ O_2}}\ \wedge\ x \in L\}$.

The functor $L\,\mathtt{where}\,O \geq O_2$ yields a list of X and is defined by:

(Def. 7) $L\,\mathtt{where}\,O \geq O_2 = \{x : \overline{\overline{x\ O_2}} \subseteq \overline{\overline{x\ O}}\ \wedge\ x \in L\}$.

The functor $L\,\mathtt{where}\,O < O_2$ yielding a list of X is defined as follows:

(Def. 8) $L\,\mathtt{where}\,O < O_2 = \{x : \overline{\overline{x\ O}} \in \overline{\overline{x\ O_2}}\ \wedge\ x \in L\}$.

The functor $L\,\mathtt{where}\,O > O_2$ yields a list of X and is defined by:

(Def. 9) $L\,\mathtt{where}\,O > O_2 = \{x : \overline{\overline{x\ O_2}} \in \overline{\overline{x\ O}}\ \wedge\ x \in L\}$.

Let us consider X, L, O, n. The functor $L\,\mathtt{where}\,O = n$ yielding a list of X is defined as follows:

(Def. 10) $L\,\mathtt{where}\,O = n = \{x : \overline{\overline{x\ O}} = n\ \wedge\ x \in L\}$.

The functor $L\,\mathtt{where}\,O \leq n$ yielding a list of X is defined by:

(Def. 11) $L\,\mathtt{where}\,O \leq n = \{x : \overline{\overline{x\ O}} \subseteq n\ \wedge\ x \in L\}$.

The functor $L\,\mathtt{where}\,O \geq n$ yielding a list of X is defined as follows:

(Def. 12) $L\,\mathtt{where}\,O \geq n = \{x : n \subseteq \overline{\overline{x\ O}}\ \wedge\ x \in L\}$.

The functor $L\,\mathtt{where}\,O < n$ yields a list of X and is defined as follows:

(Def. 13) $L\,\mathtt{where}\,O < n = \{x : \overline{\overline{x\ O}} \in n\ \wedge\ x \in L\}$.

The functor $L\,\mathtt{where}\,O > n$ yields a list of X and is defined by:

(Def. 14) $L\,\mathtt{where}\,O > n = \{x : n \in \overline{\overline{x\ O}}\ \wedge\ x \in L\}$.

One can prove the following propositions:

(3) $x \in L\,\mathtt{where}\,O$ iff $x \in L$ and $x\ O \neq \emptyset$.

(4) $L\,\mathtt{where}\,O \subseteq L$.

(5) If $L \subseteq \operatorname{dom} O$, then $L\,\mathtt{where}\,O = L$.

(6) If $n \neq 0$ and $L_1 \subseteq L_2$, then $L_1\,\mathtt{where}\,O \geq n \subseteq L_2\,\mathtt{where}\,O$.

(7) $L\,\mathtt{where}\,O \geq 1 = L\,\mathtt{where}\,O$.

(8) If $L_1 \subseteq L_2$, then L_1 `where` $O > n \subseteq L_2$ `where` O.

(9) L `where` $O > 0 = L$ `where` O.

(10) If $n \neq 0$ and $L_1 \subseteq L_2$, then L_1 `where` $O = n \subseteq L_2$ `where` O.

(11) L `where` $O \geq n + 1 = L$ `where` $O > n$.

(12) L `where` $O \leq n = L$ `where` $O < n + 1$.

(13) If $n \leq m$ and $L_1 \subseteq L_2$ and $O_1 \subseteq O_2$, then L_1 `where` $O_1 \geq m \subseteq L_2$ `where` $O_2 \geq n$.

(14) If $n \leq m$ and $L_1 \subseteq L_2$ and $O_1 \subseteq O_2$, then L_1 `where` $O_1 > m \subseteq L_2$ `where` $O_2 > n$.

(15) If $n \leq m$ and $L_1 \subseteq L_2$ and $O_1 \subseteq O_2$, then L_1 `where` $O_2 \leq n \subseteq L_2$ `where` $O_1 \leq m$.

(16) If $n \leq m$ and $L_1 \subseteq L_2$ and $O_1 \subseteq O_2$, then L_1 `where` $O_2 < n \subseteq L_2$ `where` $O_1 < m$.

(17) If $O_1 \subseteq O_2$ and $L_1 \subseteq L_2$ and $O \subseteq O_3$, then L_1 `where` $O \geq O_2 \subseteq L_2$ `where` $O_3 \geq O_1$.

(18) If $O_1 \subseteq O_2$ and $L_1 \subseteq L_2$ and $O \subseteq O_3$, then L_1 `where` $O > O_2 \subseteq L_2$ `where` $O_3 > O_1$.

(19) If $O_1 \subseteq O_2$ and $L_1 \subseteq L_2$ and $O \subseteq O_3$, then L_1 `where` $O_3 \leq O_1 \subseteq L_2$ `where` $O \leq O_2$.

(20) If $O_1 \subseteq O_2$ and $L_1 \subseteq L_2$ and $O \subseteq O_3$, then L_1 `where` $O_3 < O_1 \subseteq L_2$ `where` $O < O_2$.

(21) L `where` $O > O_1 \subseteq L$ `where` O.

(22) If $O_1 \subseteq O_2$ and $L_1 \subseteq L_2$, then L_1 `where` $O_1 \subseteq L_2$ `where` O_2.

(23) $a \in L|O$ iff there exists b such that $a \in b\ O$ and $b \in L$.

Let us consider X, A, B. We introduce A `and` B as a synonym of $A \cap B$. We introduce A `or` B as a synonym of $A \cup B$. We introduce A `butnot` B as a synonym of $A \setminus B$.

Let us consider X, A, B. Then A `and` B is a list of X. Then A `or` B is a list of X. Then A `butnot` B is a list of X.

We now state several propositions:

(24) If $L_1 \neq \emptyset$ and $L_2 \neq \emptyset$, then $(L_1$ `or` $L_2)\&O = (L_1\&O)$ `and`$(L_2\&O)$.

(25) If $L_1 \subseteq L_2$ and $O_1 \subseteq O_2$, then $L_1|O_1 \subseteq L_2|O_2$.

(26) If $O_1 \subseteq O_2$, then $L\&O_1 \subseteq L\&O_2$.

(27) $L\&(O_1$ `and` $O_2) = (L\&O_1)$ `and`$(L\&O_2)$.

(28) If $L_1 \neq \emptyset$ and $L_1 \subseteq L_2$, then $L_2\&O \subseteq L_1\&O$.

2. Operations

One can prove the following two propositions:

(29) For all operations O_1, O_2 of X such that for every x holds $x\ O_1 = x\ O_2$ holds $O_1 = O_2$.

(30) For all operations O_1, O_2 of X such that for every L holds $L|O_1 = L|O_2$ holds $O_1 = O_2$.

The functor $\mathtt{not}\, O$ yielding an operation of X is defined as follows:

(Def. 15) For every L holds $L|\mathtt{not}\, O = \bigcup\{(x\ O = \emptyset \to \{x\}, \emptyset) : x \in L\}$.

Let us consider X and let O_1, O_2 be operations of X. We introduce $O_1\ \mathtt{and}\ O_2$ as a synonym of $O_1 \cap O_2$. We introduce $O_1\ \mathtt{or}\ O_2$ as a synonym of $O_1 \cup O_2$. We introduce $O_1\ \mathtt{butnot}\ O_2$ as a synonym of $O_1 \setminus O_2$. We introduce $O_1|O_2$ as a synonym of $O_1 \cdot O_2$.

Let us consider X and let O_1, O_2 be operations of X. Then $O_1\ \mathtt{and}\ O_2$ is an operation of X and it can be characterized by the condition:

(Def. 16) For every L holds $L|(O_1\ \mathtt{and}\ O_2) = \bigcup\{(x\ O_1)\ \mathtt{and}(x\ O_2) : x \in L\}$.

Then $O_1\ \mathtt{or}\ O_2$ is an operation of X and it can be characterized by the condition:

(Def. 17) For every L holds $L|(O_1\ \mathtt{or}\ O_2) = \bigcup\{(x\ O_1)\ \mathtt{or}(x\ O_2) : x \in L\}$.

Then $O_1\ \mathtt{butnot}\ O_2$ is an operation of X and it can be characterized by the condition:

(Def. 18) For every L holds $L|(O_1\ \mathtt{butnot}\ O_2) = \bigcup\{(x\ O_1)\ \mathtt{butnot}(x\ O_2) : x \in L\}$.

Then $O_1|O_2$ is an operation of X and it can be characterized by the condition:

(Def. 19) For every L holds $L|(O_1|O_2) = L|O_1|O_2$.

The functor $O_1 \& O_2$ yielding an operation of X is defined as follows:

(Def. 20) For every L holds $L|(O_1 \& O_2) = \bigcup\{(x\ O_1) \& O_2 : x \in L\}$.

We now state a number of propositions:

(31) $x\ (O_1\ \mathtt{and}\ O_2) = (x\ O_1)\ \mathtt{and}(x\ O_2)$.

(32) $x\ (O_1\ \mathtt{or}\ O_2) = (x\ O_1)\ \mathtt{or}(x\ O_2)$.

(33) $x\ (O_1\ \mathtt{butnot}\ O_2) = (x\ O_1)\ \mathtt{butnot}(x\ O_2)$.

(34) $x\ (O_1|O_2) = (x\ O_1)|O_2$.

(35) $x\ (O_1 \& O_2) = (x\ O_1) \& O_2$.

(36) $z, s \in \mathtt{not}\, O$ iff $z = s$ and $z \in X$ and $z \notin \operatorname{dom} O$.

(37) $\mathtt{not}\, O = \mathrm{id}_{X \setminus \operatorname{dom} O}$.

(38) $\operatorname{dom} \mathtt{not}\ \mathtt{not}\, O = \operatorname{dom} O$.

(39) $L\ \mathtt{where}\ \mathtt{not}\ \mathtt{not}\, O = L\ \mathtt{where}\, O$.

(40) $L\ \mathtt{where}\, O = 0 = L\ \mathtt{where}\ \mathtt{not}\, O$.

(41) $\mathtt{not}\ \mathtt{not}\ \mathtt{not}\, O = \mathtt{not}\, O$.

(42) $\mathtt{not}\, O_1\ \mathtt{or}\ \mathtt{not}\, O_2 \subseteq \mathtt{not}(O_1\ \mathtt{and}\ O_2)$.

(43) $\mathtt{not}(O_1 \mathtt{\ or\ } O_2) = \mathtt{not}\ O_1 \mathtt{\ and\ not\ } O_2$.

(44) If $\operatorname{dom} O_1 = X$ and $\operatorname{dom} O_2 = X$, then $(O_1 \mathtt{\ or\ } O_2)\&O = (O_1\&O) \mathtt{\ and\ } (O_2\&O)$.

Let us consider X, O. We say that O is filtering if and only if:

(Def. 21) $O \subseteq \mathrm{id}_X$.

Next we state the proposition

(45) O is filtering iff $O = \mathrm{id}_{\operatorname{dom} O}$.

Let us consider X, O. Note that $\mathtt{not}\ O$ is filtering.

Let us consider X. Note that there exists an operation of X which is filtering.

In the sequel F_1, F_2 denote filtering operations of X.

Let us consider X, F, O. One can check the following observations:

* $F \mathtt{\ and\ } O$ is filtering,
* $O \mathtt{\ and\ } F$ is filtering, and
* $F \mathtt{\ butnot\ } O$ is filtering.

Let us consider X, F_1, F_2. One can verify that $F_1 \mathtt{\ or\ } F_2$ is filtering.

(46) If $z \in x\ F$, then $z = x$.

(47) $L|F = L \mathtt{\ where\ } F$.

(48) $\mathtt{not\ not}\ F = F$.

(49) $\mathtt{not}(F_1 \mathtt{\ and\ } F_2) = \mathtt{not}\ F_1 \mathtt{\ or\ not\ } F_2$.

(50) $\operatorname{dom}(O \mathtt{\ or\ not\ } O) = X$.

(51) $F \mathtt{\ or\ not\ } F = \mathrm{id}_X$.

(52) $O \mathtt{\ and\ not\ } O = \emptyset$.

(53) $(O_1 \mathtt{\ or\ } O_2) \mathtt{\ and\ not\ } O_1 \subseteq O_2$.

3. Rough Queries

Let A be a finite sequence and let a be a set. The functor #occurrences(a, A) yielding a natural number is defined as follows:

(Def. 22) #occurrences$(a, A) = \overline{\{i : i \in \operatorname{dom} A \ \wedge\ a \in A(i)\}}$.

We now state two propositions:

(54) For every finite sequence A and for every set a holds #occurrences$(a, A) \leq \operatorname{len} A$.

