FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

Sorting Operators for Finite Sequences

Yatsuka Nakamura
Shinshu University
Nagano

Summary. Two kinds of sorting operators, descendent one and ascendent one are introduced for finite sequences of reals. They are also called rearrangement of finite sequences of reals. Maximum and minimum values of finite sequences of reals are also defined. We also discuss relations between these concepts.

MML Identifier: `RFINSEQ2`.

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

Let f be a finite sequence of elements of $\mathbb{R}$. The functor $\max_{\rm p} f$ yielding a natural number is defined by the conditions (Def. 1).

(Def. 1)(i) If $\mathrm{len}\, f = 0$, then $\max_{\rm p} f = 0$, and

(ii) if $\mathrm{len}\, f > 0$, then $\max_{\rm p} f \in \mathrm{dom}\, f$ and for every natural number i and for all real numbers r_1, r_2 such that $i \in \mathrm{dom}\, f$ and $r_1 = f(i)$ and $r_2 = f(\max_{\rm p} f)$ holds $r_1 \leqslant r_2$ and for every natural number j such that $j \in \mathrm{dom}\, f$ and $f(j) = f(\max_{\rm p} f)$ holds $\max_{\rm p} f \leqslant j$.

Let f be a finite sequence of elements of $\mathbb{R}$. The functor $\min_{\rm p} f$ yields a natural number and is defined by the conditions (Def. 2).

(Def. 2)(i) If $\mathrm{len}\, f = 0$, then $\min_{\rm p} f = 0$, and

(ii) if $\mathrm{len}\, f > 0$, then $\min_{\rm p} f \in \mathrm{dom}\, f$ and for every natural number i and for all real numbers r_1, r_2 such that $i \in \mathrm{dom}\, f$ and $r_1 = f(i)$ and $r_2 = f(\min_{\rm p} f)$ holds $r_1 \geqslant r_2$ and for every natural number j such that $j \in \mathrm{dom}\, f$ and $f(j) = f(\min_{\rm p} f)$ holds $\min_{\rm p} f \leqslant j$.

Let f be a finite sequence of elements of $\mathbb{R}$. The functor $\max f$ yields a real number and is defined by:

(Def. 3) $\max f = f(\max_{\rm p} f)$.

The functor $\min f$ yields a real number and is defined by:

ISSN 1426–2630

(Def. 4) $\min f = f(\min_{\mathrm{p}} f)$.

The following propositions are true:

(1) Let f be a finite sequence of elements of $\mathbb{R}$ and i be a natural number. If $1 \leqslant i$ and $i \leqslant \operatorname{len} f$, then $f(i) \leqslant f(\max_{\mathrm{p}} f)$ and $f(i) \leqslant \max f$.

(2) Let f be a finite sequence of elements of $\mathbb{R}$ and i be a natural number. If $1 \leqslant i$ and $i \leqslant \operatorname{len} f$, then $f(i) \geqslant f(\min_{\mathrm{p}} f)$ and $f(i) \geqslant \min f$.

(3) For every finite sequence f of elements of $\mathbb{R}$ and for every real number r such that $f = \langle r \rangle$ holds $\max_{\mathrm{p}} f = 1$ and $\max f = r$.

(4) For every finite sequence f of elements of $\mathbb{R}$ and for every real number r such that $f = \langle r \rangle$ holds $\min_{\mathrm{p}} f = 1$ and $\min f = r$.

(5) Let f be a finite sequence of elements of $\mathbb{R}$ and r_1, r_2 be real numbers. If $f = \langle r_1, r_2 \rangle$, then $\max f = \max(r_1, r_2)$ and $\max_{\mathrm{p}} f = (r_1 = \max(r_1, r_2) \to 1, 2)$.

(6) Let f be a finite sequence of elements of $\mathbb{R}$ and r_1, r_2 be real numbers. If $f = \langle r_1, r_2 \rangle$, then $\min f = \min(r_1, r_2)$ and $\min_{\mathrm{p}} f = (r_1 = \min(r_1, r_2) \to 1, 2)$.

(7) For all finite sequences f_1, f_2 of elements of $\mathbb{R}$ such that $\operatorname{len} f_1 = \operatorname{len} f_2$ and $\operatorname{len} f_1 > 0$ holds $\max(f_1 + f_2) \leqslant \max f_1 + \max f_2$.

(8) For all finite sequences f_1, f_2 of elements of $\mathbb{R}$ such that $\operatorname{len} f_1 = \operatorname{len} f_2$ and $\operatorname{len} f_1 > 0$ holds $\min(f_1 + f_2) \geqslant \min f_1 + \min f_2$.

(9) Let f be a finite sequence of elements of $\mathbb{R}$ and a be a real number. If $\operatorname{len} f > 0$ and $a > 0$, then $\max(a \cdot f) = a \cdot \max f$ and $\max_{\mathrm{p}}(a \cdot f) = \max_{\mathrm{p}} f$.

(10) Let f be a finite sequence of elements of $\mathbb{R}$ and a be a real number. If $\operatorname{len} f > 0$ and $a > 0$, then $\min(a \cdot f) = a \cdot \min f$ and $\min_{\mathrm{p}}(a \cdot f) = \min_{\mathrm{p}} f$.

(11) For every finite sequence f of elements of $\mathbb{R}$ such that $\operatorname{len} f > 0$ holds $\max(-f) = -\min f$ and $\max_{\mathrm{p}}(-f) = \min_{\mathrm{p}} f$.

(12) For every finite sequence f of elements of $\mathbb{R}$ such that $\operatorname{len} f > 0$ holds $\min(-f) = -\max f$ and $\min_{\mathrm{p}}(-f) = \max_{\mathrm{p}} f$.

(13) Let f be a finite sequence of elements of $\mathbb{R}$ and n be a natural number. If $1 \leqslant n$ and $n < \operatorname{len} f$, then $\max(f_{\restriction n}) \leqslant \max f$ and $\min(f_{\restriction n}) \geqslant \min f$.

(14) For all finite sequences f, g of elements of $\mathbb{R}$ such that f and g are fiberwise equipotent holds $\max f = \max g$.

(15) For all finite sequences f, g of elements of $\mathbb{R}$ such that f and g are fiberwise equipotent holds $\min f = \min g$.

Let f be a finite sequence of elements of $\mathbb{R}$. The functor $\operatorname{sort_d} f$ yields a non-increasing finite sequence of elements of $\mathbb{R}$ and is defined by:

(Def. 5) f and $\operatorname{sort_d} f$ are fiberwise equipotent.

Next we state four propositions:

(16) For every finite sequence R of elements of $\mathbb{R}$ such that $\operatorname{len} R = 0$ or $\operatorname{len} R = 1$ holds R is non-decreasing.

(17) Let R be a finite sequence of elements of $\mathbb{R}$. Then R is non-decreasing if and only if for all natural numbers n, m such that $n \in \operatorname{dom} R$ and $m \in \operatorname{dom} R$ and $n < m$ holds $R(n) \leqslant R(m)$.

(18) Let R be a non-decreasing finite sequence of elements of $\mathbb{R}$ and n be a natural number. Then $R{\restriction}n$ is a non-decreasing finite sequence of elements of $\mathbb{R}$.

(19) Let R_1, R_2 be non-decreasing finite sequences of elements of $\mathbb{R}$. If R_1 and R_2 are fiberwise equipotent, then $R_1 = R_2$.

Let f be a finite sequence of elements of $\mathbb{R}$. The functor $\operatorname{sort_a} f$ yields a non-decreasing finite sequence of elements of $\mathbb{R}$ and is defined as follows:

(Def. 6) f and $\operatorname{sort_a} f$ are fiberwise equipotent.

Next we state a number of propositions:

(20) For every non-increasing finite sequence f of elements of $\mathbb{R}$ holds $\operatorname{sort_d} f = f$.

(21) For every non-decreasing finite sequence f of elements of $\mathbb{R}$ holds $\operatorname{sort_a} f = f$.

(22) For every finite sequence f of elements of $\mathbb{R}$ holds $\operatorname{sort_d} \operatorname{sort_d} f = \operatorname{sort_d} f$.

(23) For every finite sequence f of elements of $\mathbb{R}$ holds $\operatorname{sort_a} \operatorname{sort_a} f = \operatorname{sort_a} f$.

(24) For every finite sequence f of elements of $\mathbb{R}$ such that f is non-increasing holds $-f$ is non-decreasing.

(25) For every finite sequence f of elements of $\mathbb{R}$ such that f is non-decreasing holds $-f$ is non-increasing.

(26) Let f, g be finite sequences of elements of $\mathbb{R}$ and P be a permutation of $\operatorname{dom} g$. If $f = g \cdot P$ and $\operatorname{len} g \geqslant 1$, then $-f = (-g) \cdot P$.

(27) Let f, g be finite sequences of elements of $\mathbb{R}$. Suppose f and g are fiberwise equipotent. Then $-f$ and $-g$ are fiberwise equipotent.

(28) For every finite sequence f of elements of $\mathbb{R}$ holds $\operatorname{sort_d}(-f) = -\operatorname{sort_a} f$.

(29) For every finite sequence f of elements of $\mathbb{R}$ holds $\operatorname{sort_a}(-f) = -\operatorname{sort_d} f$.

(30) For every finite sequence f of elements of $\mathbb{R}$ holds $\operatorname{dom} \operatorname{sort_d} f = \operatorname{dom} f$ and $\operatorname{len} \operatorname{sort_d} f = \operatorname{len} f$.

(31) For every finite sequence f of elements of $\mathbb{R}$ holds $\operatorname{dom} \operatorname{sort_a} f = \operatorname{dom} f$ and $\operatorname{len} \operatorname{sort_a} f = \operatorname{len} f$.

(32) For every finite sequence f of elements of $\mathbb{R}$ such that $\operatorname{len} f \geqslant 1$ holds $\operatorname{max_p} \operatorname{sort_d} f = 1$ and $\operatorname{min_p} \operatorname{sort_a} f = 1$ and $(\operatorname{sort_d} f)(1) = \max f$ and $(\operatorname{sort_a} f)(1) = \min f$.

References

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

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

[3] Czesław Byliński. A classical first order language. *Formalized Mathematics*, 1(**4**):669–676, 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. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[7] Agata Darmochwał and Yatsuka Nakamura. The topological space $\mathcal{E}^2_{\mathrm{T}}$. Arcs, line segments and special polygonal arcs. *Formalized Mathematics*, 2(**5**):617–621, 1991.

[8] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Scalar multiple of Riemann definite integral. *Formalized Mathematics*, 9(**1**):191–196, 2001.

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

[10] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

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

[12] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*

[13] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

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

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

Received October 17, 2003

FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

Magnitude Relation Properties of Radix-2^k SD Number

Masaaki Niimura
Shinshu University
Nagano

Yasushi Fuwa
Shinshu University
Nagano

Summary. In this article, magnitude relation properties of Radix-2^k SD number are discussed. Until now, the Radix-2^k SD Number has been proposed for the high-speed calculations for RSA Cryptograms. In RSA Cryptograms, many modulo calculations are used, and modulo calculations need a comparison between two numbers.

In this article, we discuss magnitude relation of Radix-2^k SD Number. In the first section, we present some useful theorems for operations of Radix-2^k SD Number. In the second section, we prove some properties of the primary numbers expressed by Radix-2^k SD Number such as 0, 1, and Radix(k). In the third section, we prove primary magnitude relations between two Radix-2^k SD Numbers. In the fourth section, we define Max/Min numbers in some cases. And in the last section, we prove some relations between the addition of Max/Min numbers.

MML Identifier: `RADIX_5`.

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

1. Some Useful Theorems

The following propositions are true:

(1) For every natural number k such that $k \geqslant 2$ holds $\mathrm{Radix}\, k - 1 \in k\, {-\mathrm{SD}}$.

(2) For all natural numbers i, n such that $i > 1$ and $i \in \mathrm{Seg}\, n$ holds $i -' 1 \in \mathrm{Seg}\, n$.

(3) For every natural number k such that $2 \leqslant k$ holds $4 \leqslant \mathrm{Radix}\, k$.