(55) For every finite sequence A and for every set a holds $A \neq \emptyset$ and #occurrences$(a, A) = \operatorname{len} A$ iff $a \in \bigcap \operatorname{rng} A$.

The functor max# A yielding a natural number is defined as follows:

(Def. 23) For every set a holds #occurrences$(a, A) \leq$ max# A and for every n such that for every set a holds #occurrences$(a, A) \leq n$ holds max# $A \leq n$.

(56) For every finite sequence A holds $\max\#\, A \leq \operatorname{len} A$.

(57) For every finite sequence A and for every set a such that $\#\text{occurrences}(a, A) = \operatorname{len} A$ holds $\max\#\, A = \operatorname{len} A$.

Let us consider X, let A be a finite sequence of elements of 2^X, and let n be a natural number. The functor $\texttt{rough}\, n(A)$ yields a list of X and is defined as follows:

(Def. 24) $\texttt{rough}\, n(A) = \{x : n \leq \#\text{occurrences}(x, A)\}$ if $X \neq \emptyset$.

Let m be a natural number. The functor $\texttt{rough}\, n\text{-}m(A)$ yields a list of X and is defined by:

(Def. 25) $\texttt{rough}\, n\text{-}m(A) = \{x : n \leq \#\text{occurrences}(x, A) \wedge \#\text{occurrences}(x, A) \leq m\}$ if $X \neq \emptyset$.

Let us consider X and let A be a finite sequence of elements of 2^X. The functor $\texttt{rough}(A)$ yielding a list of X is defined by:

(Def. 26) $\texttt{rough}(A) = \texttt{rough}\, \max\#\, A(A)$.

Next we state several propositions:

(58) For every finite sequence A of elements of 2^X holds $\texttt{rough}\, n\text{-}\operatorname{len} A(A) = \texttt{rough}\, n(A)$.

(59) For every finite sequence A of elements of 2^X such that $n \leq m$ holds $\texttt{rough}\, m(A) \subseteq \texttt{rough}\, n(A)$.

(60) Let A be a finite sequence of elements of 2^X and n_1, n_2, m_1, m_2 be natural numbers. If $n_1 \leq m_1$ and $n_2 \leq m_2$, then $\texttt{rough}\, m_1\text{-}n_2(A) \subseteq \texttt{rough}\, n_1\text{-}m_2(A)$.

(61) For every finite sequence A of elements of 2^X holds $\texttt{rough}\, n\text{-}m(A) \subseteq \texttt{rough}\, n(A)$.

(62) For every finite sequence A of elements of 2^X such that $A \neq \emptyset$ holds $\texttt{rough}\, \operatorname{len} A(A) = \bigcap \operatorname{rng} A$.

(63) For every finite sequence A of elements of 2^X holds $\texttt{rough}\, 1(A) = \bigcup A$.

(64) For all lists L_1, L_2 of X holds $\texttt{rough}\, 2(\langle L_1, L_2\rangle) = L_1\ \texttt{and}\ L_2$.

(65) For all lists L_1, L_2 of X holds $\texttt{rough}\, 1(\langle L_1, L_2\rangle) = L_1\ \texttt{or}\ L_2$.

4. Constructor Database

We introduce constructor databases which are extensions of 1-sorted structures and are systems

$\langle$ a carrier, constructors, a ref-operation $\rangle$,

where the carrier is a set, the constructors constitute a list of the carrier, and the ref-operation is a relation between the carrier and the constructors.

Let X be a 1-sorted structure. A list of X is a list of the carrier of X. An operation of X is an operation of the carrier of X.

Let us consider X, let S be a subset of X, and let R be a relation between X and S. The functor ${}^{@}R$ yields a binary relation on X and is defined by:

(Def. 27) ${}^{@}R = R$.

Let X be a constructor database and let a be an element of X. The functor $a\,\mathtt{ref}$ yielding a list of X is defined as follows:

(Def. 28) $a\,\mathtt{ref} = a\ {}^{@}$the ref-operation of X.

The functor $a\,\mathtt{occur}$ yields a list of X and is defined as follows:

(Def. 29) $a\,\mathtt{occur} = a\ ({}^{@}$the ref-operation of $X)^{\smile}$.

The following proposition is true

(66) For every constructor database X and for all elements x, y of X holds $x \in y\,\mathtt{ref}$ iff $y \in x\,\mathtt{occur}$.

Let X be a constructor database. We say that X is ref-finite if and only if:

(Def. 30) For every element x of X holds $x\,\mathtt{ref}$ is finite.

One can verify that every constructor database which is finite is also ref-finite.

Let us note that there exists a constructor database which is finite and non empty.

Let X be a ref-finite constructor database and let x be an element of X. Observe that $x\,\mathtt{ref}$ is finite.

Let X be a constructor database and let A be a finite sequence of elements of the constructors of X. The functor $\mathtt{atleast}(A)$ yielding a list of X is defined by:

(Def. 31) $\mathtt{atleast}(A) = \{x \in X\colon \operatorname{rng} A \subseteq x\,\mathtt{ref}\}$ if the carrier of $X \neq \emptyset$.

The functor $\mathtt{atmost}(A)$ yielding a list of X is defined as follows:

(Def. 32) $\mathtt{atmost}(A) = \{x \in X\colon x\,\mathtt{ref} \subseteq \operatorname{rng} A\}$ if the carrier of $X \neq \emptyset$.

The functor $\mathtt{exactly}(A)$ yields a list of X and is defined by:

(Def. 33) $\mathtt{exactly}(A) = \{x \in X\colon x\,\mathtt{ref} = \operatorname{rng} A\}$ if the carrier of $X \neq \emptyset$.

Let n be a natural number. The functor $\mathtt{atleast\ minus}\,n(A)$ yields a list of X and is defined by:

(Def. 34) $\mathtt{atleast\ minus}\,n(A) = \{x \in X\colon \overline{\overline{\operatorname{rng} A \setminus x\,\mathtt{ref}}} \leq n\}$ if the carrier of $X \neq \emptyset$.

Let X be a ref-finite constructor database, let A be a finite sequence of elements of the constructors of X, and let n be a natural number. The functor $\mathtt{atmost\ plus}\,n(A)$ yields a list of X and is defined by:

(Def. 35) $\mathtt{atmost\ plus}\,n(A) = \{x \in X\colon \overline{\overline{x\,\mathtt{ref} \setminus \operatorname{rng} A}} \leq n\}$ if the carrier of $X \neq \emptyset$.

Let m be a natural number. The functor $\mathtt{exactly\ plus}\,n\,\mathtt{minus}\,m(A)$ yielding a list of X is defined by:

(Def. 36) $\texttt{exactly plus}\, n\, \texttt{minus}\, m(A) = \{x \in X\colon \overline{\overline{x\,\texttt{ref} \setminus \operatorname{rng} A}} \leq n \wedge \overline{\overline{\operatorname{rng} A \setminus x\,\texttt{ref}}} \leq m\}$ if the carrier of $X \neq \emptyset$.

In the sequel X denotes a constructor database, x denotes an element of X, B denotes a finite sequence of elements of the constructors of Y, and y denotes an element of Y.

The following propositions are true:

(67) $\texttt{atleast minus}\, 0(A) = \texttt{atleast}(A)$.

(68) $\texttt{atmost plus}\, 0(B) = \texttt{atmost}(B)$.

(69) $\texttt{exactly plus}\, 0\, \texttt{minus}\, 0(B) = \texttt{exactly}(B)$.

(70) If $n \leq m$, then $\texttt{atleast minus}\, n(A) \subseteq \texttt{atleast minus}\, m(A)$.

(71) If $n \leq m$, then $\texttt{atmost plus}\, n(B) \subseteq \texttt{atmost plus}\, m(B)$.

(72) For all natural numbers n_1, n_2, m_1, m_2 such that $n_1 \leq m_1$ and $n_2 \leq m_2$ holds $\texttt{exactly plus}\, n_1\, \texttt{minus}\, n_2(B) \subseteq \texttt{exactly plus}\, m_1\, \texttt{minus}\, m_2(B)$.

(73) $\texttt{atleast}(A) \subseteq \texttt{atleast minus}\, n(A)$.

(74) $\texttt{atmost}(B) \subseteq \texttt{atmost plus}\, n(B)$.

(75) $\texttt{exactly}(B) \subseteq \texttt{exactly plus}\, n\, \texttt{minus}\, m(B)$.

(76) $\texttt{exactly}(A) = \texttt{atleast}(A)\, \texttt{and}\, \texttt{atmost}(A)$.

(77) $\texttt{exactly plus}\, n\, \texttt{minus}\, m(B) = \texttt{atleast minus}\, m(B)\, \texttt{and}\, \texttt{atmost plus}\, n(B)$.

(78) If $A \neq \emptyset$, then $\texttt{atleast}(A) = \bigcap\{x\, \texttt{occur} : x \in \operatorname{rng} A\}$.

(79) For all elements c_1, c_2 of X such that $A = \langle c_1, c_2\rangle$ holds $\texttt{atleast}(A) = c_1\, \texttt{occur}\, \texttt{and}\, c_2\, \texttt{occur}$.

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. Information retrieval and rendering with MML query. *LNCS*, 4108:266–279, 2006.
[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. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[8] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[9] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[10] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[11] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 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.
[14] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[15] Bo Zhang, Hiroshi Yamazaki, and Yatsuka Nakamura. Set sequences and monotone class. *Formalized Mathematics*, 13(**4**):435–441, 2005.

Received December 18, 2011

FORMALIZED MATHEMATICS
Vol. 20, No. 2, Pages 157–159, 2012
DOI: 10.2478/v10037-012-0018-9

VERSITA
versita.com/fm/

Routh's, Menelaus' and Generalized Ceva's Theorems

Boris A. Shminke
Shakhtyorskaya 2
453850 Meleuz, Russia

Summary. The goal of this article is to formalize Ceva's theorem that is in the [8] on the web. Alongside with it formalizations of Routh's, Menelaus' and generalized form of Ceva's theorem itself are provided.

MML identifier: MENELAUS, version: 7.12.02 4.181.1147

The papers [1], [4], [3], [6], [5], [2], [7], and [9] provide the notation and terminology for this paper.

1. Some Properties of the Area of Triangle

We use the following convention: A, B, C, A_1, B_1, C_1, A_2, B_2, C_2 are points of $\mathcal{E}^2_{\mathrm{T}}$, l_1, m_1, n_1 are real numbers, and X, Y, Z are subsets of $\mathcal{E}^2_{\mathrm{T}}$.

Let us consider X, Y. We introduce X is parallel to Y as a synonym of X misses Y.

Let us consider X, Y, Z. We say that X, Y, Z are concurrent if and only if:

(Def. 1) X is parallel to Y and Y is parallel to Z and Z is parallel to X or there exists A such that $A \in X$ and $A \in Y$ and $A \in Z$.

One can prove the following propositions:

(1) $(A + B)_{\mathbf{1}} = A_{\mathbf{1}} + B_{\mathbf{1}}$ and $(A + B)_{\mathbf{2}} = A_{\mathbf{2}} + B_{\mathbf{2}}$.

(2) $(l_1 \cdot A)_{\mathbf{1}} = l_1 \cdot A_{\mathbf{1}}$ and $(l_1 \cdot A)_{\mathbf{2}} = l_1 \cdot A_{\mathbf{2}}$.

(3) $(-A)_{\mathbf{1}} = -A_{\mathbf{1}}$ and $(-A)_{\mathbf{2}} = -A_{\mathbf{2}}$.

(4) $(l_1 \cdot A + m_1 \cdot B)_{\mathbf{1}} = l_1 \cdot A_{\mathbf{1}} + m_1 \cdot B_{\mathbf{1}}$ and $(l_1 \cdot A + m_1 \cdot B)_{\mathbf{2}} = l_1 \cdot A_{\mathbf{2}} + m_1 \cdot B_{\mathbf{2}}$.

ISSN 1426–2630(p), 1898-9934(e)

(5) $((-l_1)\cdot A)_{\mathbf{1}} = -l_1 \cdot A_{\mathbf{1}}$ and $((-l_1)\cdot A)_{\mathbf{2}} = -l_1 \cdot A_{\mathbf{2}}$.

(6) $(l_1 \cdot A - m_1 \cdot B)_{\mathbf{1}} = l_1 \cdot A_{\mathbf{1}} - m_1 \cdot B_{\mathbf{1}}$ and $(l_1 \cdot A - m_1 \cdot B)_{\mathbf{2}} = l_1 \cdot A_{\mathbf{2}} - m_1 \cdot B_{\mathbf{2}}$.

(7) The area of $\triangle((1-l_1)\cdot A + l_1 \cdot A_1, B, C) = (1-l_1)\cdot$the area of $\triangle(A,B,C) + l_1 \cdot$ the area of $\triangle(A_1,B,C)$.