ISSN 1426–2630

(4) For every natural number k and for every 1-tuple t_1 of k −SD holds $\mathrm{SDDec}\, t_1 = \mathrm{DigA}(t_1, 1)$.

2. Properties of Primary Radix-2^k SD Number

Next we state several propositions:

(5) For all natural numbers i, k, n such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(\mathrm{DecSD}(0, n, k), i) = 0$.

(6) For all natural numbers n, k such that $n \geqslant 1$ holds $\mathrm{SDDec}\, \mathrm{DecSD}(0, n, k) = 0$.

(7) For all natural numbers k, n such that $1 \in \mathrm{Seg}\, n$ and $k \geqslant 2$ holds $\mathrm{DigA}(\mathrm{DecSD}(1, n, k), 1) = 1$.

(8) For all natural numbers i, k, n such that $i \in \mathrm{Seg}\, n$ and $i > 1$ and $k \geqslant 2$ holds $\mathrm{DigA}(\mathrm{DecSD}(1, n, k), i) = 0$.

(9) For all natural numbers n, k such that $n \geqslant 1$ and $k \geqslant 2$ holds $\mathrm{SDDec}\, \mathrm{DecSD}(1, n, k) = 1$.

(10) For every natural number k such that $k \geqslant 2$ holds $\mathrm{SD\_Add\_Carry}\, \mathrm{Radix}\, k = 1$.

(11) For every natural number k such that $k \geqslant 2$ holds $\mathrm{SD\_Add\_Data}(\mathrm{Radix}\, k, k) = 0$.

3. Primary Magnitude Relation of Radix-2^k SD Number

Next we state four propositions:

(12) Let n be a natural number. Suppose $n \geqslant 1$. Let k be a natural number and t_1, t_2 be n-tuples of k −SD. If for every natural number i such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(t_1, i) = \mathrm{DigA}(t_2, i)$, then $\mathrm{SDDec}\, t_1 = \mathrm{SDDec}\, t_2$.

(13) Let n be a natural number. Suppose $n \geqslant 1$. Let k be a natural number and t_1, t_2 be n-tuples of k −SD. If for every natural number i such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(t_1, i) \geqslant \mathrm{DigA}(t_2, i)$, then $\mathrm{SDDec}\, t_1 \geqslant \mathrm{SDDec}\, t_2$.

(14) Let n be a natural number. Suppose $n \geqslant 1$. Let k be a natural number. Suppose $k \geqslant 2$. Let t_1, t_2, t_3, t_4 be n-tuples of k −SD. Suppose that for every natural number i such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(t_1, i) = \mathrm{DigA}(t_3, i)$ and $\mathrm{DigA}(t_2, i) = \mathrm{DigA}(t_4, i)$ or $\mathrm{DigA}(t_2, i) = \mathrm{DigA}(t_3, i)$ and $\mathrm{DigA}(t_1, i) = \mathrm{DigA}(t_4, i)$. Then $\mathrm{SDDec}\, t_3 + \mathrm{SDDec}\, t_4 = \mathrm{SDDec}\, t_1 + \mathrm{SDDec}\, t_2$.

(15) Let n, k be natural numbers. Suppose $n \geqslant 1$ and $k \geqslant 2$. Let t_1, t_2, t_3 be n-tuples of k −SD. Suppose that for every natural number i such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(t_1, i) = \mathrm{DigA}(t_3, i)$ and $\mathrm{DigA}(t_2, i) = 0$ or $\mathrm{DigA}(t_2, i) =$

$\mathrm{DigA}(t_3, i)$ and $\mathrm{DigA}(t_1, i) = 0$. Then $\mathrm{SDDec}\, t_3 + \mathrm{SDDec}\,\mathrm{DecSD}(0, n, k) = \mathrm{SDDec}\, t_1 + \mathrm{SDDec}\, t_2$.

4. Definition of Max/Min Radix-2^k SD Numbers in Some Digits

Let i, m, k be natural numbers. Let us assume that $k \geqslant 2$. The functor $\mathrm{SDMinDigit}(m, k, i)$ yielding an element of k −SD is defined as follows:

(Def. 1) $\mathrm{SDMinDigit}(m, k, i) = \begin{cases} -\mathrm{Radix}\, k + 1, & \text{if } 1 \leqslant i \text{ and } i < m, \\ 0, & \text{otherwise.} \end{cases}$

Let n, m, k be natural numbers. The functor $\mathrm{SDMin}(n, m, k)$ yields a n-tuple of k −SD and is defined by:

(Def. 2) For every natural number i such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(\mathrm{SDMin}(n, m, k), i) = \mathrm{SDMinDigit}(m, k, i)$.

Let i, m, k be natural numbers. Let us assume that $k \geqslant 2$. The functor $\mathrm{SDMaxDigit}(m, k, i)$ yielding an element of k −SD is defined as follows:

(Def. 3) $\mathrm{SDMaxDigit}(m, k, i) = \begin{cases} \mathrm{Radix}\, k - 1, & \text{if } 1 \leqslant i \text{ and } i < m, \\ 0, & \text{otherwise.} \end{cases}$

Let n, m, k be natural numbers. The functor $\mathrm{SDMax}(n, m, k)$ yields a n-tuple of k −SD and is defined by:

(Def. 4) For every natural number i such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(\mathrm{SDMax}(n, m, k), i) = \mathrm{SDMaxDigit}(m, k, i)$.

Let i, m, k be natural numbers. Let us assume that $k \geqslant 2$. The functor $\mathrm{FminDigit}(m, k, i)$ yielding an element of k −SD is defined by:

(Def. 5) $\mathrm{FminDigit}(m, k, i) = \begin{cases} 1, & \text{if } i = m, \\ 0, & \text{otherwise.} \end{cases}$

Let n, m, k be natural numbers. The functor $\mathrm{Fmin}(n, m, k)$ yields a n-tuple of k −SD and is defined as follows:

(Def. 6) For every natural number i such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(\mathrm{Fmin}(n, m, k), i) = \mathrm{FminDigit}(m, k, i)$.

Let i, m, k be natural numbers. Let us assume that $k \geqslant 2$. The functor $\mathrm{FmaxDigit}(m, k, i)$ yielding an element of k −SD is defined as follows:

(Def. 7) $\mathrm{FmaxDigit}(m, k, i) = \begin{cases} \mathrm{Radix}\, k - 1, & \text{if } i = m, \\ 0, & \text{otherwise.} \end{cases}$

Let n, m, k be natural numbers. The functor $\mathrm{Fmax}(n, m, k)$ yielding a n-tuple of k −SD is defined as follows:

(Def. 8) For every natural number i such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(\mathrm{Fmax}(n, m, k), i) = \mathrm{FmaxDigit}(m, k, i)$.

5. Properties of Max/Min Radix-2^k SD Numbers

Next we state four propositions:

(16) Let n, m, k be natural numbers. Suppose $n \geqslant 1$ and $k \geqslant 2$ and $m \in \mathrm{Seg}\, n$. Let i be a natural number. If $i \in \mathrm{Seg}\, n$, then $\mathrm{DigA}(\mathrm{SDMax}(n, m, k), i) + \mathrm{DigA}(\mathrm{SDMin}(n, m, k), i) = 0$.

(17) Let n be a natural number. Suppose $n \geqslant 1$. Let m, k be natural numbers. If $m \in \mathrm{Seg}\, n$ and $k \geqslant 2$, then $\mathrm{SDDec}\,\mathrm{SDMax}(n, m, k) + \mathrm{SDDec}\,\mathrm{SDMin}(n, m, k) = \mathrm{SDDec}\,\mathrm{DecSD}(0, n, k)$.

(18) Let n be a natural number. Suppose $n \geqslant 1$. Let m, k be natural numbers. If $m \in \mathrm{Seg}\, n$ and $k \geqslant 2$, then $\mathrm{SDDec}\,\mathrm{Fmin}(n, m, k) = \mathrm{SDDec}\,\mathrm{SDMax}(n, m, k) + \mathrm{SDDec}\,\mathrm{DecSD}(1, n, k)$.

(19) For all natural numbers n, m, k such that $m \in \mathrm{Seg}\, n$ and $k \geqslant 2$ holds $\mathrm{SDDec}\,\mathrm{Fmin}(n+1, m+1, k) = \mathrm{SDDec}\,\mathrm{Fmin}(n+1, m, k) + \mathrm{SDDec}\,\mathrm{Fmax}(n+1, m, k)$.

References

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

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

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

[4] Yoshinori Fujisawa and Yasushi Fuwa. Definitions of radix-2^k signed-digit number and its adder algorithm. *Formalized Mathematics*, 9(**1**):71–75, 2001.

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

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

[7] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

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

Received November 7, 2003

FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

High Speed Modulo Calculation Algorithm with Radix-2^k SD Number

Masaaki Niimura
Shinshu University
Nagano

Yasushi Fuwa
Shinshu University
Nagano

Summary. In RSA Cryptograms, many modulo calculations are used, but modulo calculation is based on many subtractions and it takes long a time to calculate it. In this article, we explain a new modulo calculation algorithm using a table. And we prove that upper 3 digits of Radix-2^k SD numbers are enough to specify the answer.

In the first section, we present some useful theorems for operations of Radix-2^k SD Number. In the second section, we define Upper 3 Digits of Radix-2^k SD number and prove that property. In the third section, we prove some property connected with the minimum digits of Radix-2^k SD number. In the fourth section, we identify the range of modulo arithmetic result and prove that the Upper 3 Digits indicate two possible answers. And in the last section, we define a function to select true answer from the results of Upper 3 Digits.

MML Identifier: `RADIX_6`.

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

1. Some Useful Theorems

The following two propositions are true:

(1) Let n be a natural number. Suppose $n \geqslant 1$. Let m, k be natural numbers. If $m \geqslant 1$ and $k \geqslant 2$, then $\mathrm{SDDec}\,\mathrm{Fmin}(m+n, m, k) = \mathrm{SDDec}\,\mathrm{Fmin}(m, m, k)$.

(2) For all natural numbers m, k such that $m \geqslant 1$ and $k \geqslant 2$ holds $\mathrm{SDDec}\,\mathrm{Fmin}(m, m, k) > 0$.

ISSN 1426–2630

2. Definitions of Upper 3 Digits of Radix-2^k SD Number and Its Property

Let i, m, k be natural numbers and let r be a $m+2$-tuple of k −SD. Let us assume that $i \in \mathrm{Seg}(m+2)$. The functor $\mathrm{M0Digit}(r, i)$ yielding an element of k −SD is defined as follows:

(Def. 1) $\quad \mathrm{M0Digit}(r, i) = \begin{cases} r(i), & \text{if } i \geqslant m, \\ 0, & \text{if } i < m. \end{cases}$

Let m, k be natural numbers and let r be a $m+2$-tuple of k −SD. The functor $\mathrm{M0}(r)$ yielding a $m+2$-tuple of k −SD is defined as follows:

(Def. 2) For every natural number i such that $i \in \mathrm{Seg}(m+2)$ holds $\mathrm{DigA}(\mathrm{M0}(r), i) = \mathrm{M0Digit}(r, i)$.

Let i, m, k be natural numbers and let r be a $m+2$-tuple of k −SD. Let us assume that $k \geqslant 2$ and $i \in \mathrm{Seg}(m+2)$. The functor $\mathrm{MmaxDigit}(r, i)$ yielding an element of k −SD is defined as follows:

(Def. 3) $\quad \mathrm{MmaxDigit}(r, i) = \begin{cases} r(i), & \text{if } i \geqslant m, \\ \mathrm{Radix}\, k - 1, & \text{if } i < m. \end{cases}$

Let m, k be natural numbers and let r be a $m+2$-tuple of k −SD. The functor $\mathrm{Mmax}(r)$ yields a $m+2$-tuple of k −SD and is defined as follows:

(Def. 4) For every natural number i such that $i \in \mathrm{Seg}(m+2)$ holds $\mathrm{DigA}(\mathrm{Mmax}(r), i) = \mathrm{MmaxDigit}(r, i)$.