(8) If $\measuredangle(A,B,C) = 0$ and A, B, C are mutually different, then $\measuredangle(B,C,A) = \pi$ or $\measuredangle(B,A,C) = \pi$.

(9) A, B and C are collinear iff the area of $\triangle(A,B,C) = 0$.

(10) The area of $\triangle(0_{\mathcal{E}^2_{\mathrm{T}}}, B, C) = \frac{B_{\mathbf{1}}\cdot C_{\mathbf{2}} - C_{\mathbf{1}}\cdot B_{\mathbf{2}}}{2}$.

(11) The area of $\triangle(A + A_1, B, C) =$ ((the area of $\triangle(A,B,C)$) + (the area of $\triangle(A_1,B,C)$)) − the area of $\triangle(0_{\mathcal{E}^2_{\mathrm{T}}}, B, C)$.

(12) If $A \in \mathcal{L}(B,C)$, then $A \in \mathrm{Line}(B,C)$.

(13) If $B \neq C$, then A, B and C are collinear iff $A \in \mathrm{Line}(B,C)$.

(14) If A, B, C form a triangle and $A_1 = (1-l_1)\cdot B + l_1 \cdot C$, then $A \neq A_1$.

(15) Suppose A, B, C form a triangle. Then

(i) A, C, B form a triangle,

(ii) B, A, C form a triangle,

(iii) B, C, A form a triangle,

(iv) C, A, B form a triangle, and

(v) C, B, A form a triangle.

(16) Suppose A, B, C form a triangle and $A_1 = (1-l_1)\cdot B + l_1 \cdot C$ and $B_1 = (1-m_1)\cdot C + m_1 \cdot A$ and $m_1 \neq 1$. Then $(1-m_1) + l_1 \cdot m_1 \neq 0$ if and only if $\mathrm{Line}(A, A_1)$ is not parallel to $\mathrm{Line}(B, B_1)$.

2. Ceva's Theorem and Others

The following propositions are true:

(17) Suppose $A_1 = (1-l_1)\cdot B + l_1 \cdot C$ and $B_1 = (1-m_1)\cdot C + m_1 \cdot A$ and $C_1 = (1-n_1)\cdot A + n_1 \cdot B$. Then the area of $\triangle(A_1, B_1, C_1) = ((1-l_1)\cdot(1-m_1)\cdot(1-n_1) + l_1 \cdot m_1 \cdot n_1)\cdot$ the area of $\triangle(A,B,C)$.

(18) Suppose A, B, C form a triangle and $A_1 = (1-l_1)\cdot B + l_1 \cdot C$ and $B_1 = (1-m_1)\cdot C + m_1 \cdot A$ and $C_1 = (1-n_1)\cdot A + n_1 \cdot B$ and $l_1 \neq 1$ and $m_1 \neq 1$ and $n_1 \neq 1$. Then A_1, B_1 and C_1 are collinear if and only if $\frac{l_1}{1-l_1} \cdot \frac{m_1}{1-m_1} \cdot \frac{n_1}{1-n_1} = -1$.

(19) Suppose that A, B, C form a triangle and $A_1 = (1-l_1)\cdot B + l_1 \cdot C$ and $B_1 = (1-m_1)\cdot C + m_1 \cdot A$ and $C_1 = (1-n_1)\cdot A + n_1 \cdot B$ and $l_1 \neq 1$ and $m_1 \neq 1$ and $n_1 \neq 1$ and A, A_1 and C_2 are collinear and B, B_1 and C_2 are collinear and B, B_1 and A_2 are collinear and C, C_1 and A_2 are collinear and A, A_1 and B_2 are collinear and C, C_1 and B_2 are collinear. Then

(i) $((1-m_1)+l_1\cdot m_1)\cdot((1-l_1)+n_1\cdot l_1)\cdot((1-n_1)+m_1\cdot n_1)\neq 0$, and

(ii) the area of $\triangle(A_2,B_2,C_2)=\frac{(m_1\cdot n_1\cdot l_1-(1-m_1)\cdot(1-n_1)\cdot(1-l_1))^2}{((1-m_1)+l_1\cdot m_1)\cdot((1-l_1)+n_1\cdot l_1)\cdot((1-n_1)+m_1\cdot n_1)}\cdot$ the area of $\triangle(A,B,C)$.

(20) Suppose that A, B, C form a triangle and $A_1=\frac{2}{3}\cdot B+\frac{1}{3}\cdot C$ and $B_1=\frac{2}{3}\cdot C+\frac{1}{3}\cdot A$ and $C_1=\frac{2}{3}\cdot A+\frac{1}{3}\cdot B$ and A, A_1 and C_2 are collinear and B, B_1 and C_2 are collinear and B, B_1 and A_2 are collinear and C, C_1 and A_2 are collinear and A, A_1 and B_2 are collinear and C, C_1 and B_2 are collinear. Then the area of $\triangle(A_2,B_2,C_2)=\frac{\text{the area of }\triangle(A,B,C)}{7}$.

(21) Suppose that A, B, C form a triangle and $A_1=(1-l_1)\cdot B+l_1\cdot C$ and $B_1=(1-m_1)\cdot C+m_1\cdot A$ and $C_1=(1-n_1)\cdot A+n_1\cdot B$ and $l_1\neq 1$ and $m_1\neq 1$ and $n_1\neq 1$ and $(1-m_1)+l_1\cdot m_1\neq 0$ and $(1-l_1)+n_1\cdot l_1\neq 0$ and $(1-n_1)+m_1\cdot n_1\neq 0$. Then $\frac{l_1}{1-l_1}\cdot\frac{m_1}{1-m_1}\cdot\frac{n_1}{1-n_1}=1$ if and only if there exists A_2 such that A, A_1 and A_2 are collinear and B, B_1 and A_2 are collinear and C, C_1 and A_2 are collinear.

(22) Suppose A, B, C form a triangle and $A_1=(1-l_1)\cdot B+l_1\cdot C$ and $B_1=(1-m_1)\cdot C+m_1\cdot A$ and $C_1=(1-n_1)\cdot A+n_1\cdot B$ and $l_1\neq 1$ and $m_1\neq 1$ and $n_1\neq 1$. Then $\frac{l_1}{1-l_1}\cdot\frac{m_1}{1-m_1}\cdot\frac{n_1}{1-n_1}=1$ if and only if $\mathrm{Line}(A,A_1)$, $\mathrm{Line}(B,B_1)$, $\mathrm{Line}(C,C_1)$ are concurrent.

REFERENCES

[1] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.

[2] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[3] Akihiro Kubo. Lines in n-dimensional Euclidean spaces. *Formalized Mathematics*, 11(**4**):371–376, 2003.

[4] Akihiro Kubo and Yatsuka Nakamura. Angle and triangle in Euclidian topological space. *Formalized Mathematics*, 11(**3**):281–287, 2003.

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

[6] Marco Riccardi. Heron's formula and Ptolemy's theorem. *Formalized Mathematics*, 16(**2**):97–101, 2008, doi:10.2478/v10037-008-0014-2.

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

[8] Freek Wiedijk. Formalizing 100 theorems. `http://www.cs.ru.nl/~freek/100/`.

[9] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

Received January 16, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 2, Pages 161–174, 2012
DOI: 10.2478/v10037-012-0019-8

VERSITA
versita.com/fm/

Simple Graphs as Simplicial Complexes: the Mycielskian of a Graph[1]

Piotr Rudnicki
University of Alberta
Edmonton, Canada

Lorna Stewart
University of Alberta
Edmonton, Canada

Summary. Harary [10, p. 7] claims that Veblen [20, p. 2] first suggested to formalize simple graphs using simplicial complexes. We have developed basic terminology for simple graphs as at most 1-dimensional complexes.

We formalize this new setting and then reprove Mycielski's [12] construction resulting in a triangle-free graph with arbitrarily large chromatic number. A different formalization of similar material is in [15].

MML identifier: SCMYCIEL, version: 7.12.02 4.181.1147

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

1. Preliminaries

One can prove the following propositions:

(1) For all sets x, X holds $\langle x, X\rangle \notin X$.

(2) For all sets x, X holds $\langle x, X\rangle \neq X$.

(3) For all sets x, X holds $\langle x, X\rangle \neq x$.

(4) For all sets x_1, y_1, x_2, y_2, X such that x_1, $x_2 \in X$ and $\{x_1, \langle y_1, X\rangle\} = \{x_2, \langle y_2, X\rangle\}$ holds $x_1 = x_2$ and $y_1 = y_2$.

(5) For all sets X, v such that $3 \subseteq \overline{\overline{X}}$ there exist sets v_1, v_2 such that v_1, $v_2 \in X$ and $v_1 \neq v$ and $v_2 \neq v$ and $v_1 \neq v_2$.

(6) For every set x holds $S_{\{x\}} = \{\{x\}\}$.

[1]This work has been partially supported by the NSERC grant OGP 9207.

ISSN 1426–2630(p), 1898-9934(e)

Let us observe that there exists a finite sequence which is finite-yielding.

The following proposition is true

(7) Let X be a non empty finite set and P be a partition of X. If $\overline{\overline{P}} < \overline{\overline{X}}$, then there exist sets p, x, y such that $p \in P$ and x, $y \in p$ and $x \neq y$.

Let us note that $\bigcup\{\emptyset\}$ is empty.

Next we state three propositions:

(8) For every set x holds $\bigcup\{\emptyset, \{x\}\} = \{x\}$.

(9) For every set X and for every subset s of X such that s is 1-element there exists a set x such that $x \in X$ and $s = \{x\}$.

(10) For every set X holds $\overline{\overline{\{\{X, \langle x, X\rangle\}; x \text{ ranges over elements of } X\colon x \in X\}}} = \overline{\overline{X}}$.

Let G be a set. The functor PairsOf G yielding a subset of G is defined as follows:

(Def. 1) For every set e holds $e \in \text{PairsOf } G$ iff $e \in G$ and $\overline{e} = 2$.

The following propositions are true:

(11) For every set X and for every set e such that $e \in \text{PairsOf } X$ there exist sets x, y such that $x \neq y$ and x, $y \in \bigcup X$ and $e = \{x, y\}$.

(12) For all sets X, x, y such that $x \neq y$ and $\{x, y\} \in X$ holds $\{x, y\} \in \text{PairsOf } X$.

(13) For all sets X, x, y such that $\{x, y\} \in \text{PairsOf } X$ holds $x \neq y$ and x, $y \in \bigcup X$.

(14) For all sets G, H such that $G \subseteq H$ holds $\text{PairsOf } G \subseteq \text{PairsOf } H$.

(15) For every finite set X holds $\overline{\overline{\{\{x, \langle y, \bigcup X\rangle\}; x \text{ ranges over elements of } \bigcup X, y \text{ ranges over elements of } \bigcup X : \{x, y\} \in \text{PairsOf } X\}}} = 2 \cdot \overline{\overline{\text{PairsOf } X}}$.

(16) For every finite set X holds $\overline{\overline{\{\langle x, y\rangle; x \text{ ranges over elements of } \bigcup X, y \text{ ranges over elements of } \bigcup X : \{x, y\} \in \text{PairsOf } X\}}} = 2 \cdot \overline{\overline{\text{PairsOf } X}}$.

Let X be a finite set. Note that PairsOf X is finite.

Let X be a set. We say that X is void if and only if:

(Def. 2) $X = \{\emptyset\}$.

One can verify that there exists a set which is void.

Let us observe that every set which is void is also finite.

Let G be a void set. Observe that $\bigcup G$ is empty.

Next we state two propositions:

(17) For every set X such that X is void holds $\text{PairsOf } X = \emptyset$.

(18) For every set X such that $\bigcup X = \emptyset$ holds $X = \emptyset$ or $X = \{\emptyset\}$.

Let X be a set. We say that X is pair free if and only if:

(Def. 3) PairsOf X is empty.

We now state the proposition

(19) For all sets X, x such that $\overline{\overline{\bigcup X}} = 1$ holds X is pair free.

Let us observe that there exists a set which is finite-membered and non empty.

Let X be a finite-membered set and let Y be a set. Observe that $X \cap Y$ is finite-membered and $X \setminus Y$ is finite-membered.

2. Simple Graphs as Simplicial Complexes

Let n be a natural number and let X be a set. We say that X is at most n-dimensional if and only if:

(Def. 4) For every set x such that $x \in X$ holds $\overline{\overline{x}} \subseteq n + 1$.

Let n be a natural number. Observe that every set which is at most n-dimensional is also finite-membered.

Let n be a natural number. Observe that there exists a set which is at most n-dimensional, subset-closed, and non empty.

Next we state two propositions:

(20) For every subset-closed non empty set G holds $\emptyset \in G$.