Let i, m, k be natural numbers and let r be a $m+2$-tuple of k −SD. Let us assume that $k \geqslant 2$ and $i \in \mathrm{Seg}(m+2)$. The functor $\mathrm{MminDigit}(r, i)$ yields an element of k −SD and is defined by:

(Def. 5) $\quad \mathrm{MminDigit}(r, i) = \begin{cases} r(i), & \text{if } i \geqslant m, \\ -\mathrm{Radix}\, k + 1, & \text{if } i < m. \end{cases}$

Let m, k be natural numbers and let r be a $m+2$-tuple of k −SD. The functor $\mathrm{Mmin}(r)$ yielding a $m+2$-tuple of k −SD is defined by:

(Def. 6) For every natural number i such that $i \in \mathrm{Seg}(m+2)$ holds $\mathrm{DigA}(\mathrm{Mmin}(r), i) = \mathrm{MminDigit}(r, i)$.

One can prove the following two propositions:

(3) For all natural numbers m, k such that $m \geqslant 1$ and $k \geqslant 2$ and for every $m+2$-tuple r of k −SD holds $\mathrm{SDDec}\,\mathrm{Mmax}(r) \geqslant \mathrm{SDDec}\, r$.

(4) For all natural numbers m, k such that $m \geqslant 1$ and $k \geqslant 2$ and for every $m+2$-tuple r of k −SD holds $\mathrm{SDDec}\, r \geqslant \mathrm{SDDec}\,\mathrm{Mmin}(r)$.

3. Properties of Minimum Digits of Radix-2^k SD Number

Let n, k be natural numbers and let x be an integer. We say that x needs digits of n, k if and only if:

(Def. 7) $x < (\mathrm{Radix}\, k)^n$ and $x \geqslant (\mathrm{Radix}\, k)^{n-'1}$.

One can prove the following three propositions:

(5) For all natural numbers x, n, k, i such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(\mathrm{DecSD}(x, n, k), i) \geqslant 0$.

(6) For all natural numbers n, k, x such that $n \geqslant 1$ and $k \geqslant 2$ and x needs digits of n, k holds $\mathrm{DigA}(\mathrm{DecSD}(x, n, k), n) > 0$.

(7) For all natural numbers f, m, k such that $m \geqslant 1$ and $k \geqslant 2$ and f needs digits of m, k holds $f \geqslant \mathrm{SDDec}\, \mathrm{Fmin}(m + 2, m, k)$.

4. Modulo Calculation Algorithm Using Upper 3 Digits of Radix-2^k SD Number

Next we state several propositions:

(8) For all integers m_1, m_2, f such that $m_2 < m_1 + f$ and $f > 0$ there exists an integer s such that $-f < m_1 - s \cdot f$ and $m_2 - s \cdot f < f$.

(9) Let m, k be natural numbers. Suppose $m \geqslant 1$ and $k \geqslant 2$. Let r be a $m+2$-tuple of k –SD. Then $\mathrm{SDDec}\, \mathrm{Mmax}(r) + \mathrm{SDDec}\, \mathrm{DecSD}(0, m+2, k) = \mathrm{SDDec}\, \mathrm{M0}(r) + \mathrm{SDDec}\, \mathrm{SDMax}(m + 2, m, k)$.

(10) For all natural numbers m, k such that $m \geqslant 1$ and $k \geqslant 2$ and for every $m + 2$-tuple r of k –SD holds $\mathrm{SDDec}\, \mathrm{Mmax}(r) < \mathrm{SDDec}\, \mathrm{M0}(r) + \mathrm{SDDec}\, \mathrm{Fmin}(m + 2, m, k)$.

(11) Let m, k be natural numbers. Suppose $m \geqslant 1$ and $k \geqslant 2$. Let r be a $m+2$-tuple of k –SD. Then $\mathrm{SDDec}\, \mathrm{Mmin}(r) + \mathrm{SDDec}\, \mathrm{DecSD}(0, m+2, k) = \mathrm{SDDec}\, \mathrm{M0}(r) + \mathrm{SDDec}\, \mathrm{SDMin}(m + 2, m, k)$.

(12) Let m, k be natural numbers and r be a $m + 2$-tuple of k –SD. If $m \geqslant 1$ and $k \geqslant 2$, then $\mathrm{SDDec}\, \mathrm{M0}(r) + \mathrm{SDDec}\, \mathrm{DecSD}(0, m + 2, k) = \mathrm{SDDec}\, \mathrm{Mmin}(r) + \mathrm{SDDec}\, \mathrm{SDMax}(m + 2, m, k)$.

(13) For all natural numbers m, k such that $m \geqslant 1$ and $k \geqslant 2$ and for every $m + 2$-tuple r of k –SD holds $\mathrm{SDDec}\, \mathrm{M0}(r) < \mathrm{SDDec}\, \mathrm{Mmin}(r) + \mathrm{SDDec}\, \mathrm{Fmin}(m + 2, m, k)$.

(14) Let m, k, f be natural numbers and r be a $m+2$-tuple of k –SD. Suppose $m \geqslant 1$ and $k \geqslant 2$ and f needs digits of m, k. Then there exists an integer s such that $-f < \mathrm{SDDec}\, \mathrm{M0}(r) - s \cdot f$ and $\mathrm{SDDec}\, \mathrm{Mmax}(r) - s \cdot f < f$.

(15) Let m, k, f be natural numbers and r be a $m+2$-tuple of k –SD. Suppose $m \geqslant 1$ and $k \geqslant 2$ and f needs digits of m, k. Then there exists an integer s such that $-f < \mathrm{SDDec}\, \mathrm{Mmin}(r) - s \cdot f$ and $\mathrm{SDDec}\, \mathrm{M0}(r) - s \cdot f < f$.

(16) Let m, k be natural numbers and r be a $m + 2$-tuple of k –SD. If $m \geqslant 1$ and $k \geqslant 2$, then $\mathrm{SDDec}\, \mathrm{M0}(r) \leqslant \mathrm{SDDec}\, r$ and $\mathrm{SDDec}\, r \leqslant \mathrm{SDDec}\, \mathrm{Mmax}(r)$ or $\mathrm{SDDec}\, \mathrm{Mmin}(r) \leqslant \mathrm{SDDec}\, r$ and $\mathrm{SDDec}\, r < \mathrm{SDDec}\, \mathrm{M0}(r)$.

5. How to Identify the Range of Modulo Arithmetic Result

Let i, m, k be natural numbers and let r be a $m+2$-tuple of k −SD. Let us assume that $i \in \mathrm{Seg}(m+2)$. The functor $\mathrm{MmaskDigit}(r, i)$ yielding an element of k −SD is defined by:

(Def. 8) $$\mathrm{MmaskDigit}(r, i) = \begin{cases} r(i), & \text{if } i < m, \\ 0, & \text{if } i \geqslant m. \end{cases}$$

Let m, k be natural numbers and let r be a $m+2$-tuple of k −SD. The functor $\mathrm{Mmask}(r)$ yields a $m+2$-tuple of k −SD and is defined by:

(Def. 9) For every natural number i such that $i \in \mathrm{Seg}(m+2)$ holds $\mathrm{DigA}(\mathrm{Mmask}(r), i) = \mathrm{MmaskDigit}(r, i)$.

One can prove the following two propositions:

(17) For all natural numbers m, k and for every $m+2$-tuple r of k −SD such that $m \geqslant 1$ and $k \geqslant 2$ holds $\mathrm{SDDec}\,\mathrm{M0}(r) + \mathrm{SDDec}\,\mathrm{Mmask}(r) = \mathrm{SDDec}\,r + \mathrm{SDDec}\,\mathrm{DecSD}(0, m+2, k)$.

(18) For all natural numbers m, k and for every $m+2$-tuple r of k −SD such that $m \geqslant 1$ and $k \geqslant 2$ holds if $\mathrm{SDDec}\,\mathrm{Mmask}(r) > 0$, then $\mathrm{SDDec}\,r > \mathrm{SDDec}\,\mathrm{M0}(r)$.

Let i, m, k be natural numbers. Let us assume that $k \geqslant 2$. The functor $\mathrm{FSDMinDigit}(m, k, i)$ yields an element of k −SD and is defined as follows:

(Def. 10) $$\mathrm{FSDMinDigit}(m, k, i) = \begin{cases} 0, & \text{if } i > m, \\ 1, & \text{if } i = m, \\ -\mathrm{Radix}\,k + 1, & \text{otherwise.} \end{cases}$$

Let n, m, k be natural numbers. The functor $\mathrm{FSDMin}(n, m, k)$ yields a n-tuple of k −SD and is defined as follows:

(Def. 11) For every natural number i such that $i \in \mathrm{Seg}\,n$ holds $\mathrm{DigA}(\mathrm{FSDMin}(n, m, k), i) = \mathrm{FSDMinDigit}(m, k, i)$.

One can prove the following proposition

(19) For every natural number n such that $n \geqslant 1$ and for all natural numbers m, k such that $m \in \mathrm{Seg}\,n$ and $k \geqslant 2$ holds $\mathrm{SDDec}\,\mathrm{FSDMin}(n, m, k) = 1$.

Let n, m, k be natural numbers and let r be a $m+2$-tuple of k −SD. We say that r is zero over n if and only if:

(Def. 12) For every natural number i such that $i > n$ holds $\mathrm{DigA}(r, i) = 0$.

We now state the proposition

(20) Let m be a natural number. Suppose $m \geqslant 1$. Let n, k be natural numbers and r be a $m+2$-tuple of k −SD. If $k \geqslant 2$ and $n \in \mathrm{Seg}(m+2)$ and $\mathrm{Mmask}(r)$ is zero over n and $\mathrm{DigA}(\mathrm{Mmask}(r), n) > 0$, then $\mathrm{SDDec}\,\mathrm{Mmask}(r) > 0$.

References

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

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

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

[4] Yoshinori Fujisawa and Yasushi Fuwa. Definitions of radix-2^k signed-digit number and its adder algorithm. *Formalized Mathematics*, 9(**1**):71–75, 2001.

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

[6] Masaaki Niimura and Yasushi Fuwa. Magnitude relation properties of radix-2^k SD number. *Formalized Mathematics*, 12(**1**):5–8, 2004.

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

[8] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

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

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

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

Received November 7, 2003

FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

Transitive Closure of Fuzzy Relations[1]

Takashi Mitsuishi
Miyagi University

Grzegorz Bancerek
Białystok Technical University

MML Identifier: LFUZZY_1.

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

1. Inclusion of Fuzzy Sets

In this paper X, Y denote non empty sets.

Let X be a non empty set. Observe that every membership function of X is real-yielding.

Let f, g be real-yielding functions. The predicate $f \sqsubseteq g$ is defined by:

(Def. 1) $\operatorname{dom} f \subseteq \operatorname{dom} g$ and for every set x such that $x \in \operatorname{dom} f$ holds $f(x) \leqslant g(x)$.

Let X be a non empty set and let f, g be membership functions of X. Let us observe that $f \sqsubseteq g$ if and only if:

(Def. 2) For every element x of X holds $f(x) \leqslant g(x)$.

We introduce $f \subseteq g$ as a synonym of $f \sqsubseteq g$.

Let X, Y be non empty sets and let f, g be membership functions of X, Y. Let us observe that $f \sqsubseteq g$ if and only if:

(Def. 3) For every element x of X and for every element y of Y holds $f(\langle x, y\rangle) \leqslant g(\langle x, y\rangle)$.

One can prove the following propositions:

[1]This work has been partially supported by the Polish Academy of Sciences and the Japan Society for the Promotion of Science (JSPS Grant 0324101 and JSPS Grant-in-aid 15700195) when the first author was visiting Białystok Technical University as postdoctoral fellow.

ISSN 1426–2630

(1) For all membership functions R, S of X such that for every element x of X holds $R(x) = S(x)$ holds $R = S$.

(2) Let R, S be membership functions of X, Y. Suppose that for every element x of X and for every element y of Y holds $R(\langle x, y\rangle) = S(\langle x, y\rangle)$. Then $R = S$.

(3) For all membership functions R, S of X holds $R = S$ iff $R \subseteq S$ and $S \subseteq R$.

(4) For every membership function R of X holds $R \subseteq R$.

(5) For all membership functions R, S, T of X such that $R \subseteq S$ and $S \subseteq T$ holds $R \subseteq T$.