(21) Let n be a natural number, X be an at most n-dimensional set, and x be an element of X. If $x \in X$, then $\overline{\overline{x}} \leq n + 1$.

Let n be a natural number and let X, Y be at most n-dimensional sets. Note that $X \cup Y$ is at most n-dimensional.

Let n be a natural number, let X be an at most n-dimensional set, and let Y be a set. Note that $X \cap Y$ is at most n-dimensional and $X \setminus Y$ is at most n-dimensional.

Let n be a natural number and let X be an at most n-dimensional set. Observe that every at most n-dimensional set is at most n-dimensional.

Let s be a set. We say that s is simple graph-like if and only if:

(Def. 5) s is at most 1-dimensional, subset-closed, and non empty.

Let us note that every set which is simple graph-like is also at most 1-dimensional, subset-closed, and non empty and every set which is at most 1-dimensional, subset-closed, and non empty is also simple graph-like.

The following proposition is true

(22) $\{\emptyset\}$ is simple graph-like.

One can verify that $\{\emptyset\}$ is simple graph-like.

One can verify that there exists a set which is simple graph-like.

A simple graph is a simple graph-like set.

One can verify that there exists a simple graph which is void and there exists a simple graph which is finite.

Let G be a set. We introduce Vertices G as a synonym of $\bigcup G$. We introduce Edges G as a synonym of PairsOf G.

Let X be a set. We introduce X is edgesless as a synonym of X is pair free.

We now state three propositions:

(23) For every simple graph G such that Vertices G is finite holds G is finite.

(24) For every simple graph G and for every set x holds $x \in$ Vertices G iff $\{x\} \in G$.

(25) For every set x holds $\{\emptyset, \{x\}\}$ is a simple graph.

Let X be a finite finite-membered set. The functor order X yielding a natural number is defined by:

(Def. 6) order $X = \overline{\overline{\bigcup X}}$.

Let X be a finite set. The functor size X yielding a natural number is defined by:

(Def. 7) size $X = \overline{\overline{\text{PairsOf } X}}$.

Next we state the proposition

(26) For every finite simple graph G holds order $G \leq \overline{\overline{G}}$.

Let G be a simple graph. A vertex of G is an element of Vertices G. An edge of G is an element of Edges G.

The following propositions are true:

(27) For every simple graph G holds $G = \{\emptyset\} \cup S_{(\text{Vertices } G)} \cup$ Edges G.

(28) For every simple graph G such that Vertices $G = \emptyset$ holds G is void.

(29) Let G be a simple graph and x be a set. If $x \in G$ and $x \neq \emptyset$, then there exists a set y such that $x = \{y\}$ and $y \in$ Vertices G or $x \in$ Edges G.

(30) For every simple graph G and for every set x such that Vertices $G = \{x\}$ holds $G = \{\emptyset, \{x\}\}$.

(31) For every set X there exists a simple graph G such that G is edgesless and Vertices $G = X$.

Let G be a simple graph and let v be an element of Vertices G. The functor Adjacent(v) yielding a subset of Vertices G is defined by:

(Def. 8) For every element x of Vertices G holds $x \in$ Adjacent(v) iff $\{v, x\} \in$ Edges G.

Let X be a set. A simple graph is called a simple graph of X if:

(Def. 9) Vertices it $= X$.

Let X be a set. The functor CompleteSGraph X yields a simple graph of X and is defined by:

(Def. 10) CompleteSGraph $X = \{V; V$ ranges over finite subsets of X: $\overline{\overline{V}} \leq 2\}$.

One can prove the following proposition

(32) For every simple graph G such that for all sets x, y such that x, $y \in$ Vertices G holds $\{x, y\} \in G$ holds $G =$ CompleteSGraph Vertices G.

Let X be a finite set. One can check that CompleteSGraph X is finite.

The following propositions are true:

(33) For every set X and for every set x such that $x \in X$ holds $\{x\} \in$ CompleteSGraph X.

(34) For every set X and for all sets x, y such that x, $y \in X$ holds $\{x, y\} \in$ CompleteSGraph X.

(35) CompleteSGraph $\emptyset = \{\emptyset\}$.

(36) For every set x holds CompleteSGraph$\{x\} = \{\emptyset, \{x\}\}$.

(37) For all sets x, y holds CompleteSGraph$\{x, y\} = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$.

(38) For all sets X, Y such that $X \subseteq Y$ holds CompleteSGraph $X \subseteq$ CompleteSGraph Y.

(39) For every simple graph G and for every set x such that $x \in$ Vertices G holds CompleteSGraph$\{x\} \subseteq G$.

Let G be a simple graph. One can check that there exists a subset of G which is simple graph-like.

Let G be a simple graph. A subgraph of G is a simple graph-like subset of G.

Let G be a simple graph. The functor Complement G yields a simple graph and is defined as follows:

(Def. 11) Complement $G =$ CompleteSGraph Vertices $G \setminus$ Edges G.

Let us observe that the functor Complement G is involutive.

Next we state two propositions:

(40) For every simple graph G holds Vertices $G =$ Vertices Complement G.

(41) Let G be a simple graph and x, y be sets. If $x \neq y$ and x, $y \in$ Vertices G, then $\{x, y\} \in$ Edges G iff $\{x, y\} \notin$ Edges Complement G.

3. Induced Subgraphs

Let G be a simple graph and let L be a set. The subgraph induced by G yielding a subset of G is defined by:

(Def. 12) The subgraph induced by $G = G \cap 2^L$.

Let G be a simple graph and let L be a set. Observe that the subgraph induced by G is simple graph-like.

Next we state two propositions:

(42) For every simple graph G holds $G =$ the subgraph induced by G.

(43) For every simple graph G and for every set L holds the subgraph induced by $G =$ the subgraph induced by G.

Let G be a finite simple graph and let L be a set. Observe that the subgraph induced by G is finite.

Let G be a simple graph and let L be a finite set. One can check that the subgraph induced by G is finite.

One can prove the following three propositions:

(44) For all simple graphs G, H such that $G \subseteq H$ holds $G \subseteq$ the subgraph induced by H.

(45) For every simple graph G and for every set L holds Vertices (the subgraph induced by G) $=$ Vertices $G \cap L$.

(46) For every simple graph G and for every set x such that $x \in$ Vertices G holds the subgraph induced by $G = \{\emptyset, \{x\}\}$.

4. Clique, Clique Number, Clique Cover

Let G be a simple graph. We say that G is a clique if and only if:

(Def. 13) $G =$ CompleteSGraph Vertices G.

The following propositions are true:

(47) Let G be a simple graph. Suppose that for all sets x, y such that $x \neq y$ and x, $y \in$ Vertices G holds $\{x, y\} \in$ Edges G. Then G is a clique.

(48) $\{\emptyset\}$ is a clique.

Observe that there exists a simple graph which is a clique. Let G be a simple graph. Note that there exists a subgraph of G which is a clique.

Let G be a simple graph. A clique of G is a clique subgraph of G.

Next we state the proposition

(49) For every set X holds CompleteSGraph X is a clique.

Let X be a set. One can check that CompleteSGraph X is a clique.

Next we state two propositions:

(50) For every simple graph G and for every set x such that $x \in$ Vertices G holds $\{\emptyset, \{x\}\}$ is a clique of G.

(51) Let G be a simple graph and x, y be sets. If x, $y \in$ Vertices G and $\{x, y\} \in G$, then $\{\emptyset, \{x\}, \{y\}, \{x, y\}\}$ is a clique of G.

Let G be a simple graph. Observe that there exists a clique of G which is finite.

We now state two propositions:

(52) For every simple graph G and for every set x such that $x \in \bigcup G$ there exists a finite clique C of G such that Vertices $C = \{x\}$.

(53) For every a clique simple graph C and for all sets u, v such that u, $v \in$ Vertices C holds $\{u, v\} \in C$.

Let G be a simple graph. We say that G has finite clique number if and only if:

(Def. 14) There exists a finite clique C of G such that for every finite clique D of G holds order $D \leq$ order C.

Let us note that there exists a simple graph which has finite clique number.

Let us observe that every simple graph which is finite also has finite clique number.

Let G be a simple graph with finite clique number. The functor $\omega(G)$ yielding a natural number is defined as follows:

(Def. 15) There exists a finite clique C of G such that order $C = \omega(G)$ and for every finite clique T of G holds order $T \leq \omega(G)$.

We now state several propositions:

(54) For every simple graph G with finite clique number such that $\omega(G) = 0$ holds Vertices $G = \emptyset$.

(55) For every void simple graph G holds $\omega(G) = 0$.

(56) Let G be a simple graph and x, y be sets. If $\{x, y\} \in G$, then the subgraph induced by G is a clique of G.

(57) For every simple graph G with finite clique number such that Edges $G \neq \emptyset$ holds $\omega(G) \geq 2$.

(58) For all simple graphs G, H with finite clique number such that $G \subseteq H$ holds $\omega(G) \leq \omega(H)$.

(59) For every finite set X holds $\omega(\text{CompleteSGraph } X) = \overline{\overline{X}}$.

Let G be a simple graph and let P be a partition of Vertices G. We say that P is clique-wise if and only if:

(Def. 16) For every set x such that $x \in P$ holds the subgraph induced by G is a clique of G.

Let G be a simple graph. Observe that there exists a partition of Vertices G which is clique-wise.

Let G be a simple graph. A clique-partition of G is a clique-wise partition of Vertices G.

Let G be a void simple graph. Note that every partition of Vertices G which is empty is also clique-wise.

Let G be a simple graph. We say that G has finite clique cover if and only if:

(Def. 17) There exists a clique-partition of G which is finite.

One can verify that every simple graph which is finite also has finite clique cover.

Let G be a simple graph with finite clique cover. Note that there exists a clique-partition of G which is finite.

Let G be a simple graph with finite clique cover and let S be a subset of Vertices G. One can verify that the subgraph induced by G has finite clique cover.

Let G be a simple graph with finite clique cover. The functor $\kappa(G)$ yielding a natural number is defined by:

(Def. 18) There exists a finite clique-partition C of G such that $\overline{\overline{C}} = \kappa(G)$ and for every finite clique-partition C of G holds $\kappa(G) \leq \overline{\overline{C}}$.

5. Stable Set, Coloring

Let G be a simple graph and let S be a subset of Vertices G. We say that S is stable if and only if:

(Def. 19) For all sets x, y such that $x \neq y$ and x, $y \in S$ holds $\{x, y\} \notin G$.

We now state two propositions:

(60) For every simple graph G holds $\emptyset_{\text{Vertices } G}$ is stable.

(61) For every simple graph G and for every subset S of Vertices G and for every set v such that $S = \{v\}$ holds S is stable.

Let G be a simple graph. Observe that every subset of Vertices G which is trivial is also stable.

Let G be a simple graph. Note that there exists a subset of Vertices G which is stable.

Let G be a simple graph. A stable set of G is a stable subset of Vertices G.

The following two propositions are true:

(62) For every simple graph G and for all sets x, y such that x, $y \in$ Vertices G and $\{x, y\} \notin G$ holds $\{x, y\}$ is a stable set of G.

(63) For every simple graph G with finite clique number such that $\omega(G) = 1$ holds Vertices G is a stable set of G.

Let G be a simple graph. Note that there exists a stable set of G which is finite.

One can prove the following proposition

(64) For every simple graph G and for every stable set A of G holds every subset of A is a stable set of G.

Let G be a simple graph and let P be a partition of Vertices G. We say that P is stable-wise if and only if:

(Def. 20) For every set x such that $x \in P$ holds x is a stable set of G.

The following proposition is true

(65) For every simple graph G holds SmallestPartition(Vertices G) is stable-wise.

Let G be a simple graph. Note that there exists a partition of Vertices G which is stable-wise. A coloring of G is a stable-wise partition of Vertices G. We say that G is finitely colorable if and only if:

(Def. 21) There exists a coloring of G which is finite.

One can verify that there exists a simple graph which is finitely colorable.

Let us note that every simple graph which is finite is also finitely colorable.

Let G be a finitely colorable simple graph. Note that there exists a coloring of G which is finite.

We now state two propositions:

(66) Let G be a simple graph, S be a clique of G, and L be a set. If $L \subseteq$ Vertices S, then the subgraph induced by G is a clique of G.

(67) Let G be a simple graph, C be a coloring of G, and S be a subset of Vertices G. Then $C\restriction S$ is a coloring of the subgraph induced by G.

Let G be a finitely colorable simple graph and let S be a set. One can check that the subgraph induced by G is finitely colorable. The functor $\chi(G)$ yielding a natural number is defined as follows:

(Def. 22) There exists a finite coloring C of G such that $\overline{\overline{C}} = \chi(G)$ and for every finite coloring C of G holds $\chi(G) \leq \overline{\overline{C}}$.