(6) Let X, Y, Z be non empty sets, R, S be membership functions of X, Y, and T, U be membership functions of Y, Z. If $R \subseteq S$ and $T \subseteq U$, then $R\,T \subseteq S\,U$.

Let X be a non empty set and let f, g be membership functions of X. Let us note that the functor $\min(f, g)$ is commutative. Let us note that the functor $\max(f, g)$ is commutative.

We now state two propositions:

(7) For all membership functions f, g of X holds $\min(f, g) \subseteq f$.

(8) For all membership functions f, g of X holds $f \subseteq \max(f, g)$.

2. Properties of Fuzzy Relations

Let X be a non empty set and let R be a membership function of X, X. We say that R is reflexive if and only if:

(Def. 4) $\mathrm{Imf}(X, X) \subseteq R$.

Let X be a non empty set and let R be a membership function of X, X. Let us observe that R is reflexive if and only if:

(Def. 5) For every element x of X holds $R(\langle x, x\rangle) = 1$.

Let X be a non empty set and let R be a membership function of X, X. We say that R is symmetric if and only if:

(Def. 6) $\mathrm{converse}\, R = R$.

Let X be a non empty set and let R be a membership function of X, X. Let us observe that R is symmetric if and only if:

(Def. 7) For all elements x, y of X holds $R(\langle x, y\rangle) = R(\langle y, x\rangle)$.

Let X be a non empty set and let R be a membership function of X, X. We say that R is transitive if and only if:

(Def. 8) $R\,R \subseteq R$.

Let X be a non empty set and let R be a membership function of X, X. Let us observe that R is transitive if and only if:

(Def. 9) For all elements x, y, z of X holds $R(\langle x, y\rangle) \sqcap R(\langle y, z\rangle) \preceq R(\langle x, z\rangle)$.

Let X be a non empty set and let R be a membership function of X, X. We say that R is antisymmetric if and only if:

(Def. 10) For all elements x, y of X such that $R(\langle x, y\rangle) \neq 0$ and $R(\langle y, x\rangle) \neq 0$ holds $x = y$.

Let X be a non empty set and let R be a membership function of X, X. Let us observe that R is antisymmetric if and only if:

(Def. 11) For all elements x, y of X such that $R(\langle x, y\rangle) \neq 0$ and $x \neq y$ holds $R(\langle y, x\rangle) = 0$.

Let us consider X. Note that $\mathrm{Imf}(X, X)$ is symmetric, transitive, reflexive, and antisymmetric.

Let us consider X. Observe that there exists a membership function of X, X which is reflexive, transitive, symmetric, and antisymmetric.

Next we state two propositions:

(9) For all membership functions R, S of X, X such that R is symmetric and S is symmetric holds converse $\min(R, S) = \min(R, S)$.

(10) For all membership functions R, S of X, X such that R is symmetric and S is symmetric holds converse $\max(R, S) = \max(R, S)$.

Let us consider X and let R, S be symmetric membership functions of X, X. Note that $\min(R, S)$ is symmetric and $\max(R, S)$ is symmetric.

One can prove the following proposition

(11) For all membership functions R, S of X, X such that R is transitive and S is transitive holds $\min(R, S) \min(R, S) \subseteq \min(R, S)$.

Let us consider X and let R, S be transitive membership functions of X, X. Observe that $\min(R, S)$ is transitive.

Let A be a set and let X be a non empty set. Then $\chi_{A,X}$ is a membership function of X.

One can prove the following propositions:

(12) For every binary relation r on X such that r is reflexive in X holds $\chi_{r,[: X, X :]}$ is reflexive.

(13) For every binary relation r on X such that r is antisymmetric holds $\chi_{r,[: X, X :]}$ is antisymmetric.

(14) For every binary relation r on X such that r is symmetric holds $\chi_{r,[: X, X :]}$ is symmetric.

(15) For every binary relation r on X such that r is transitive holds $\chi_{r,[: X, X :]}$ is transitive.

(16) $\mathrm{Zmf}(X, X)$ is symmetric, antisymmetric, and transitive.

(17) $\mathrm{Umf}(X, X)$ is symmetric, transitive, and reflexive.

(18) For every membership function R of X, X holds $\max(R, \operatorname{converse} R)$ is symmetric.

(19) For every membership function R of X, X holds $\min(R, \operatorname{converse} R)$ is symmetric.

(20) Let R be a membership function of X, X and R' be a membership function of X, X. If R' is symmetric and $R \subseteq R'$, then $\max(R, \operatorname{converse} R) \subseteq R'$.

(21) Let R be a membership function of X, X and R' be a membership function of X, X. If R' is symmetric and $R' \subseteq R$, then $R' \subseteq \min(R, \operatorname{converse} R)$.

3. Transitive Closure

Let X be a non empty set, let R be a membership function of X, X, and let n be a natural number. The functor R^n yielding a membership function of X, X is defined by the condition (Def. 12).

(Def. 12) There exists a function F from $\mathbb{N}$ into $[0,1]^{[: X, X :]}$ such that

(i) $R^n = F(n)$,

(ii) $F(0) = \operatorname{Imf}(X, X)$, and

(iii) for every natural number k there exists a membership function Q of X, X such that $F(k) = Q$ and $F(k+1) = Q\,R$.

In the sequel X denotes a non empty set and R denotes a membership function of X, X.

Next we state several propositions:

(22) $\operatorname{Imf}(X, X)\,R = R$.

(23) $R\,\operatorname{Imf}(X, X) = R$.

(24) $R^0 = \operatorname{Imf}(X, X)$.

(25) $R^1 = R$.

(26) For every natural number n holds $R^{(n+1)} = R^n\,R$.

(27) For all natural numbers m, n holds $R^{(m+n)} = R^m\,R^n$.

(28) For all natural numbers m, n holds $R^{(m \cdot n)} = (R^n)^m$.

Let X be a non empty set and let R be a membership function of X, X. The functor $\operatorname{TrCl} R$ yields a membership function of X, X and is defined as follows:

(Def. 13) $\operatorname{TrCl} R = \bigsqcup_{\mathrm{FuzzyLattice}[: X, X :]} \{R^n; n \text{ ranges over natural numbers: } n > 0\}$.

Next we state several propositions:

(29) For all elements x, y of X holds $(\operatorname{TrCl} R)(\langle x, y \rangle) = \bigsqcup_{\mathrm{RealPoset}[0,1]} \pi_{\langle x, y \rangle} \{R^n; n \text{ ranges over natural numbers: } n > 0\}$.

(30) $R \subseteq \operatorname{TrCl} R$.

(31) For every natural number n such that $n > 0$ holds $R^n \subseteq \mathrm{TrCl}\,R$.

(32) For every subset Q of FuzzyLattice X and for every element x of X holds $(\bigsqcup_{\mathrm{FuzzyLattice}\,X} Q)(x) = \bigsqcup_{\mathrm{RealPoset}[0,1]} \pi_x Q$.

(33) Let R be a complete Heyting lattice, X be a subset of R, and y be an element of R. Then $y \sqcap \bigsqcup_R X = \bigsqcup_R \{y \sqcap x; x$ ranges over elements of R: $x \in X\}$.

(34) Let R be a membership function of X, X and Q be a subset of FuzzyLattice$[\!: X, X :\!]$. Then $R\,({}^{@}\bigsqcup_{\mathrm{FuzzyLattice}[: X, X :]} Q) = \bigsqcup_{\mathrm{FuzzyLattice}[: X, X :]} \{R\,({}^{@}r); r$ ranges over elements of FuzzyLattice$[\!: X, X :\!]$: $r \in Q\}$.

(35) Let R be a membership function of X, X and Q be a subset of FuzzyLattice$[\!: X, X :\!]$. Then $({}^{@}\bigsqcup_{\mathrm{FuzzyLattice}[: X, X :]} Q)\,R = \bigsqcup_{\mathrm{FuzzyLattice}[: X, X :]} \{({}^{@}r)\,R; r$ ranges over elements of FuzzyLattice$[\!: X, X :\!]$: $r \in Q\}$.

(36) Let R be a membership function of X, X. Then $\mathrm{TrCl}\,R\ \mathrm{TrCl}\,R = \bigsqcup_{\mathrm{FuzzyLattice}[: X, X :]} \{R^i\,R^j; i$ ranges over natural numbers, j ranges over natural numbers: $i > 0\ \wedge\ j > 0\}$.

Let X be a non empty set and let R be a membership function of X, X. Note that $\mathrm{TrCl}\,R$ is transitive.

We now state four propositions:

(37) Let R be a membership function of X, X and n be a natural number. If R is transitive and $n > 0$, then $R^n \subseteq R$.

(38) For every membership function R of X, X such that R is transitive holds $R = \mathrm{TrCl}\,R$.

(39) For all membership functions R, S of X, X and for every natural number n such that $R \subseteq S$ holds $R^n \subseteq S^n$.

(40) For all membership functions R, S of X, X such that S is transitive and $R \subseteq S$ holds $\mathrm{TrCl}\,R \subseteq S$.

References

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

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

[3] Grzegorz Bancerek. Sequences of ordinal numbers. *Formalized Mathematics*, 1(**2**):281–290, 1990.

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

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

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

[7] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.

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

[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[10] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[11] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[12] Czesław Byliński. Galois connections. *Formalized Mathematics*, 6(**1**):131–143, 1997.
[13] Noboru Endou, Takashi Mitsuishi, and Keiji Ohkubo. Properties of fuzzy relation. *Formalized Mathematics*, 9(**4**):691–695, 2001.
[14] Adam Grabowski and Robert Milewski. Boolean posets, posets under inclusion and products of relational structures. *Formalized Mathematics*, 6(**1**):117–121, 1997.
[15] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[16] Takashi Mitsuishi and Grzegorz Bancerek. Lattice of fuzzy sets. *Formalized Mathematics*, 11(**4**):393–398, 2003.
[17] Takashi Mitsuishi, Noboru Endou, and Yasunari Shidama. The concept of fuzzy set and membership function and basic properties of fuzzy set operation. *Formalized Mathematics*, 9(**2**):351–356, 2001.
[18] Takashi Mitsuishi, Katsumi Wasaki, and Yasunari Shidama. The concept of fuzzy relation and basic properties of its operation. *Formalized Mathematics*, 9(**3**):517–524, 2001.
[19] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.
[20] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.
[21] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[22] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[23] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[24] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[25] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[26] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[27] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Received November 23, 2003

FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

Basic Properties of Rough Sets and Rough Membership Function[1]

Adam Grabowski
University of Białystok

Summary. We present basic concepts concerning rough set theory. We define tolerance and approximation spaces and rough membership function. Different rough inclusions as well as the predicate of rough equality of sets are also introduced.

MML Identifier: `ROUGHS_1`.

The notation and terminology used here are introduced in the following papers: [21], [9], [25], [19], [1], [13], [22], [11], [20], [26], [28], [6], [2], [10], [5], [27], [8], [3], [15], [14], [7], [4], [16], [23], [24], [17], [18], and [12].

1. Preliminaries

Let A be a set. One can verify that $\langle A, \mathrm{id}_A \rangle$ is discrete.

The following proposition is true

(1) For every set X such that $\nabla_X \subseteq \mathrm{id}_X$ holds X is trivial.

Let A be a relational structure. We say that A is diagonal if and only if:

(Def. 1) The internal relation of $A \subseteq \mathrm{id}_{\text{the carrier of } A}$.

Let A be a non trivial set. Observe that $\langle A, \nabla_A \rangle$ is non diagonal.

We now state the proposition

(2) For every reflexive relational structure L holds $\mathrm{id}_{\text{the carrier of } L} \subseteq$ the internal relation of L.

[1]This work has been partially supported by the CALCULEMUS grant HPRN-CT-2000-00102.

ISSN 1426–2630

Let us note that every reflexive relational structure which is non discrete is also non trivial and every relational structure which is reflexive and trivial is also discrete.

One can prove the following proposition

(3) For every set X and for every total reflexive binary relation R on X holds $\mathrm{id}_X \subseteq R$.

One can verify that every relational structure which is discrete is also diagonal and every relational structure which is non diagonal is also non discrete.

One can verify that there exists a relational structure which is non diagonal and non empty.