One can prove the following three propositions:

(68) For all finitely colorable simple graphs G, H such that $G \subseteq H$ holds $\chi(G) \leq \chi(H)$.

(69) For every finite set X holds $\chi(\text{CompleteSGraph}\, X) = \overline{\overline{X}}$.

(70) Let G be a finitely colorable simple graph, C be a finite coloring of G, and c be a set. Suppose $c \in C$ and $\overline{\overline{C}} = \chi(G)$. Then there exists an element v of Vertices G such that $v \in c$ and for every element d of C such that $d \neq c$ there exists an element w of Vertices G such that $w \in \text{Adjacent}(v)$ and $w \in d$.

Let G be a simple graph. We say that G has finite stability number if and only if:

(Def. 23) There exists a finite stable set A of G such that for every finite stable set B of G holds $\overline{\overline{B}} \leq \overline{\overline{A}}$.

One can check that every simple graph which is finite also has finite stability number.

Let G be a simple graph with finite stability number. Observe that every stable set of G is finite.

Let us note that there exists a simple graph which is non void and has finite stability number.

Let G be a simple graph with finite stability number. The functor $\alpha(G)$ yielding a natural number is defined as follows:

(Def. 24) There exists a finite stable set A of G such that $\overline{\overline{A}} = \alpha(G)$ and for every finite stable set T of G holds $\overline{\overline{T}} \leq \alpha(G)$.

Let G be a non void simple graph with finite stability number. One can check that $\alpha(G)$ is positive.

Next we state the proposition

(71) For every simple graph G with finite stability number such that $\alpha(G) = 1$ holds G is a clique.

Let us observe that every simple graph which has finite clique number and finite stability number is also finite.

We now state four propositions:

(72) For every simple graph G and for every clique C of G holds Vertices C is a stable set of Complement G.

(73) For every simple graph G and for every clique C of Complement G holds Vertices C is a stable set of G.

(74) For every simple graph G and for every stable set C of G holds the subgraph induced by Complement G is a clique of Complement G.

(75) For every simple graph G and for every stable set C of Complement G holds the subgraph induced by G is a clique of G.

Let G be a simple graph with finite clique number. One can check that Complement G has finite stability number.

Let G be a simple graph with finite stability number. Note that Complement G has finite clique number.

We now state several propositions:

(76) For every simple graph G with finite clique number holds $\omega(G) = \alpha(\text{Complement } G)$.

(77) For every simple graph G with finite stability number holds $\alpha(G) = \omega(\text{Complement } G)$.

(78) For every simple graph G holds every clique-partition of Complement G is a coloring of G.

(79) For every simple graph G holds every clique-partition of G is a coloring of Complement G.

(80) For every simple graph G holds every coloring of G is a clique-partition of Complement G.

(81) For every simple graph G holds every coloring of Complement G is a clique-partition of G.

Let G be a finitely colorable simple graph. One can check that Complement G has finite clique cover.

Let G be a simple graph with finite clique cover.

One can check that Complement G is finitely colorable.

One can prove the following propositions:

(82) For every finitely colorable simple graph G holds $\chi(G) = \kappa(\text{Complement } G)$.

(83) For every simple graph G with finite clique cover holds $\kappa(G) = \chi(\text{Complement } G)$.

6. Mycielskian of a Graph

Let G be a simple graph. The functor Mycielskian G yielding a simple graph is defined by the condition (Def. 25).

(Def. 25) Mycielskian $G = \{\emptyset\} \cup \{\{x\} : x \text{ ranges over elements of } \bigcup G \cup \bigcup G \times \{\bigcup G\} \cup \{\bigcup G\}\} \cup \text{Edges } G \cup \{\{x, \langle y, \bigcup G\rangle\}; x \text{ ranges over elements of } \bigcup G, y \text{ ranges over elements of } \bigcup G : \{x, y\} \in \text{Edges } G\} \cup \{\{\bigcup G, \langle x, \bigcup G\rangle\}; x \text{ ranges over elements of } \bigcup G : x \in \text{Vertices } G\}$.

We now state several propositions:

(84) For every simple graph G holds $G \subseteq$ Mycielskian G.

(85) Let G be a simple graph and v be a set. Then $v \in$ Vertices Mycielskian G if and only if one of the following conditions is satisfied:

(i) $v \in \bigcup G$, or

(ii) there exists a set x such that $x \in \bigcup G$ and $v = \langle x, \bigcup G\rangle$, or

(iii) $v = \bigcup G$.

(86) For every simple graph G holds Vertices Mycielskian $G = \bigcup G \cup \bigcup G \times \{\bigcup G\} \cup \{\bigcup G\}$.

(87) For every simple graph G holds $\bigcup G \in \bigcup$ Mycielskian G.

(88) For every void simple graph G holds Mycielskian $G = \{\emptyset, \{\bigcup G\}\}$.

Let G be a finite simple graph. Note that Mycielskian G is finite.

The following propositions are true:

(89) For every finite simple graph G holds order Mycielskian $G = 2 \cdot \text{order } G + 1$.

(90) Let G be a simple graph and e be a set. Then $e \in$ Edges Mycielskian G if and only if one of the following conditions is satisfied:

(i) $e \in$ Edges G, or

(ii) there exist elements x, y of $\bigcup G$ such that $e = \{x, \langle y, \bigcup G\rangle\}$ and $\{x, y\} \in$ Edges G, or

(iii) there exists an element y of $\bigcup G$ such that $e = \{\bigcup G, \langle y, \bigcup G\rangle\}$ and $y \in \bigcup G$.

(91) Let G be a simple graph. Then Edges Mycielskian $G = \text{Edges } G \cup \{\{x, \langle y, \bigcup G\rangle\}; x \text{ ranges over elements of } \bigcup G, y \text{ ranges over elements of } \bigcup G : \{x, y\} \in \text{Edges } G\} \cup \{\{\bigcup G, \langle y, \bigcup G\rangle\}; y \text{ ranges over elements of } \bigcup G : y \in \bigcup G\}$.

(92) For every finite simple graph G holds size Mycielskian $G = 3 \cdot$ size $G +$ order G.

(93) Let G be a simple graph and s, t be sets. Suppose $\{s, t\} \in$ Edges Mycielskian G. Then

(i) $\{s, t\} \in$ Edges G, or

(ii) $s \in \bigcup G$ or $s = \bigcup G$ but there exists a set y such that $y \in \bigcup G$ and $t = \langle y, \bigcup G \rangle$, or

(iii) $t \in \bigcup G$ or $t = \bigcup G$ but there exists a set y such that $y \in \bigcup G$ and $s = \langle y, \bigcup G \rangle$.

(94) For every simple graph G and for every set u such that $\{\bigcup G, u\} \in$ Edges Mycielskian G there exists a set x such that $x \in \bigcup G$ and $u = \langle x, \bigcup G \rangle$.

(95) For every simple graph G and for every set u such that $u \in$ Vertices G holds $\{\langle u, \bigcup G \rangle\} \in$ Mycielskian G.

(96) For every simple graph G and for every set u such that $u \in$ Vertices G holds $\{\langle u, \bigcup G \rangle, \bigcup G\} \in$ Mycielskian G.

(97) For every simple graph G and for all sets x, y holds $\{\langle x, \bigcup G \rangle, \langle y, \bigcup G \rangle\} \notin$ Edges Mycielskian G.

(98) For every simple graph G and for all sets x, y such that $x \neq y$ holds $\{\langle x, \bigcup G \rangle, \langle y, \bigcup G \rangle\} \notin$ Mycielskian G.

(99) For every simple graph G and for all sets x, y such that $\{\langle x, \bigcup G \rangle, y\} \in$ Edges Mycielskian G holds $x \neq y$ but $x \in \bigcup G$ but $y \in \bigcup G$ or $y = \bigcup G$.

(100) For every simple graph G and for all sets x, y such that $\{\langle x, \bigcup G \rangle, y\} \in$ Mycielskian G holds $x \neq y$.

(101) For every simple graph G and for all sets x, y such that $y \in \bigcup G$ and $\{\langle x, \bigcup G \rangle, y\} \in$ Mycielskian G holds $\{x, y\} \in G$.

(102) For every simple graph G and for all sets x, y such that $\{x, y\} \in$ Edges G holds $\{\langle x, \bigcup G \rangle, y\} \in$ Mycielskian G.

(103) For every simple graph G and for all sets x, y such that x, $y \in$ Vertices G and $\{x, y\} \in$ Mycielskian G holds $\{x, y\} \in G$.

(104) For every simple graph G holds $G =$ the subgraph induced by Mycielskian G.

(105) Let G be a simple graph and C be a finite clique of Mycielskian G. If $3 \leq$ order C, then for every vertex v of C holds $v \neq \bigcup G$.

(106) For every simple graph G with finite clique number such that $\omega(G) = 0$ and for every finite clique D of Mycielskian G holds order $D \leq 1$.

(107) For every simple graph G and for every set x such that Vertices $G = \{x\}$ holds Mycielskian $G = \{\emptyset, \{x\}, \{\langle x, \bigcup G \rangle\}, \{\bigcup G\}, \{\langle x, \bigcup G \rangle, \bigcup G\}\}$.

(108) For every simple graph G with finite clique number such that $\omega(G) = 1$

and for every finite clique D of Mycielskian G holds order $D \leq 2$.

(109) For every simple graph G with finite clique number such that $2 \leq \omega(G)$ and for every finite clique D of Mycielskian G holds order $D \leq \omega(G)$.

Let G be a simple graph with finite clique number. Note that Mycielskian G has finite clique number.

We now state two propositions:

(110) For every simple graph G with finite clique number such that $2 \leq \omega(G)$ holds $\omega(\text{Mycielskian } G) = \omega(G)$.

(111) For every finitely colorable simple graph G there exists a coloring E of Mycielskian G such that $\overline{\overline{E}} = 1 + \chi(G)$.

Let G be a finitely colorable simple graph. Observe that Mycielskian G is finitely colorable.

We now state the proposition

(112) For every finitely colorable simple graph G holds $\chi(\text{Mycielskian } G) = 1 + \chi(G)$.

Let G be a simple graph. The Mycielskian sequence of G yields a many sorted set indexed by $\mathbb{N}$ and is defined by the condition (Def. 26).

(Def. 26) There exists a function m_1 such that

(i) the Mycielskian sequence of $G = m_1$,

(ii) $m_1(0) = G$, and

(iii) for every natural number k and for every simple graph G such that $G = m_1(k)$ holds $m_1(k+1) = \text{Mycielskian } G$.

We now state two propositions:

(113) For every simple graph G holds (the Mycielskian sequence of G)$(0) = G$.

(114) Let G be a simple graph and n be a natural number. Then (the Mycielskian sequence of G)(n) is a simple graph.

Let G be a simple graph and let n be a natural number. Observe that (the Mycielskian sequence of G)(n) is simple graph-like.

The following proposition is true

(115) Let G, H be simple graphs and n be a natural number. Then (the Mycielskian sequence of G)$(n+1) =$ Mycielskian (the Mycielskian sequence of G)(n).

Let G be a simple graph with finite clique number and let n be a natural number. One can check that (the Mycielskian sequence of G)(n) has finite clique number.

Let G be a finitely colorable simple graph and let n be a natural number. One can check that (the Mycielskian sequence of G)(n) is finitely colorable.

Let G be a finite simple graph and let n be a natural number. Observe that (the Mycielskian sequence of G)(n) is finite.

One can prove the following propositions:

(116) Let G be a finite simple graph and n be a natural number. Then order (the Mycielskian sequence of G)$(n) = (2^n \cdot \operatorname{order} G + 2^n) - 1$.

(117) Let G be a finite simple graph and n be a natural number. Then size (the Mycielskian sequence of G)$(n) = 3^n \cdot \operatorname{size} G + (3^n - 2^n) \cdot \operatorname{order} G + ((n + 1)\operatorname{block} 3)$.

(118) Let n be a natural number. Then ω((the Mycielskian sequence of CompleteSGraph 2)$(n)) = 2$ and χ((the Mycielskian sequence of CompleteSGraph 2)$(n)) = n + 2$.

(119) For every natural number n there exists a finite simple graph G such that $\omega(G) = 2$ and $\chi(G) > n$.

(120) For every natural number n there exists a finite simple graph G such that $\alpha(G) = 2$ and $\kappa(G) > n$.