We now state three propositions:

(4) Let A be a non diagonal non empty relational structure. Then there exist elements x, y of A such that $x \neq y$ and $\langle x, y \rangle \in$ the internal relation of A.

(5) For every set D and for all finite sequences p, q of elements of D holds $\bigcup(p \frown q) = \bigcup p \cup \bigcup q$.

(6) For all functions p, q such that q is disjoint valued and $p \subseteq q$ holds p is disjoint valued.

One can verify that every function which is empty is also disjoint valued.

Let A be a set. One can verify that there exists a finite sequence of elements of A which is disjoint valued.

Let A be a non empty set. Observe that there exists a finite sequence of elements of A which is non empty and disjoint valued.

Let A be a set, let X be a finite sequence of elements of 2^A, and let n be a natural number. Then $X(n)$ is a subset of A.

Let A be a set and let X be a finite sequence of elements of 2^A. Then $\bigcup X$ is a subset of A.

Let A be a finite set and let R be a binary relation on A. One can check that $\langle A, R \rangle$ is finite.

One can prove the following proposition

(7) For all sets X, x, y and for every tolerance T of X such that $x \in [y]_T$ holds $y \in [x]_T$.

2. Tolerance and Approximation Spaces

Let P be a relational structure. We say that P has equivalence relation if and only if:

(Def. 2) The internal relation of P is an equivalence relation of the carrier of P.

We say that P has tolerance relation if and only if:

(Def. 3) The internal relation of P is a tolerance of the carrier of P.

Let us note that every relational structure which has equivalence relation has also tolerance relation.

Let A be a set. Observe that $\langle A, \mathrm{id}_A \rangle$ has equivalence relation.

One can verify that there exists a relational structure which is discrete, finite, and non empty and has equivalence relation and there exists a relational structure which is non diagonal, finite, and non empty and has equivalence relation.

An approximation space is a non empty relational structure with equivalence relation. A tolerance space is a non empty relational structure with tolerance relation.

Let A be a tolerance space. Note that the internal relation of A is total, reflexive, and symmetric.

Let A be an approximation space. Observe that the internal relation of A is transitive.

Let A be a tolerance space and let X be a subset of A. The functor $\mathrm{LAp}(X)$ yielding a subset of A is defined as follows:

(Def. 4) $\mathrm{LAp}(X) = \{x; x$ ranges over elements of A: $[x]_{\text{the internal relation of } A} \subseteq X\}$.

The functor $\mathrm{UAp}(X)$ yielding a subset of A is defined as follows:

(Def. 5) $\mathrm{UAp}(X) = \{x; x$ ranges over elements of A: $[x]_{\text{the internal relation of } A}$ meets $X\}$.

Let A be a tolerance space and let X be a subset of A. The functor $\mathrm{BndAp}(X)$ yielding a subset of A is defined as follows:

(Def. 6) $\mathrm{BndAp}(X) = \mathrm{UAp}(X) \setminus \mathrm{LAp}(X)$.

Let A be a tolerance space and let X be a subset of A. We say that X is rough if and only if:

(Def. 7) $\mathrm{BndAp}(X) \neq \emptyset$.

We introduce X is exact as an antonym of X is rough.

In the sequel A is a tolerance space and X, Y are subsets of A.

Next we state a number of propositions:

(8) For every set x such that $x \in \mathrm{LAp}(X)$ holds $[x]_{\text{the internal relation of } A} \subseteq X$.

(9) For every element x of A such that $[x]_{\text{the internal relation of } A} \subseteq X$ holds $x \in \mathrm{LAp}(X)$.

(10) For every set x such that $x \in \mathrm{UAp}(X)$ holds $[x]_{\text{the internal relation of } A}$ meets X.

(11) For every element x of A such that $[x]_{\text{the internal relation of } A}$ meets X holds $x \in \mathrm{UAp}(X)$.

(12) $\mathrm{LAp}(X) \subseteq X$.

(13) $X \subseteq \mathrm{UAp}(X)$.

(14) $\mathrm{LAp}(X) \subseteq \mathrm{UAp}(X)$.

(15) X is exact iff $\mathrm{LAp}(X) = X$.

(16) X is exact iff $\mathrm{UAp}(X) = X$.

(17) $X = \mathrm{LAp}(X)$ iff $X = \mathrm{UAp}(X)$.

(18) $\mathrm{LAp}(\emptyset_A) = \emptyset$.

(19) $\mathrm{UAp}(\emptyset_A) = \emptyset$.

(20) $\mathrm{LAp}(\Omega_A) = \Omega_A$.

(21) $\mathrm{UAp}(\Omega_A) = \Omega_A$.

(22) $\mathrm{LAp}(X \cap Y) = \mathrm{LAp}(X) \cap \mathrm{LAp}(Y)$.

(23) $\mathrm{UAp}(X \cup Y) = \mathrm{UAp}(X) \cup \mathrm{UAp}(Y)$.

(24) If $X \subseteq Y$, then $\mathrm{LAp}(X) \subseteq \mathrm{LAp}(Y)$.

(25) If $X \subseteq Y$, then $\mathrm{UAp}(X) \subseteq \mathrm{UAp}(Y)$.

(26) $\mathrm{LAp}(X) \cup \mathrm{LAp}(Y) \subseteq \mathrm{LAp}(X \cup Y)$.

(27) $\mathrm{UAp}(X \cap Y) \subseteq \mathrm{UAp}(X) \cap \mathrm{UAp}(Y)$.

(28) $\mathrm{LAp}(X^{\mathrm{c}}) = (\mathrm{UAp}(X))^{\mathrm{c}}$.

(29) $\mathrm{UAp}(X^{\mathrm{c}}) = (\mathrm{LAp}(X))^{\mathrm{c}}$.

(30) $\mathrm{UAp}(\mathrm{LAp}(\mathrm{UAp}(X))) = \mathrm{UAp}(X)$.

(31) $\mathrm{LAp}(\mathrm{UAp}(\mathrm{LAp}(X))) = \mathrm{LAp}(X)$.

(32) $\mathrm{BndAp}(X) = \mathrm{BndAp}(X^{\mathrm{c}})$.

In the sequel A is an approximation space and X is a subset of A.

The following four propositions are true:

(33) $\mathrm{LAp}(\mathrm{LAp}(X)) = \mathrm{LAp}(X)$.

(34) $\mathrm{LAp}(\mathrm{LAp}(X)) = \mathrm{UAp}(\mathrm{LAp}(X))$.

(35) $\mathrm{UAp}(\mathrm{UAp}(X)) = \mathrm{UAp}(X)$.

(36) $\mathrm{UAp}(\mathrm{UAp}(X)) = \mathrm{LAp}(\mathrm{UAp}(X))$.

Let A be an approximation space. Note that there exists a subset of A which is exact.

Let A be an approximation space and let X be a subset of A. One can check that $\mathrm{LAp}(X)$ is exact and $\mathrm{UAp}(X)$ is exact.

The following proposition is true

(37) Let A be an approximation space, X be a subset of A, and x, y be sets. If $x \in \mathrm{UAp}(X)$ and $\langle x, y \rangle \in$ the internal relation of A, then $y \in \mathrm{UAp}(X)$.

Let A be a non diagonal approximation space. Observe that there exists a subset of A which is rough.

Let A be an approximation space and let X be a subset of A. Rough set of X is defined by:

(Def. 8) It $= \langle \mathrm{LAp}(X), \mathrm{UAp}(X) \rangle$.

3. Membership Function

Let A be a finite tolerance space and let x be an element of A. One can check that $\mathrm{card}([x]_{\text{the internal relation of } A})$ is non empty.

Let A be a finite tolerance space and let X be a subset of A. The functor $\mathrm{MemberFunc}(X, A)$ yielding a function from the carrier of A into $\mathbb{R}$ is defined by:

(Def. 9) For every element x of A holds $(\mathrm{MemberFunc}(X, A))(x) = \frac{\mathrm{card}(X \cap [x]_{\text{the internal relation of } A})}{\mathrm{card}([x]_{\text{the internal relation of } A})}$.

In the sequel A denotes a finite tolerance space, X denotes a subset of A, and x denotes an element of A.

One can prove the following propositions:

(38) $0 \leqslant (\mathrm{MemberFunc}(X, A))(x)$ and $(\mathrm{MemberFunc}(X, A))(x) \leqslant 1$.

(39) $(\mathrm{MemberFunc}(X, A))(x) \in [0, 1]$.

In the sequel A is a finite approximation space, X, Y are subsets of A, and x is an element of A.

We now state four propositions:

(40) $(\mathrm{MemberFunc}(X, A))(x) = 1$ iff $x \in \mathrm{LAp}(X)$.

(41) $(\mathrm{MemberFunc}(X, A))(x) = 0$ iff $x \in (\mathrm{UAp}(X))^{\mathrm{c}}$.

(42) $0 < (\mathrm{MemberFunc}(X, A))(x)$ and $(\mathrm{MemberFunc}(X, A))(x) < 1$ iff $x \in \mathrm{BndAp}(X)$.

(43) For every discrete approximation space A holds every subset of A is exact.

Let A be a discrete approximation space. Note that every subset of A is exact.

The following propositions are true:

(44) For every discrete finite approximation space A and for every subset X of A holds $\mathrm{MemberFunc}(X, A) = \chi_{X, \text{the carrier of } A}$.

(45) Let A be a finite approximation space, X be a subset of A, and x, y be sets. If $\langle x, y \rangle \in$ the internal relation of A, then $(\mathrm{MemberFunc}(X, A))(x) = (\mathrm{MemberFunc}(X, A))(y)$.

(46) $(\mathrm{MemberFunc}(X^{\mathrm{c}}, A))(x) = 1 - (\mathrm{MemberFunc}(X, A))(x)$.

(47) If $X \subseteq Y$, then $(\mathrm{MemberFunc}(X, A))(x) \leqslant (\mathrm{MemberFunc}(Y, A))(x)$.

(48) $(\mathrm{MemberFunc}(X \cup Y, A))(x) \geqslant (\mathrm{MemberFunc}(X, A))(x)$.

(49) $(\mathrm{MemberFunc}(X \cap Y, A))(x) \leqslant (\mathrm{MemberFunc}(X, A))(x)$.

(50) $(\mathrm{MemberFunc}(X \cup Y, A))(x) \geqslant \max((\mathrm{MemberFunc}(X, A))(x), (\mathrm{MemberFunc}(Y, A))(x))$.

(51) If X misses Y, then $(\mathrm{MemberFunc}(X \cup Y, A))(x) = (\mathrm{MemberFunc}(X, A))(x) + (\mathrm{MemberFunc}(Y, A))(x)$.

(52) $(\mathrm{MemberFunc}(X \cap Y, A))(x) \leqslant \min((\mathrm{MemberFunc}(X, A))(x), (\mathrm{MemberFunc}(Y, A))(x))$.

Let A be a finite tolerance space, let X be a finite sequence of elements of $2^{\text{the carrier of } A}$, and let x be an element of A. The functor $\mathrm{FinSeqM}(x, X)$ yields a finite sequence of elements of $\mathbb{R}$ and is defined as follows:

(Def. 10) $\operatorname{dom} \mathrm{FinSeqM}(x, X) = \operatorname{dom} X$ and for every natural number n such that $n \in \operatorname{dom} X$ holds $(\mathrm{FinSeqM}(x, X))(n) = (\mathrm{MemberFunc}(X(n), A))(x)$.

We now state several propositions:

(53) Let X be a finite sequence of elements of $2^{\text{the carrier of } A}$, x be an element of A, and y be an element of $2^{\text{the carrier of } A}$. Then $\mathrm{FinSeqM}(x, X \frown \langle y \rangle) = (\mathrm{FinSeqM}(x, X)) \frown \langle (\mathrm{MemberFunc}(y, A))(x) \rangle$.

(54) $(\mathrm{MemberFunc}(\emptyset_A, A))(x) = 0$.

(55) For every disjoint valued finite sequence X of elements of $2^{\text{the carrier of } A}$ holds $(\mathrm{MemberFunc}(\bigcup X, A))(x) = \sum \mathrm{FinSeqM}(x, X)$.

(56) $\mathrm{LAp}(X) = \{x; x$ ranges over elements of A: $(\mathrm{MemberFunc}(X, A))(x) = 1\}$.