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. Tarski's classes and ranks. *Formalized Mathematics*, 1(**3**):563–567, 1990.
[5] Grzegorz Bancerek. Mizar analysis of algorithms: Preliminaries. *Formalized Mathematics*, 15(**3**):87–110, 2007, doi:10.2478/v10037-007-0011-x.
[6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[9] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[10] Frank Harary. *Graph theory*. Addison-Wesley, 1969.
[11] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[12] J. Mycielski. Sur le coloriage des graphes. *Colloquium Mathematicum*, 3:161–162, 1955.
[13] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[14] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.
[15] Piotr Rudnicki and Lorna Stewart. The Mycielskian of a graph. *Formalized Mathematics*, 19(**1**):27–34, 2011, doi: 10.2478/v10037-011-0005-6.
[16] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[17] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[18] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.
[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[20] Oswald Veblen. *Analysis Situs*, volume V. AMS Colloquium Publications, 1931.

Received February 7, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 2, Pages 175–179, 2012
DOI: 10.2478/v10037-012-0020-2

VERSITA
versita.com/fm/

Extended Euclidean Algorithm and CRT Algorithm[1]

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yosiki Aoki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article we formalize some number theoretical algorithms, Euclidean Algorithm and Extended Euclidean Algorithm [9]. Besides the a gcd b, Extended Euclidean Algorithm can calculate a pair of two integers (x, y) that holds $ax + by = a$ gcd b. In addition, we formalize an algorithm that can compute a solution of the Chinese remainder theorem by using Extended Euclidean Algorithm. Our aim is to support the implementation of number theoretic tools. Our formalization of those algorithms is based on the source code of the NZMATH, a number theory oriented calculation system developed by Tokyo Metropolitan University [8].

MML identifier: `NTALGO_1`, version: `7.12.02 4.181.1147`

The terminology and notation used in this paper have been introduced in the following papers: [3], [4], [5], [12], [10], [11], [1], [2], [7], [13], and [6].

1. Euclidean Algorithm

One can prove the following proposition

(1) For all integers x, p holds $x \bmod p \bmod p = x \bmod p$.

Let a, b be elements of $\mathbb{Z}$. The functor $\mathrm{ALGO}_{\mathrm{GCD}}(a, b)$ yielding an element of $\mathbb{N}$ is defined by the condition (Def. 1).

(Def. 1) There exist sequences A, B of $\mathbb{N}$ such that

(i) $A(0) = |a|$,

(ii) $B(0) = |b|$,

[1]This work was supported by JSPS KAKENHI 21240001 and 22300285.

ISSN 1426–2630(p), 1898-9934(e)

(iii) for every element i of $\mathbb{N}$ holds $A(i+1) = B(i)$ and $B(i+1) = A(i) \bmod B(i)$, and

(iv) $\mathrm{ALGO}_{\mathrm{GCD}}(a, b) = A(\min^*\{i \in \mathbb{N}\colon B(i) = 0\})$.

Next we state the proposition

(2) For all elements a, b of $\mathbb{Z}$ holds $\mathrm{ALGO}_{\mathrm{GCD}}(a, b) = a \gcd b$.

2. Extended Euclidean Algorithm

The scheme *QuadChoiceRec* deals with non empty sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$, an element $\mathcal{E}$ of $\mathcal{A}$, an element $\mathcal{F}$ of $\mathcal{B}$, an element $\mathcal{G}$ of $\mathcal{C}$, an element $\mathcal{H}$ of $\mathcal{D}$, and a 9-ary predicate $\mathcal{P}$, and states that:

> There exists a function f from $\mathbb{N}$ into $\mathcal{A}$ and there exists a function g from $\mathbb{N}$ into $\mathcal{B}$ and there exists a function h from $\mathbb{N}$ into $\mathcal{C}$ and there exists a function i from $\mathbb{N}$ into $\mathcal{D}$ such that $f(0) = \mathcal{E}$ and $g(0) = \mathcal{F}$ and $h(0) = \mathcal{G}$ and $i(0) = \mathcal{H}$ and for every element n of $\mathbb{N}$ holds $\mathcal{P}[n, f(n), g(n), h(n), i(n), f(n+1), g(n+1), h(n+1), i(n+1)]$

provided the parameters satisfy the following condition:

- Let n be an element of $\mathbb{N}$, x be an element of $\mathcal{A}$, y be an element of $\mathcal{B}$, z be an element of $\mathcal{C}$, and w be an element of $\mathcal{D}$. Then there exists an element x_1 of $\mathcal{A}$ and there exists an element y_1 of $\mathcal{B}$ and there exists an element z_1 of $\mathcal{C}$ and there exists an element w_1 of $\mathcal{D}$ such that $\mathcal{P}[n, x, y, z, w, x_1, y_1, z_1, w_1]$.

Let x, y be elements of $\mathbb{Z}$. The functor $\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y)$ yielding an element of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is defined by the condition (Def. 2).

(Def. 2) There exist sequences g, w, q, t of $\mathbb{Z}$ and there exist sequences a, b, v, u of $\mathbb{Z}$ and there exists an element i_1 of $\mathbb{N}$ such that $a(0) = 1$ and $b(0) = 0$ and $g(0) = x$ and $q(0) = 0$ and $u(0) = 0$ and $v(0) = 1$ and $w(0) = y$ and $t(0) = 0$ and for every element i of $\mathbb{N}$ holds $q(i+1) = g(i) \operatorname{div} w(i)$ and $t(i+1) = g(i) \bmod w(i)$ and $a(i+1) = u(i)$ and $b(i+1) = v(i)$ and $g(i+1) = w(i)$ and $u(i+1) = a(i) - q(i+1) \cdot u(i)$ and $v(i+1) = b(i) - q(i+1) \cdot v(i)$ and $w(i+1) = t(i+1)$ and $i_1 = \min^*\{i \in \mathbb{N}\colon w(i) = 0\}$ and if $0 \leq g(i_1)$, then $\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y) = \langle a(i_1), b(i_1), g(i_1)\rangle$ and if $g(i_1) < 0$, then $\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y) = \langle -a(i_1), -b(i_1), -g(i_1)\rangle$.

One can prove the following propositions:

(3) For all integers i_3, i_2 such that $i_3 \leq 0$ holds $i_2 \bmod i_3 \leq 0$.

(4) For all integers i_3, i_2 such that $i_3 < 0$ holds $-(i_2 \bmod i_3) < -i_3$.

(5) For all elements x, y of $\mathbb{Z}$ such that $|y| \neq 0$ holds $|x \bmod y| < |y|$.

(6) For all elements x, y of $\mathbb{Z}$ holds $(\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y))_{\mathbf{3},3} = x \gcd y$ and $(\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y))_{\mathbf{1},3} \cdot x + (\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y))_{\mathbf{2},3} \cdot y = x \gcd y$.

Let x, p be elements of $\mathbb{Z}$. The functor $\mathrm{ALGO}_{\mathrm{INVERSE}}(x,p)$ yielding an element of $\mathbb{Z}$ is defined by the condition (Def. 3).

(Def. 3) Let y be an element of $\mathbb{Z}$ such that $y = x \bmod p$. Then

(i) if $(\mathrm{ALGO}_{\mathrm{EXGCD}}(p,y))_{\mathbf{3},3} = 1$, then if $(\mathrm{ALGO}_{\mathrm{EXGCD}}(p,y))_{\mathbf{2},3} < 0$, then there exists an element z of $\mathbb{Z}$ such that $z = (\mathrm{ALGO}_{\mathrm{EXGCD}}(p,y))_{\mathbf{2},3}$ and $\mathrm{ALGO}_{\mathrm{INVERSE}}(x,p) = p + z$ and if $0 \leq (\mathrm{ALGO}_{\mathrm{EXGCD}}(p,y))_{\mathbf{2},3}$, then $\mathrm{ALGO}_{\mathrm{INVERSE}}(x,p) = (\mathrm{ALGO}_{\mathrm{EXGCD}}(p,y))_{\mathbf{2},3}$, and

(ii) if $(\mathrm{ALGO}_{\mathrm{EXGCD}}(p,y))_{\mathbf{3},3} \neq 1$, then $\mathrm{ALGO}_{\mathrm{INVERSE}}(x,p) = \emptyset$.

Next we state the proposition

(7) For all elements x, p, y of $\mathbb{Z}$ such that $y = x \bmod p$ and $(\mathrm{ALGO}_{\mathrm{EXGCD}}(p,y))_{\mathbf{3},3} = 1$ holds $\mathrm{ALGO}_{\mathrm{INVERSE}}(x,p) \cdot x \bmod p = 1 \bmod p$.

3. CRT Algorithm

Let n_1 be a non empty finite sequence of elements of $\mathbb{Z} \times \mathbb{Z}$. The functor $\mathrm{ALGO}_{\mathrm{CRT}}\, n_1$ yielding an element of $\mathbb{Z}$ is defined by the conditions (Def. 4).

(Def. 4)(i) If $\operatorname{len} n_1 = 1$, then $\mathrm{ALGO}_{\mathrm{CRT}}\, n_1 = n_1(1)_{\mathbf{1}}$, and

(ii) if $\operatorname{len} n_1 \neq 1$, then there exist finite sequences m, n, p_1, p_2 of elements of $\mathbb{Z}$ and there exist elements M_0, M of $\mathbb{Z}$ such that $\operatorname{len} m = \operatorname{len} n_1$ and $\operatorname{len} n = \operatorname{len} n_1$ and $\operatorname{len} p_1 = \operatorname{len} n_1 - 1$ and $\operatorname{len} p_2 = \operatorname{len} n_1 - 1$ and $m(1) = 1$ and for every natural number i such that $1 \leq i \leq \operatorname{len} m - 1$ there exist elements d, x, y of $\mathbb{Z}$ such that $x = n_1(i)_{\mathbf{2}}$ and $m(i+1) = m(i) \cdot x$ and $y = m(i+1)$ and $d = n_1(i+1)_{\mathbf{2}}$ and $p_2(i) = \mathrm{ALGO}_{\mathrm{INVERSE}}(y,d)$ and $p_1(i) = y$ and $M_0 = n_1(\operatorname{len} m)_{\mathbf{2}}$ and $M = p_1(\operatorname{len} m - 1) \cdot M_0$ and $n(1) = n_1(1)_{\mathbf{1}}$ and for every natural number i such that $1 \leq i \leq \operatorname{len} m - 1$ there exist elements u, u_0, u_1 of $\mathbb{Z}$ such that $u_0 = n_1(i+1)_{\mathbf{1}}$ and $u_1 = n_1(i+1)_{\mathbf{2}}$ and $u = (u_0 - n(i)) \cdot p_2(i) \bmod u_1$ and $n(i+1) = n(i) + u \cdot p_1(i)$ and $\mathrm{ALGO}_{\mathrm{CRT}}\, n_1 = n(\operatorname{len} m) \bmod M$.

One can prove the following propositions:

(8) For all elements a, b of $\mathbb{Z}$ such that $b \neq 0$ holds $a \bmod b \equiv a \pmod b$.

(9) For all elements a, b of $\mathbb{Z}$ such that $b \neq 0$ holds $a \bmod b \gcd b = a \gcd b$.

(10) Let a, b, c be elements of $\mathbb{Z}$. Suppose $c \neq 0$ and $a = b \bmod c$ and b and c are relative prime. Then a and c are relative prime.

(11) Let n_1 be a non empty finite sequence of elements of $\mathbb{Z} \times \mathbb{Z}$ and a, b be finite sequences of elements of $\mathbb{Z}$. Suppose that

(i) $\operatorname{len} a = \operatorname{len} b$,

(ii) $\operatorname{len} a = \operatorname{len} n_1$,

(iii) for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} n_1$ holds $b(i) \neq 0$,

(iv) for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} n_1$ holds $n_1(i)_{\mathbf{1}} = a(i)$ and $n_1(i)_{\mathbf{2}} = b(i)$, and

(v) for all natural numbers i, j such that i, $j \in \operatorname{Seg}\operatorname{len} n_1$ and $i \neq j$ holds $b(i)$ and $b(j)$ are relative prime.

Let i be a natural number. If $i \in \operatorname{Seg}\operatorname{len} n_1$, then $\operatorname{ALGO}_{\mathrm{CRT}}\, n_1 \bmod b(i) = a(i) \bmod b(i)$.

(12) Let x, y be elements of $\mathbb{Z}$ and b, m be non empty finite sequences of elements of $\mathbb{Z}$. Suppose that

(i) $2 \leq \operatorname{len} b$,

(ii) for all natural numbers i, j such that i, $j \in \operatorname{Seg}\operatorname{len} b$ and $i \neq j$ holds $b(i)$ and $b(j)$ are relative prime,

(iii) for every natural number i such that $i \in \operatorname{Seg}\operatorname{len} b$ holds $x \bmod b(i) = y \bmod b(i)$, and

(iv) $m(1) = 1$.