(57) $\mathrm{UAp}(X) = \{x; x$ ranges over elements of A: $(\mathrm{MemberFunc}(X, A))(x) > 0\}$.

(58) $\mathrm{BndAp}(X) = \{x; x$ ranges over elements of A: $0 < (\mathrm{MemberFunc}(X, A))(x) \ \wedge \ (\mathrm{MemberFunc}(X, A))(x) < 1\}$.

4. Rough Inclusion

In the sequel A is a tolerance space and X, Y, Z are subsets of A.

Let A be a tolerance space and let X, Y be subsets of A. The predicate $X \subseteq_* Y$ is defined as follows:

(Def. 11) $\mathrm{LAp}(X) \subseteq \mathrm{LAp}(Y)$.

The predicate $X \subseteq^* Y$ is defined as follows:

(Def. 12) $\mathrm{UAp}(X) \subseteq \mathrm{UAp}(Y)$.

Let A be a tolerance space and let X, Y be subsets of A. The predicate $X \subseteq_*^* Y$ is defined as follows:

(Def. 13) $X \subseteq_* Y$ and $X \subseteq^* Y$.

One can prove the following three propositions:

(59) If $X \subseteq_* Y$ and $Y \subseteq_* Z$, then $X \subseteq_* Z$.

(60) If $X \subseteq^* Y$ and $Y \subseteq^* Z$, then $X \subseteq^* Z$.

(61) If $X \subseteq_*^* Y$ and $Y \subseteq_*^* Z$, then $X \subseteq_*^* Z$.

5. Rough Equality of Sets

Let A be a tolerance space and let X, Y be subsets of A. The predicate $X =_* Y$ is defined by:

(Def. 14) $\mathrm{LAp}(X) = \mathrm{LAp}(Y)$.

Let us notice that the predicate $X =_* Y$ is reflexive and symmetric. The predicate $X =^* Y$ is defined as follows:

(Def. 15) $\mathrm{UAp}(X) = \mathrm{UAp}(Y)$.

Let us notice that the predicate $X =^* Y$ is reflexive and symmetric. The predicate $X =_*^* Y$ is defined by:

(Def. 16) $\mathrm{LAp}(X) = \mathrm{LAp}(Y)$ and $\mathrm{UAp}(X) = \mathrm{UAp}(Y)$.

Let us notice that the predicate $X =_*^* Y$ is reflexive and symmetric.

Let A be a tolerance space and let X, Y be subsets of A. Let us observe that $X =_* Y$ if and only if:

(Def. 17) $X \subseteq_* Y$ and $Y \subseteq_* X$.

Let us observe that $X =^* Y$ if and only if:

(Def. 18) $X \subseteq^* Y$ and $Y \subseteq^* X$.

Let us observe that $X =_*^* Y$ if and only if:

(Def. 19) $X =_* Y$ and $X =^* Y$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[3] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[4] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.
[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[10] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[12] Adam Grabowski. On the category of posets. *Formalized Mathematics*, 5(**4**):501–505, 1996.
[13] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[14] Andrzej Nędzusiak. Probability. *Formalized Mathematics*, 1(**4**):745–749, 1990.
[15] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.
[16] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.

[17] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.
[18] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.
[19] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.
[20] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[21] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[22] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[23] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[24] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[25] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[26] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[27] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[28] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Received November 23, 2003

FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

Correctness of Non Overwriting Programs. Part I

Yatsuka Nakamura
Shinshu University
Nagano

Summary. Non overwriting program is a program where each variable used in it is written only just one time, but the control variables used for "for-statement" are exceptional. Contrarily, variables are allowed to be read many times. There are other restrictions for the non overwriting program. For statements, only the following are allowed: "substituting-statement", "if-else-statement", "for-statement" (with break and without break), function (correct one) – "call-statement" and "return-statement". Grammar of non overwriting program is like the one of the C-language. For type of variables, "int", "real", "char" and "float" can be used, and array of them can also be used. For operation, "+", "−" and "*" are used for a type "int"; "+", "−", "*" and "/" are used for a type "float". User can also define structures like in C. Non overwriting program can be translated to (predicative) logic formula in definition part to define functions. If a new function is correctly defined, a corresponding program is correct, if it does not use arrays. If it uses arrays, area check is necessary in the following theorem.

Semantic correctness is shown by some theorems following the definition. These theorems must tie up the result of the program and mathematical concepts introduced before. Correctness is proven *function-wise*. We must use only *correctness-proven* functions to define a new function (to write a new program as a form of a function). Here, we present two programs of division function of two natural numbers and of two integers. An algorithm is checked for each case by proving correctness of the definitions. We also perform an area check of the index of arrays used in one of the programs.

MML Identifier: `PRGCOR_1`.

The articles [6], [3], [2], [7], [5], [8], [1], and [4] provide the terminology and notation for this paper.

One can prove the following propositions:

ISSN 1426–2630

(1) For all natural numbers n, m, k holds $(n+k) -' (m+k) = n -' m$.

(2) For all natural numbers n, k such that $k > 0$ and $n \bmod 2 \cdot k \geqslant k$ holds $(n \bmod 2 \cdot k) - k = n \bmod k$ and $(n \bmod k) + k = n \bmod 2 \cdot k$.

(3) For all natural numbers n, k such that $k > 0$ and $n \bmod 2 \cdot k \geqslant k$ holds $n \div k = (n \div 2 \cdot k) \cdot 2 + 1$.

(4) For all natural numbers n, k such that $k > 0$ and $n \bmod 2 \cdot k < k$ holds $n \bmod 2 \cdot k = n \bmod k$.

(5) For all natural numbers n, k such that $k > 0$ and $n \bmod 2 \cdot k < k$ holds $n \div k = (n \div 2 \cdot k) \cdot 2$.

Let C be a set, let f be a partial function from C to $\mathbb{Z}$, and let x be a set. One can verify that $f(x)$ is integer.

Next we state two propositions:

(6) Let m, n be natural numbers. Suppose $m > 0$. Then there exists a natural number i such that for every natural number k_2 such that $k_2 < i$ holds $m \cdot 2^{k_2} \leqslant n$ and $m \cdot 2^i > n$.

(7) For every integer i and for every finite sequence f such that $1 \leqslant i$ and $i \leqslant \operatorname{len} f$ holds $i \in \operatorname{dom} f$.

Let n, m be integers. Let us assume that $n \geqslant 0$ and $m > 0$. The functor $\mathrm{Idiv1Prg}(n, m)$ yields an integer and is defined by the condition (Def. 1).

(Def. 1) There exist finite sequences s_1, s_2, p_1 of elements of $\mathbb{Z}$ such that

(i) $\operatorname{len} s_1 = n + 1$,

(ii) $\operatorname{len} s_2 = n + 1$,

(iii) $\operatorname{len} p_1 = n + 1$,

(iv) if $n < m$, then $\mathrm{Idiv1Prg}(n, m) = 0$, and

(v) if $n \not< m$, then $s_1(1) = m$ and there exists an integer i such that $1 \leqslant i$ and $i \leqslant n$ and for every integer k such that $1 \leqslant k$ and $k < i$ holds $s_1(k+1) = s_1(k) \cdot 2$ and $s_1(k+1) \not> n$ and $s_1(i+1) = s_1(i) \cdot 2$ and $s_1(i+1) > n$ and $p_1(i+1) = 0$ and $s_2(i+1) = n$ and for every integer j such that $1 \leqslant j$ and $j \leqslant i$ holds if $s_2((i+1)-(j-1)) \geqslant s_1((i+1)-j)$, then $s_2((i+1)-j) = s_2((i+1)-(j-1)) - s_1((i+1)-j)$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2 + 1$ and if $s_2((i+1)-(j-1)) \not\geqslant s_1((i+1)-j)$, then $s_2((i+1)-j) = s_2((i+1)-(j-1))$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2$ and $\mathrm{Idiv1Prg}(n, m) = p_1(1)$.

Next we state four propositions:

(8) Let n, m be integers. Suppose $n \geqslant 0$ and $m > 0$. Let s_1, s_2, p_1 be finite sequences of elements of $\mathbb{Z}$ and i be an integer. Suppose that

(i) $\operatorname{len} s_1 = n + 1$,

(ii) $\operatorname{len} s_2 = n + 1$,

(iii) $\operatorname{len} p_1 = n + 1$, and

(iv) if $n \not< m$, then $s_1(1) = m$ and $1 \leqslant i$ and $i \leqslant n$ and for every integer k such that $1 \leqslant k$ and $k < i$ holds $s_1(k+1) = s_1(k) \cdot 2$ and $s_1(k+1) \not> n$ and $s_1(i+1) = s_1(i) \cdot 2$ and $s_1(i+1) > n$ and $p_1(i+1) = 0$ and $s_2(i+1) = n$ and for every integer j such that $1 \leqslant j$ and $j \leqslant i$ holds if $s_2((i+1)-(j-1)) \geqslant s_1((i+1)-j)$, then $s_2((i+1)-j) = s_2((i+1)-(j-1)) - s_1((i+1)-j)$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2 + 1$ and if $s_2((i+1)-(j-1)) \not\geqslant s_1((i+1)-j)$, then $s_2((i+1)-j) = s_2((i+1)-(j-1))$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2$ and $\mathrm{Idiv1Prg}(n,m) = p_1(1)$.

Then

(v) $\mathrm{len}\, s_1 = n+1$,

(vi) $\mathrm{len}\, s_2 = n+1$,

(vii) $\mathrm{len}\, p_1 = n+1$,

(viii) if $n < m$, then $\mathrm{Idiv1Prg}(n,m) = 0$, and

(ix) if $n \not< m$, then $1 \in \mathrm{dom}\, s_1$ and $s_1(1) = m$ and $1 \leqslant i$ and $i \leqslant n$ and for every integer k such that $1 \leqslant k$ and $k < i$ holds $k+1 \in \mathrm{dom}\, s_1$ and $k \in \mathrm{dom}\, s_1$ and $s_1(k+1) = s_1(k) \cdot 2$ and $s_1(k+1) \not> n$ and $i+1 \in \mathrm{dom}\, s_1$ and $i \in \mathrm{dom}\, s_1$ and $s_1(i+1) = s_1(i) \cdot 2$ and $s_1(i+1) > n$ and $i+1 \in \mathrm{dom}\, p_1$ and $p_1(i+1) = 0$ and $i+1 \in \mathrm{dom}\, s_2$ and $s_2(i+1) = n$ and for every integer j such that $1 \leqslant j$ and $j \leqslant i$ holds $(i+1)-(j-1) \in \mathrm{dom}\, s_2$ and $(i+1)-j \in \mathrm{dom}\, s_1$ and if $s_2((i+1)-(j-1)) \geqslant s_1((i+1)-j)$, then $(i+1)-j \in \mathrm{dom}\, s_2$ and $(i+1)-j \in \mathrm{dom}\, s_1$ and $s_2((i+1)-j) = s_2((i+1)-(j-1)) - s_1((i+1)-j)$ and $(i+1)-j \in \mathrm{dom}\, p_1$ and $(i+1)-(j-1) \in \mathrm{dom}\, p_1$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2 + 1$ and if $s_2((i+1)-(j-1)) \not\geqslant s_1((i+1)-j)$, then $(i+1)-j \in \mathrm{dom}\, s_2$ and $(i+1)-(j-1) \in \mathrm{dom}\, s_2$ and $s_2((i+1)-j) = s_2((i+1)-(j-1))$ and $(i+1)-j \in \mathrm{dom}\, p_1$ and $(i+1)-(j-1) \in \mathrm{dom}\, p_1$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2$ and $1 \in \mathrm{dom}\, p_1$ and $\mathrm{Idiv1Prg}(n,m) = p_1(1)$.

(9) For all natural numbers n, m such that $m > 0$ holds $\mathrm{Idiv1Prg}((n$ **qua** integer$), (m$ **qua** integer$)) = n \div m$.

(10) For all integers n, m such that $n \geqslant 0$ and $m > 0$ holds $\mathrm{Idiv1Prg}(n,m) = n \div m$.