Let k be an element of $\mathbb{N}$. Suppose $1 \leq k \leq \operatorname{len} b$ and for every natural number i such that $1 \leq i \leq k$ holds $m(i+1) = m(i) \cdot b(i)$. Then $x \bmod m(k+1) = y \bmod m(k+1)$.

(13) For every finite sequence b of elements of $\mathbb{Z}$ such that $\operatorname{len} b = 1$ holds $\prod b = b(1)$.

(14) Let b be a finite sequence of elements of $\mathbb{Z}$. Then there exists a non empty finite sequence m of elements of $\mathbb{Z}$ such that $\operatorname{len} m = \operatorname{len} b + 1$ and $m(1) = 1$ and for every natural number i such that $1 \leq i \leq \operatorname{len} b$ holds $m(i+1) = m(i) \cdot b(i)$ and $\prod b = m(\operatorname{len} b + 1)$.

(15) Let n_1 be a non empty finite sequence of elements of $\mathbb{Z} \times \mathbb{Z}$, a, b be non empty finite sequences of elements of $\mathbb{Z}$, and x, y be elements of $\mathbb{Z}$. Suppose that $\operatorname{len} a = \operatorname{len} b$ and $\operatorname{len} a = \operatorname{len} n_1$ and for every natural number i such that $i \in \operatorname{Seg}\operatorname{len} n_1$ holds $b(i) \neq 0$ and for every natural number i such that $i \in \operatorname{Seg}\operatorname{len} n_1$ holds $n_1(i)_{\mathbf{1}} = a(i)$ and $n_1(i)_{\mathbf{2}} = b(i)$ and for all natural numbers i, j such that i, $j \in \operatorname{Seg}\operatorname{len} n_1$ and $i \neq j$ holds $b(i)$ and $b(j)$ are relative prime and for every natural number i such that $i \in \operatorname{Seg}\operatorname{len} n_1$ holds $x \bmod b(i) = a(i) \bmod b(i)$ and $y = \prod b$. Then $\operatorname{ALGO}_{\mathrm{CRT}}\, n_1 \bmod y = x \bmod y$.

References

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

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

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

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

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

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

[7] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[8] NZMATH development Group. `http://tnt.math.se.tmu.ac.jp/nzmath/`.
[9] Donald E. Knuth. *Art of Computer Programming*. Volume 2: Seminumerical Algorithms, 3rd Edition, Addison-Wesley Professional, 1997.
[10] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[11] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[12] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[13] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received February 8, 2012

FORMALIZED MATHEMATICS
Vol. 20, No. 2, Pages 181–191, 2012
DOI: 10.2478/v10037-012-0021-1

VERSITA
versita.com/fm/

Introduction to Rational Functions

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

Summary. In this article we formalize rational functions as pairs of polynomials and define some basic notions including the degree and evaluation of rational functions [8]. The main goal of the article is to provide properties of rational functions necessary to prove a theorem on the stability of networks.

MML identifier: `RATFUNC1`, version: `7.12.02 4.181.1147`

The notation and terminology used in this paper are introduced in the following articles: [14], [3], [4], [5], [18], [20], [16], [17], [1], [15], [2], [6], [12], [10], [11], [22], [19], [21], [9], [13], [23], and [7].

1. Preliminaries

One can prove the following three propositions:

(1) Let L be an add-associative right zeroed right complementable right distributive non empty double loop structure, a be an element of L, and p, q be finite sequences of elements of L. Suppose $\operatorname{len} p = \operatorname{len} q$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} p$ holds $q_i = a \cdot p_i$. Then $\sum q = a \cdot \sum p$.

(2) Let L be an add-associative right zeroed right complementable right distributive non empty double loop structure, f be a finite sequence of elements of L, and i, j be elements of $\mathbb{N}$. If $i \in \operatorname{dom} f$ and $j = i - 1$, then $\operatorname{Ins}(f_{\restriction i}, j, f_i) = f$.

(3) Let L be an add-associative right zeroed right complementable associative unital right distributive commutative non empty double loop structure, f be a finite sequence of elements of L, and i be an element of $\mathbb{N}$. If $i \in \operatorname{dom} f$, then $\prod f = f_i \cdot \prod(f_{\restriction i})$.

ISSN 1426–2630(p), 1898-9934(e)

Let L be an add-associative right zeroed right complementable well unital associative left distributive commutative almost left invertible integral domain-like non trivial double loop structure and let x, y be non zero elements of L. Note that $\frac{x}{y}$ is non zero.

Let us note that every add-associative right zeroed right complementable right distributive non empty double loop structure which is integral domain-like is also almost left cancelable and every add-associative right zeroed right complementable left distributive non empty double loop structure which is integral domain-like is also almost right cancelable.

Let x, y be integers. Note that $\max(x, y)$ is integer and $\min(x, y)$ is integer.

One can prove the following proposition

(4) For all integers x, y, z holds $\max(x + y, x + z) = x + \max(y, z)$.

2. More on Polynomials

Let L be a non empty zero structure and let p be a polynomial of L. We say that p is zero if and only if:

(Def. 1) $p = \mathbf{0}.L$.

We say that p is constant if and only if:

(Def. 2) $\deg p \leq 0$.

Let L be a non trivial zero structure. One can verify that there exists a polynomial of L which is non zero.

Let L be a non empty zero structure. One can verify that $\mathbf{0}.L$ is zero and constant.

Let L be a non degenerated multiplicative loop with zero structure. Note that $\mathbf{1}.L$ is non zero.

Let L be a non empty multiplicative loop with zero structure. Note that $\mathbf{1}.L$ is constant.

Let L be a non empty zero structure. One can verify that every polynomial of L which is zero is also constant. Note that every polynomial of L which is non constant is also non zero.

Let L be a non trivial zero structure. One can verify that there exists a polynomial of L which is non constant.

Let L be a well unital non degenerated non empty double loop structure, let z be an element of L, and let k be an element of $\mathbb{N}$. Observe that $\mathrm{rpoly}(k, z)$ is non zero.

Let L be an add-associative right zeroed right complementable distributive non degenerated double loop structure. One can check that Polynom-Ring L is non degenerated.

Let L be an integral domain-like add-associative right zeroed right complementable distributive non trivial double loop structure. Observe that Polynom-Ring L is integral domain-like.

Next we state two propositions:

(5) Let L be an add-associative right zeroed right complementable right distributive associative non empty double loop structure, p, q be polynomials of L, and a be an element of L. Then $(a \cdot p) * q = a \cdot (p * q)$.

(6) Let L be an add-associative right zeroed right complementable right distributive commutative associative non empty double loop structure, p, q be polynomials of L, and a be an element of L. Then $p*(a \cdot q) = a \cdot (p*q)$.

Let L be an add-associative right zeroed right complementable well unital commutative associative distributive almost left invertible non trivial double loop structure, let p be a non zero polynomial of L, and let a be a non zero element of L. Note that $a \cdot p$ is non zero.

Let L be an integral domain-like add-associative right zeroed right complementable distributive non trivial double loop structure and let p_1, p_2 be non zero polynomials of L. Observe that $p_1 * p_2$ is non zero.

One can prove the following proposition

(7) Let L be an add-associative right zeroed right complementable distributive Abelian integral domain-like non trivial double loop structure, p_1, p_2 be polynomials of L, and p_3 be a non zero polynomial of L. If $p_1 * p_3 = p_2 * p_3$, then $p_1 = p_2$.

Let L be a non trivial zero structure and let p be a non zero polynomial of L. One can check that degree(p) is natural.

Next we state several propositions:

(8) Let L be an add-associative right zeroed right complementable unital right distributive non empty double loop structure and p be a polynomial of L. If $\deg p = 0$, then for every element x of L holds $\mathrm{eval}(p, x) \neq 0_L$.

(9) Let L be an Abelian add-associative right zeroed right complementable well unital associative commutative distributive almost left invertible non degenerated double loop structure, p be a polynomial of L, and x be an element of L. Then $\mathrm{eval}(p, x) = 0_L$ if and only if $\mathrm{rpoly}(1, x) \mid p$.

(10) Let L be an Abelian add-associative right zeroed right complementable well unital associative commutative distributive almost left invertible integral domain-like non degenerated double loop structure, p, q be polynomials of L, and x be an element of L. If $\mathrm{rpoly}(1, x) \mid p * q$, then $\mathrm{rpoly}(1, x) \mid p$ or $\mathrm{rpoly}(1, x) \mid q$.

(11) Let L be an Abelian add-associative right zeroed right complementable well unital associative commutative distributive almost left invertible non degenerated double loop structure and f be a finite sequence of elements

of Polynom-Ring L. Suppose that for every natural number i such that $i \in \operatorname{dom} f$ there exists an element z of L such that $f(i) = \operatorname{rpoly}(1, z)$. Let p be a polynomial of L. If $p = \prod f$, then $p \neq \mathbf{0}.\, L$.

(12) Let L be an Abelian add-associative right zeroed right complementable well unital associative commutative distributive almost left invertible integral domain-like non degenerated double loop structure and f be a finite sequence of elements of Polynom-Ring L. Suppose that for every natural number i such that $i \in \operatorname{dom} f$ there exists an element z of L such that $f(i) = \operatorname{rpoly}(1, z)$. Let p be a polynomial of L. Suppose $p = \prod f$. Let x be an element of L. Then $\operatorname{eval}(p, x) = 0_L$ if and only if there exists a natural number i such that $i \in \operatorname{dom} f$ and $f(i) = \operatorname{rpoly}(1, x)$.

3. Common Roots of Polynomials

Let L be a unital non empty double loop structure, let p_1, p_2 be polynomials of L, and let x be an element of L. We say that x is a common root of p_1 and p_2 if and only if:

(Def. 3) x is a root of p_1 and x is a root of p_2.

Let L be a unital non empty double loop structure and let p_1, p_2 be polynomials of L. We say that p_1 and p_2 have a common root if and only if:

(Def. 4) There exists an element of L which is a common root of p_1 and p_2.

Let L be a unital non empty double loop structure and let p_1, p_2 be polynomials of L. We introduce p_1 and p_2 have common roots as a synonym of p_1 and p_2 have a common root. We introduce p_1 and p_2 have no common roots as an antonym of p_1 and p_2 have a common root.

Next we state several propositions:

(13) Let L be an Abelian add-associative right zeroed right complementable unital distributive non empty double loop structure, p be a polynomial of L, and x be an element of L. If x is a root of p, then x is a root of $-p$.

(14) Let L be an Abelian add-associative right zeroed right complementable unital left distributive non empty double loop structure, p_1, p_2 be polynomials of L, and x be an element of L. If x is a common root of p_1 and p_2, then x is a root of $p_1 + p_2$.

(15) Let L be an Abelian add-associative right zeroed right complementable unital distributive non empty double loop structure, p_1, p_2 be polynomials of L, and x be an element of L. If x is a common root of p_1 and p_2, then x is a root of $-(p_1 + p_2)$.

(16) Let L be an Abelian add-associative right zeroed right complementable unital distributive non empty double loop structure, p, q be polynomials

of L, and x be an element of L. If x is a common root of p and q, then x is a root of $p + q$.

(17) Let L be an Abelian add-associative right zeroed right complementable well unital associative commutative distributive almost left invertible non trivial double loop structure and p_1, p_2 be polynomials of L. If $p_1 \mid p_2$ and p_1 has roots, then p_1 and p_2 have common roots.

Let L be a unital non empty double loop structure and let p, q be polynomials of L. The common roots of p and q yields a subset of L and is defined by:

(Def. 5) The common roots of p and $q = \{x \in L\colon x \text{ is a common root of } p \text{ and } q\}$.

4. Normalized Polynomials

Let L be a non empty zero structure and let p be a polynomial of L. The leading coefficient of p yields an element of L and is defined by:

(Def. 6) The leading coefficient of $p = p(\operatorname{len} p -' 1)$.

We introduce $\operatorname{LC} p$ as a synonym of the leading coefficient of p.

Let L be a non trivial double loop structure and let p be a non zero polynomial of L. One can check that $\operatorname{LC} p$ is non zero.

One can prove the following proposition

(18) Let L be an add-associative right zeroed right complementable well unital commutative associative distributive almost left invertible non empty double loop structure, p be a polynomial of L, and a be an element of L. Then $\operatorname{LC}(a \cdot p) = a \cdot \operatorname{LC} p$.

Let L be a non empty double loop structure and let p be a polynomial of L. We say that p is normalized if and only if:

(Def. 7) $\operatorname{LC} p = 1_L$.

Let L be an add-associative right zeroed right complementable well unital commutative associative distributive almost left invertible non trivial double loop structure and let p be a non zero polynomial of L. One can check that $\frac{1_L}{\operatorname{LC} p} \cdot p$ is normalized.

Let L be a field and let p be a non zero polynomial of L. One can verify that $\operatorname{NormPolynomial} p$ is normalized.