(11) Let n, m be integers and n_2, m_2 be natural numbers. Then

(i) if $m = 0$ and $n_2 = n$ and $m_2 = m$, then $n \div m = 0$ and $n_2 \div m_2 = 0$,

(ii) if $n \geqslant 0$ and $m > 0$ and $n_2 = n$ and $m_2 = m$, then $n \div m = n_2 \div m_2$,

(iii) if $n \geqslant 0$ and $m < 0$ and $n_2 = n$ and $m_2 = -m$, then if $m_2 \cdot (n_2 \div m_2) = n_2$, then $n \div m = -(n_2 \div m_2)$ and if $m_2 \cdot (n_2 \div m_2) \neq n_2$, then $n \div m = -(n_2 \div m_2) - 1$,

(iv) if $n < 0$ and $m > 0$ and $n_2 = -n$ and $m_2 = m$, then if $m_2 \cdot (n_2 \div m_2) = n_2$, then $n \div m = -(n_2 \div m_2)$ and if $m_2 \cdot (n_2 \div m_2) \neq n_2$, then $n \div m = -(n_2 \div m_2) - 1$, and

(v) if $n < 0$ and $m < 0$ and $n_2 = -n$ and $m_2 = -m$, then $n \div m = n_2 \div m_2$.

Let n, m be integers. The functor $\mathrm{IdivPrg}(n, m)$ yields an integer and is defined by the condition (Def. 2).

(Def. 2) There exists an integer i such that

(i) if $m = 0$, then $\mathrm{IdivPrg}(n, m) = 0$, and

(ii) if $m \neq 0$, then if $n \geqslant 0$ and $m > 0$, then $\mathrm{IdivPrg}(n, m) = \mathrm{Idiv1Prg}(n, m)$ and if $n \not\geqslant 0$ or $m \not> 0$, then if $n \geqslant 0$ and $m < 0$, then $i = \mathrm{Idiv1Prg}(n, -m)$ and if $(-m) \cdot i = n$, then $\mathrm{IdivPrg}(n, m) = -i$ and if $(-m) \cdot i \neq n$, then $\mathrm{IdivPrg}(n, m) = -i - 1$ and if $n \not\geqslant 0$ or $m \not< 0$, then if $n < 0$ and $m > 0$, then $i = \mathrm{Idiv1Prg}(-n, m)$ and if $m \cdot i = -n$, then $\mathrm{IdivPrg}(n, m) = -i$ and if $m \cdot i \neq -n$, then $\mathrm{IdivPrg}(n, m) = -i - 1$ and if $n \not< 0$ or $m \not> 0$, then $\mathrm{IdivPrg}(n, m) = \mathrm{Idiv1Prg}(-n, -m)$.

The following proposition is true

(12) For all integers n, m holds $\mathrm{IdivPrg}(n, m) = n \div m$.

References

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

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

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

[4] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Formalized Mathematics*, 7(**1**):123–126, 1998.

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

[6] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

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

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

Received December 5, 2003

FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

A Tree of Execution of a Macroinstruction[1]

Artur Korniłowicz
University of Białystok

Summary. A tree of execution of a macroinstruction is defined. It is a tree decorated by the instruction locations of a computer. Successors of each vertex are determined by the set of all possible values of the instruction counter after execution of the instruction placed in the location indicated by given vertex.

MML Identifier: `AMISTD_3`.

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

For simplicity, we adopt the following convention: x, y, X are sets, m, n are natural numbers, O is an ordinal number, and R, S are binary relations.

Let D be a set, let f be a partial function from D to $\mathbb{N}$, and let n be a set. One can verify that $f(n)$ is natural.

Let R be an empty binary relation and let X be a set. Observe that $R{\restriction}X$ is empty.

One can prove the following two propositions:

(1) If $\operatorname{dom} R = \{x\}$ and $\operatorname{rng} R = \{y\}$, then $R = x \dot{\longmapsto} y$.

(2) $\operatorname{field}\{\langle x, x\rangle\} = \{x\}$.

Let X be an infinite set and let a be a set. One can verify that $X \longmapsto a$ is infinite.

One can check that there exists a function which is infinite.

Let R be a finite binary relation. One can verify that $\operatorname{field} R$ is finite.

The following proposition is true

(3) If $\operatorname{field} R$ is finite, then R is finite.

[1]The paper was written during author's post-doctoral fellowship granted by Shinshu University, Japan.

ISSN 1426–2630

Let R be an infinite binary relation. Note that field R is infinite.

One can prove the following proposition

(4) If $\operatorname{dom} R$ is finite and $\operatorname{rng} R$ is finite, then R is finite.

Let us observe that $\subseteq_{\emptyset}$ is empty.

Let X be a non empty set. One can verify that $\subseteq_X$ is non empty.

Next we state two propositions:

(5) $\subseteq_{\{x\}} = \{\langle x, x\rangle\}$.

(6) $\subseteq_X \subseteq [\!: X, X :\!]$.

Let X be a finite set. Note that $\subseteq_X$ is finite.

One can prove the following proposition

(7) If $\subseteq_X$ is finite, then X is finite.

Let X be an infinite set. One can verify that $\subseteq_X$ is infinite.

The following propositions are true:

(8) If R and S are isomorphic and R is well-ordering, then S is well-ordering.

(9) If R and S are isomorphic and R is finite, then S is finite.

(10) $x \dot{\longmapsto} y$ is an isomorphism between $\{\langle x, x\rangle\}$ and $\{\langle y, y\rangle\}$.

(11) $\{\langle x, x\rangle\}$ and $\{\langle y, y\rangle\}$ are isomorphic.

One can verify that $\overline{\emptyset}$ is empty.

The following propositions are true:

(12) $\overline{\subseteq_O} = O$.

(13) For every finite set X such that $X \subseteq O$ holds $\overline{\subseteq_X} = \operatorname{card} X$.

(14) If $\{x\} \subseteq O$, then $\overline{\subseteq_{\{x\}}} = 1$.

(15) If $\{x\} \subseteq O$, then the canonical isomorphism between $\subseteq_{\overline{\subseteq_{\{x\}}}}$ and $\subseteq_{\{x\}}$ $=$ $0 \dot{\longmapsto} x$.

Let O be an ordinal number, let X be a subset of O, and let n be a set. One can check that (the canonical isomorphism between $\subseteq_{\overline{\subseteq_X}}$ and $\subseteq_X)(n)$ is ordinal.

Let X be a natural-membered set and let n be a set. Note that (the canonical isomorphism between $\subseteq_{\overline{\subseteq_X}}$ and $\subseteq_X)(n)$ is natural.

Next we state three propositions:

(16) If $n \mapsto x = m \mapsto x$, then $n = m$.

(17) For every tree T and for every element t of T holds $t \restriction \operatorname{Seg} n \in T$.

(18) For all trees T_1, T_2 such that for every natural number n holds $T_1\text{-level}(n) = T_2\text{-level}(n)$ holds $T_1 = T_2$.

The functor TrivialInfiniteTree is defined by:

(Def. 1) $\text{TrivialInfiniteTree} = \{k \mapsto 0 : k \text{ ranges over natural numbers}\}$.

One can check that TrivialInfiniteTree is non empty and tree-like.

We now state the proposition

(19) $\mathbb{N} \approx \text{TrivialInfiniteTree}$.

Let us note that TrivialInfiniteTree is infinite.

The following proposition is true

(20) For every natural number n holds TrivialInfiniteTree-level$(n) = \{n \mapsto 0\}$.

For simplicity, we adopt the following convention: N denotes a set with non empty elements, S denotes a standard IC-Ins-separated definite non empty non void AMI over N, L, l_1 denote instruction-locations of S, J denotes an instruction of S, and F denotes a subset of the instruction locations of S.

Let N be a set with non empty elements, let S be a standard IC-Ins-separated definite non empty non void AMI over N, and let F be a finite partial state of S. Let us assume that F is non empty and F is programmed. The functor FirstLoc(F) yields an instruction-location of S and is defined by the condition (Def. 2).

(Def. 2) There exists a non empty subset M of $\mathbb{N}$ such that $M = \{\mathrm{locnum}(l); l$ ranges over elements of the instruction locations of S: $l \in \mathrm{dom}\, F\}$ and FirstLoc$(F) = \mathrm{il}_S(\min M)$.

One can prove the following four propositions:

(21) For every non empty programmed finite partial state F of S holds FirstLoc$(F) \in \mathrm{dom}\, F$.

(22) For all non empty programmed finite partial states F, G of S such that $F \subseteq G$ holds FirstLoc$(G) \leqslant$ FirstLoc(F).

(23) For every non empty programmed finite partial state F of S such that $l_1 \in \mathrm{dom}\, F$ holds FirstLoc$(F) \leqslant l_1$.

(24) For every lower non empty programmed finite partial state F of S holds FirstLoc$(F) = \mathrm{il}_S(0)$.

Let N be a set with non empty elements, let S be a standard IC-Ins-separated definite non empty non void AMI over N, and let F be a subset of the instruction locations of S. The functor LocNums(F) yields a subset of $\mathbb{N}$ and is defined by:

(Def. 3) LocNums$(F) = \{\mathrm{locnum}(l); l$ ranges over instruction-locations of S: $l \in F\}$.

We now state the proposition

(25) $\mathrm{locnum}(l_1) \in$ LocNums(F) iff $l_1 \in F$.

Let N be a set with non empty elements, let S be a standard IC-Ins-separated definite non empty non void AMI over N, and let F be an empty subset of the instruction locations of S. Observe that LocNums(F) is empty.

Let N be a set with non empty elements, let S be a standard IC-Ins-separated definite non empty non void AMI over N, and let F be a non empty subset of the instruction locations of S. Observe that LocNums(F) is non empty.

We now state several propositions:

(26) If $F = \{\mathrm{il}_S(n)\}$, then LocNums$(F) = \{n\}$.

(27) $F \approx \mathrm{LocNums}(F)$.

(28) $\overline{\overline{F}} \subseteq \overline{\subseteq_{\mathrm{LocNums}(F)}}$.

(29) If S is realistic and J is halting, then $\mathrm{LocNums}(\mathrm{NIC}(J, L)) = \{\mathrm{locnum}(L)\}$.

(30) If S is realistic and J is sequential, then $\mathrm{LocNums}(\mathrm{NIC}(J, L)) = \{\mathrm{locnum}(\mathrm{NextLoc}\, L)\}$.

Let N be a set with non empty elements, let S be a standard IC-Ins-separated definite non empty non void AMI over N, and let M be a subset of the instruction locations of S. The functor $\mathrm{LocSeq}(M)$ yielding a transfinite sequence of elements of the instruction locations of S is defined as follows:

(Def. 4) $\mathrm{dom}\,\mathrm{LocSeq}(M) = \overline{\overline{M}}$ and for every set m such that $m \in \overline{\overline{M}}$ holds $(\mathrm{LocSeq}(M))(m) = \mathrm{il}_S$((the canonical isomorphism between $\subseteq_{\overline{\subseteq_{\mathrm{LocNums}(M)}}}$ and $\subseteq_{\mathrm{LocNums}(M)})(m))$.

One can prove the following proposition

(31) If $F = \{\mathrm{il}_S(n)\}$, then $\mathrm{LocSeq}(F) = 0 \mapsto \mathrm{il}_S(n)$.

Let N be a set with non empty elements, let S be a standard IC-Ins-separated definite non empty non void AMI over N, and let M be a subset of the instruction locations of S. Note that $\mathrm{LocSeq}(M)$ is one-to-one.

Let N be a set with non empty elements, let S be a standard IC-Ins-separated definite non empty non void AMI over N, and let M be a finite partial state of S. The functor $\mathrm{ExecTree}(M)$ yields a tree decorated with elements of the instruction locations of S and is defined by the conditions (Def. 5).