5. Rational Functions

Let L be a non trivial multiplicative loop with zero structure. Rational function of L is defined by:

(Def. 8) There exists a polynomial p_1 of L and there exists a non zero polynomial p_2 of L such that it $= \langle p_1, p_2 \rangle$.

Let L be a non trivial multiplicative loop with zero structure, let p_1 be a polynomial of L, and let p_2 be a non zero polynomial of L. Then $\langle p_1, p_2 \rangle$ is a rational function of L.

Let L be a non trivial multiplicative loop with zero structure and let z be a rational function of L. Then $z_{\mathbf{1}}$ is a polynomial of L. Then $z_{\mathbf{2}}$ is a non zero polynomial of L.

Let L be a non trivial multiplicative loop with zero structure and let z be a rational function of L. We say that z is zero if and only if:

(Def. 9) $z_{\mathbf{1}} = \mathbf{0}_L$.

Let L be a non trivial multiplicative loop with zero structure. One can check that there exists a rational function of L which is non zero.

Next we state the proposition

(19) Let L be a non trivial multiplicative loop with zero structure and z be a rational function of L. Then $z = \langle z_{\mathbf{1}}, z_{\mathbf{2}} \rangle$.

Let L be an add-associative right zeroed right complementable distributive unital non trivial double loop structure and let z be a rational function of L. We say that z is irreducible if and only if:

(Def. 10) $z_{\mathbf{1}}$ and $z_{\mathbf{2}}$ have no common roots.

Let L be an add-associative right zeroed right complementable distributive unital non trivial double loop structure and let z be a rational function of L. We introduce z is reducible as an antonym of z is irreducible.

Let L be an add-associative right zeroed right complementable distributive unital non trivial double loop structure and let z be a rational function of L. We say that z is normalized if and only if:

(Def. 11) z is irreducible and $z_{\mathbf{2}}$ is normalized.

Let L be an add-associative right zeroed right complementable distributive unital non trivial double loop structure. Observe that every rational function of L which is normalized is also irreducible.

Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure and let z be a rational function of L. Note that $\mathrm{LC}(z_{\mathbf{2}})$ is non zero.

Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure and let z be a rational function of L. The norm rational function of z yields a rational function of L and is defined by:

(Def. 12) The norm rational function of $z = \langle \frac{1_L}{\mathrm{LC}(z_{\mathbf{2}})} \cdot z_{\mathbf{1}}, \frac{1_L}{\mathrm{LC}(z_{\mathbf{2}})} \cdot z_{\mathbf{2}} \rangle$.

Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral

domain-like non trivial double loop structure and let z be a rational function of L. We introduce NormRatF z as a synonym of the norm rational function of z.

Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure and let z be a non zero rational function of L. Observe that the norm rational function of z is non zero.

Let L be a non degenerated multiplicative loop with zero structure. The functor $0.L$ yields a rational function of L and is defined by:

(Def. 13) $0.L = \langle \mathbf{0}.L, \mathbf{1}.L \rangle$.

The functor $1.L$ yields a rational function of L and is defined as follows:

(Def. 14) $1.L = \langle \mathbf{1}.L, \mathbf{1}.L \rangle$.

Let L be an add-associative right zeroed right complementable distributive associative well unital non degenerated double loop structure. One can check that $0.L$ is normalized.

Let L be a non degenerated multiplicative loop with zero structure. Note that $1.L$ is non zero.

Let L be an add-associative right zeroed right complementable distributive associative well unital non degenerated double loop structure. One can verify that $1.L$ is irreducible.

Let L be an add-associative right zeroed right complementable distributive associative well unital non degenerated double loop structure. Observe that there exists a rational function of L which is irreducible and non zero.

Let L be an add-associative right zeroed right complementable distributive Abelian associative well unital non degenerated double loop structure and let x be an element of L. One can check that $\langle \mathrm{rpoly}(1,x), \mathrm{rpoly}(1,x) \rangle$ is reducible and non zero as a rational function of L.

Let L be an add-associative right zeroed right complementable distributive Abelian associative well unital non degenerated double loop structure. Observe that there exists a rational function of L which is reducible and non zero.

Let L be an add-associative right zeroed right complementable distributive associative well unital non degenerated double loop structure. One can verify that there exists a rational function of L which is normalized.

Let L be a non degenerated multiplicative loop with zero structure. One can verify that $0.L$ is zero.

Let L be an add-associative right zeroed right complementable distributive associative well unital non degenerated double loop structure. One can check that $1.L$ is normalized.

Let L be an integral domain-like add-associative right zeroed right complementable distributive non trivial double loop structure and let p, q be rational functions of L. The functor $p + q$ yields a rational function of L and is defined by:

(Def. 15) $p + q = \langle p_{\mathbf{1}} * q_{\mathbf{2}} + p_{\mathbf{2}} * q_{\mathbf{1}},\ p_{\mathbf{2}} * q_{\mathbf{2}} \rangle$.

Let L be an integral domain-like add-associative right zeroed right complementable distributive non trivial double loop structure and let p, q be rational functions of L. The functor $p * q$ yielding a rational function of L is defined by:

(Def. 16) $p * q = \langle p_{\mathbf{1}} * q_{\mathbf{1}},\ p_{\mathbf{2}} * q_{\mathbf{2}} \rangle$.

One can prove the following proposition

(20) Let L be an add-associative right zeroed right complementable well unital commutative associative distributive almost left invertible non trivial double loop structure, p be a rational function of L, and a be a non zero element of L. Then $\langle a \cdot p_{\mathbf{1}},\ a \cdot p_{\mathbf{2}} \rangle$ is irreducible if and only if p is irreducible.

6. Normalized Rational Functions

We now state the proposition

(21) Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative integral domain-like non trivial double loop structure and z be a rational function of L. Then there exists a rational function z_1 of L and there exists a non zero polynomial z_2 of L such that

(i) $z = \langle z_2 * (z_1)_{\mathbf{1}},\ z_2 * (z_1)_{\mathbf{2}} \rangle$,

(ii) z_1 is irreducible, and

(iii) there exists a finite sequence f of elements of Polynom-Ring L such that $z_2 = \prod f$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} f$ there exists an element x of L such that x is a common root of $z_{\mathbf{1}}$ and $z_{\mathbf{2}}$ and $f(i) = \operatorname{rpoly}(1, x)$.

Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure and let z be a rational function of L. The functor $\operatorname{NF} z$ yielding a rational function of L is defined by:

(Def. 17)(i) There exists a rational function z_1 of L and there exists a non zero polynomial z_2 of L such that $z = \langle z_2 * (z_1)_{\mathbf{1}},\ z_2 * (z_1)_{\mathbf{2}} \rangle$ and z_1 is irreducible and $\operatorname{NF} z$ = the norm rational function of z_1 and there exists a finite sequence f of elements of Polynom-Ring L such that $z_2 = \prod f$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} f$ there exists an element x of L such that x is a common root of $z_{\mathbf{1}}$ and $z_{\mathbf{2}}$ and $f(i) = \operatorname{rpoly}(1, x)$ if z is non zero,

(ii) $\operatorname{NF} z = 0.L$, otherwise.

Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral

domain-like non trivial double loop structure and let z be a rational function of L. Observe that $\mathrm{NF}\, z$ is normalized and irreducible.

Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure and let z be a non zero rational function of L. One can verify that $\mathrm{NF}\, z$ is non zero.

One can prove the following propositions:

(22) Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure, z be a non zero rational function of L, z_1 be a rational function of L, and z_2 be a non zero polynomial of L. Suppose that

(i) $z = \langle z_2 * (z_1)_{\mathbf{1}},\ z_2 * (z_1)_{\mathbf{2}} \rangle$,

(ii) z_1 is irreducible, and

(iii) there exists a finite sequence f of elements of Polynom-Ring L such that $z_2 = \prod f$ and for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, f$ there exists an element x of L such that x is a common root of $z_{\mathbf{1}}$ and $z_{\mathbf{2}}$ and $f(i) = \mathrm{rpoly}(1, x)$.

Then $\mathrm{NF}\, z =$ the norm rational function of z_1.

(23) Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure. Then $\mathrm{NF}\, 0.\, L = 0.\, L$.

(24) Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure. Then $\mathrm{NF}\, 1.\, L = 1.\, L$.

(25) Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure and z be an irreducible non zero rational function of L. Then $\mathrm{NF}\, z =$ the norm rational function of z.

(26) Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure, z be a rational function of L, and x be an element of L. Then $\mathrm{NF}\, \langle \mathrm{rpoly}(1, x) * z_{\mathbf{1}}, \mathrm{rpoly}(1, x) * z_{\mathbf{2}} \rangle = \mathrm{NF}\, z$.

(27) Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure and z be a rational function of L. Then $\mathrm{NF}\, \mathrm{NF}\, z = \mathrm{NF}\, z$.

(28) Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible in-

tegral domain-like non degenerated double loop structure and z be a non zero rational function of L. Then z is irreducible if and only if there exists an element a of L such that $a \neq 0_L$ and $\langle a \cdot z_{\mathbf{1}}, a \cdot z_{\mathbf{2}} \rangle = \mathrm{NF}\, z$.

7. Degree of Rational Functions

Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure and let z be a rational function of L. The functor degree(z) yielding an integer is defined as follows:

(Def. 18) $\mathrm{degree}(z) = \max(\mathrm{degree}((\mathrm{NF}\, z)_{\mathbf{1}}), \mathrm{degree}((\mathrm{NF}\, z)_{\mathbf{2}}))$.

Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure and let z be a rational function of L. We introduce $\deg z$ as a synonym of degree(z).

Next we state two propositions:

(29) Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure and z be a rational function of L. Then $\mathrm{degree}(z) \leq \max(\mathrm{degree}(z_{\mathbf{1}}), \mathrm{degree}(z_{\mathbf{2}}))$.

(30) Let L be an Abelian add-associative right zeroed right complementable well unital associative distributive commutative almost left invertible integral domain-like non trivial double loop structure and z be a non zero rational function of L. Then z is irreducible if and only if $\mathrm{degree}(z) = \max(\mathrm{degree}(z_{\mathbf{1}}), \mathrm{degree}(z_{\mathbf{2}}))$.

8. Evaluation of Rational Functions

Let L be a field, let z be a rational function of L, and let x be an element of L. The functor eval(z, x) yielding an element of L is defined by:

(Def. 19) $\mathrm{eval}(z, x) = \frac{\mathrm{eval}(z_{\mathbf{1}}, x)}{\mathrm{eval}(z_{\mathbf{2}}, x)}$.

The following propositions are true:

(31) For every field L and for every element x of L holds $\mathrm{eval}(0.\, L, x) = 0_L$.

(32) For every field L and for every element x of L holds $\mathrm{eval}(1.\, L, x) = 1_L$.

(33) Let L be a field, p, q be rational functions of L, and x be an element of L. If $\mathrm{eval}(p_{\mathbf{2}}, x) \neq 0_L$ and $\mathrm{eval}(q_{\mathbf{2}}, x) \neq 0_L$, then $\mathrm{eval}(p + q, x) = \mathrm{eval}(p, x) + \mathrm{eval}(q, x)$.

(34) Let L be a field, p, q be rational functions of L, and x be an element of L. If $\mathrm{eval}(p_{\mathbf{2}}, x) \neq 0_L$ and $\mathrm{eval}(q_{\mathbf{2}}, x) \neq 0_L$, then $\mathrm{eval}(p * q, x) = \mathrm{eval}(p, x) \cdot \mathrm{eval}(q, x)$.

(35) Let L be a field, p be a rational function of L, and x be an element of L. If $\mathrm{eval}(p_{\mathbf{2}}, x) \neq 0_L$, then $\mathrm{eval}(\text{the norm rational function of } p,\ x) = \mathrm{eval}(p, x)$.

(36) Let L be a field, p be a rational function of L, and x be an element of L. If $\mathrm{eval}(p_{\mathbf{2}}, x) \neq 0_L$, then x is a common root of $p_{\mathbf{1}}$ and $p_{\mathbf{2}}$ or $\mathrm{eval}(\mathrm{NF}\, p, x) = \mathrm{eval}(p, x)$.

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[8] H. Heuser. *Lehrbuch der Analysis*. B.G. Teubner Stuttgart, 1990.
[9] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[10] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.
[11] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.
[12] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.
[13] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[14] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.
[15] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[16] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Schur's theorem on the stability of networks. *Formalized Mathematics*, 14(**4**):135–142, 2006, doi:10.2478/v10037-006-0017-9.
[17] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[18] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[19] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[20] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[22] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[23] Hiroshi Yamazaki and Yasunari Shidama. Algebra of vector functions. *Formalized Mathematics*, 3(**2**):171–175, 1992.

Received February 8, 2012