(Def. 5)(i) $(\mathrm{ExecTree}(M))(\emptyset) = \mathrm{FirstLoc}(M)$, and

(ii) for every element t of $\mathrm{dom}\,\mathrm{ExecTree}(M)$ holds $\mathrm{succ}\, t = \{t ^\frown \langle k \rangle; k$ ranges over natural numbers: $k \in \overline{\overline{\mathrm{NIC}(\pi_{(\mathrm{ExecTree}(M))(t)} M, (\mathrm{ExecTree}(M))(t))}}\}$ and for every natural number m such that $m \in \overline{\overline{\mathrm{NIC}(\pi_{(\mathrm{ExecTree}(M))(t)} M, (\mathrm{ExecTree}(M))(t))}}$ holds $(\mathrm{ExecTree}(M))(t ^\frown \langle m \rangle) = (\mathrm{LocSeq}(\mathrm{NIC}(\pi_{(\mathrm{ExecTree}(M))(t)} M, (\mathrm{ExecTree}(M))(t))))(m)$.

One can prove the following proposition

(32) For every standard halting realistic IC-Ins-separated definite non empty non void AMI S over N holds $\mathrm{ExecTree}(\mathrm{Stop}\, S) = \mathrm{TrivialInfiniteTree} \longmapsto \mathrm{il}_S(0)$.

Acknowledgments

The author wishes to thank Andrzej Trybulec and Grzegorz Bancerek for their very useful comments during writing this article.

References

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

[2] Grzegorz Bancerek. Introduction to trees. *Formalized Mathematics*, 1(**2**):421–427, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek. Sequences of ordinal numbers. *Formalized Mathematics*, 1(**2**):281–290, 1990.
[5] Grzegorz Bancerek. The well ordering relations. *Formalized Mathematics*, 1(**1**):123–129, 1990.
[6] Grzegorz Bancerek. Zermelo theorem and axiom of choice. *Formalized Mathematics*, 1(**2**):265–267, 1990.
[7] Grzegorz Bancerek. König's lemma. *Formalized Mathematics*, 2(**3**):397–402, 1991.
[8] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[9] Czesław Byliński. A classical first order language. *Formalized Mathematics*, 1(**4**):669–676, 1990.
[10] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[11] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[12] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[13] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[14] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[15] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[16] Agata Darmochwał and Andrzej Trybulec. Similarity of formulae. *Formalized Mathematics*, 2(**5**):635–642, 1991.
[17] Artur Korniłowicz. On the composition of macro instructions of standard computers. *Formalized Mathematics*, 9(**2**):303–316, 2001.
[18] Yatsuka Nakamura and Andrzej Trybulec. A mathematical model of CPU. *Formalized Mathematics*, 3(**2**):151–160, 1992.
[19] Yasushi Tanaka. On the decomposition of the states of SCM. *Formalized Mathematics*, 5(**1**):1–8, 1996.
[20] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.
[21] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[22] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[23] Andrzej Trybulec and Yatsuka Nakamura. Some remarks on the simple concrete model of computer. *Formalized Mathematics*, 4(**1**):51–56, 1993.
[24] Andrzej Trybulec, Piotr Rudnicki, and Artur Korniłowicz. Standard ordering of instruction locations. *Formalized Mathematics*, 9(**2**):291–301, 2001.
[25] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[26] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received December 10, 2003

FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

Banach Space of Bounded Linear Operators

Yasunari Shidama
Shinshu University
Nagano

Summary. In this article, the basic properties of linear spaces which are defined as the set of all linear operators from one linear space to another, are described. Especially, the Banach space is introduced. This is defined by the set of all bounded linear operators.

MML Identifier: `LOPBAN_1`.

The notation and terminology used in this paper are introduced in the following articles: [26], [6], [24], [31], [27], [33], [32], [4], [5], [16], [23], [22], [3], [1], [2], [21], [28], [9], [7], [30], [14], [25], [17], [29], [19], [18], [8], [20], [13], [11], [12], [10], and [15].

1. Real Vector Space of Operators

Let X be a set, let Y be a non empty set, let F be a function from $[:\mathbb{R}, Y:]$ into Y, let a be a real number, and let f be a function from X into Y. Then $F^\circ(a, f)$ is an element of Y^X.

One can prove the following propositions:

(1) Let X be a non empty set and Y be a non empty loop structure. Then there exists a binary operation A_1 on (the carrier of $Y)^X$ such that for all elements f, g of (the carrier of $Y)^X$ holds $A_1(f, g) =$ (the addition of $Y)^\circ(f, g)$.

(2) Let X be a non empty set and Y be a real linear space. Then there exists a function M_1 from $[:\mathbb{R}$, (the carrier of $Y)^X:]$ into (the carrier of $Y)^X$ such that for every real number r and for every element f of (the carrier of $Y)^X$ and for every element s of X holds $M_1(\langle r, f\rangle)(s) = r \cdot f(s)$.

ISSN 1426–2630

Let X be a non empty set and let Y be a non empty loop structure. The functor $\mathrm{FuncAdd}(X, Y)$ yields a binary operation on (the carrier of $Y)^X$ and is defined by:

(Def. 1) For all elements f, g of (the carrier of $Y)^X$ holds $(\mathrm{FuncAdd}(X, Y))(f, g) =$ (the addition of $Y)^\circ(f, g)$.

Let X be a non empty set and let Y be a real linear space. The functor $\mathrm{FuncExtMult}(X, Y)$ yields a function from $[\!:\mathbb{R}$, (the carrier of $Y)^X :\!]$ into (the carrier of $Y)^X$ and is defined by the condition (Def. 2).

(Def. 2) Let a be a real number, f be an element of (the carrier of $Y)^X$, and x be an element of X. Then $(\mathrm{FuncExtMult}(X, Y))(\langle a, f\rangle)(x) = a \cdot f(x)$.

Let X be a set and let Y be a non empty zero structure. The functor $\mathrm{FuncZero}(X, Y)$ yielding an element of (the carrier of $Y)^X$ is defined as follows:

(Def. 3) $\mathrm{FuncZero}(X, Y) = X \longmapsto 0_Y$.

We adopt the following rules: X is a non empty set, Y is a real linear space, and f, g, h are elements of (the carrier of $Y)^X$.

The following two propositions are true:

(3) Let Y be a non empty loop structure and f, g, h be elements of (the carrier of $Y)^X$. Then $h = (\mathrm{FuncAdd}(X, Y))(f, g)$ if and only if for every element x of X holds $h(x) = f(x) + g(x)$.

(4) For every element x of X holds $(\mathrm{FuncZero}(X, Y))(x) = 0_Y$.

In the sequel a, b are real numbers.

The following propositions are true:

(5) $h = (\mathrm{FuncExtMult}(X, Y))(\langle a, f\rangle)$ iff for every element x of X holds $h(x) = a \cdot f(x)$.

(6) $(\mathrm{FuncAdd}(X, Y))(f, g) = (\mathrm{FuncAdd}(X, Y))(g, f)$.

(7) $(\mathrm{FuncAdd}(X, Y))(f, (\mathrm{FuncAdd}(X, Y))(g, h)) = (\mathrm{FuncAdd}(X, Y))((\mathrm{FuncAdd}(X, Y))(f, g), h)$.

(8) $(\mathrm{FuncAdd}(X, Y))(\mathrm{FuncZero}(X, Y), f) = f$.

(9) $(\mathrm{FuncAdd}(X, Y))(f, (\mathrm{FuncExtMult}(X, Y))(\langle -1, f\rangle)) = \mathrm{FuncZero}(X, Y)$.

(10) $(\mathrm{FuncExtMult}(X, Y))(\langle 1, f\rangle) = f$.

(11) $(\mathrm{FuncExtMult}(X, Y))(\langle a, (\mathrm{FuncExtMult}(X, Y))(\langle b, f\rangle)\rangle) = (\mathrm{FuncExtMult}(X, Y))(\langle a \cdot b, f\rangle)$.

(12) $(\mathrm{FuncAdd}(X, Y))((\mathrm{FuncExtMult}(X, Y))(\langle a, f\rangle), (\mathrm{FuncExtMult}(X, Y))(\langle b, f\rangle)) = (\mathrm{FuncExtMult}(X, Y))(\langle a + b, f\rangle)$.

(13) $\langle$(the carrier of $Y)^X, \mathrm{FuncZero}(X, Y), \mathrm{FuncAdd}(X, Y), \mathrm{FuncExtMult}(X, Y)\rangle$ is a real linear space.

Let X be a non empty set and let Y be a real linear space. The functor $\mathrm{RealVectSpace}(X, Y)$ yields a real linear space and is defined as follows:

(Def. 4) RealVectSpace$(X, Y) = \langle$(the carrier of $Y)^X$, FuncZero(X, Y), FuncAdd(X, Y), FuncExtMult$(X, Y)\rangle$.

Let X be a non empty set and let Y be a real linear space. One can check that RealVectSpace(X, Y) is strict.

Let X be a non empty set and let Y be a real linear space. Note that every vector of RealVectSpace(X, Y) is function-like and relation-like.

Let X be a non empty set, let Y be a real linear space, let f be a vector of RealVectSpace(X, Y), and let x be an element of X. Then $f(x)$ is a vector of Y.

One can prove the following propositions:

(14) Let X be a non empty set, Y be a real linear space, and f, g, h be vectors of RealVectSpace(X, Y). Then $h = f + g$ if and only if for every element x of X holds $h(x) = f(x) + g(x)$.

(15) Let X be a non empty set, Y be a real linear space, f, h be vectors of RealVectSpace(X, Y), and a be a real number. Then $h = a \cdot f$ if and only if for every element x of X holds $h(x) = a \cdot f(x)$.

(16) For every non empty set X and for every real linear space Y holds $0_{\mathrm{RealVectSpace}(X,Y)} = X \longmapsto 0_Y$.

2. Real Vector Space of Linear Operators

Let X be a non empty RLS structure, let Y be a non empty loop structure, and let I_1 be a function from X into Y. We say that I_1 is additive if and only if:

(Def. 5) For all vectors x, y of X holds $I_1(x + y) = I_1(x) + I_1(y)$.

Let X, Y be non empty RLS structures and let I_1 be a function from X into Y. We say that I_1 is homogeneous if and only if:

(Def. 6) For every vector x of X and for every real number r holds $I_1(r \cdot x) = r \cdot I_1(x)$.

Let X be a non empty RLS structure and let Y be a real linear space. Note that there exists a function from X into Y which is additive and homogeneous.

Let X, Y be real linear spaces. A linear operator from X into Y is an additive homogeneous function from X into Y.

Let X, Y be real linear spaces. The functor LinearOperators(X, Y) yields a subset of RealVectSpace(the carrier of X, Y) and is defined as follows:

(Def. 7) For every set x holds $x \in$ LinearOperators(X, Y) iff x is a linear operator from X into Y.

Let X, Y be real linear spaces. Note that LinearOperators(X, Y) is non empty.

One can prove the following propositions:

(17) For all real linear spaces X, Y holds LinearOperators(X,Y) is linearly closed.

(18) Let X, Y be real linear spaces. Then $\langle$LinearOperators(X,Y), Zero_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y)), Add_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y)), Mult_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y))$\rangle$ is a subspace of RealVectSpace(the carrier of X, Y).

Let X, Y be real linear spaces. One can verify that $\langle$LinearOperators(X,Y), Zero_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y)), Add_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y)), Mult_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y))$\rangle$ is Abelian, add-associative, right zeroed, right complementable, and real linear space-like.

One can prove the following proposition

(19) Let X, Y be real linear spaces. Then $\langle$LinearOperators(X,Y), Zero_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y)), Add_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y)), Mult_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y))$\rangle$ is a real linear space.

Let X, Y be real linear spaces. The functor RVectorSpaceOfLinearOperators (X,Y) yielding a real linear space is defined as follows:

(Def. 8) RVectorSpaceOfLinearOperators$(X,Y) = \langle$LinearOperators(X,Y), Zero_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y)), Add_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y)), Mult_(LinearOperators(X,Y), RealVectSpace(the carrier of X, Y))$\rangle$.

Let X, Y be real linear spaces. Observe that RVectorSpaceOfLinearOperators (X,Y) is strict.

Let X, Y be real linear spaces. Note that every element of RVectorSpaceOfLinearOperators(X,Y) is function-like and relation-like.

Let X, Y be real linear spaces, let f be an element of RVectorSpaceOfLinearOperators(X,Y), and let v be a vector of X. Then $f(v)$ is a vector of Y.

We now state four propositions:

(20) Let X, Y be real linear spaces and f, g, h be vectors of RVectorSpaceOfLinearOperators(X,Y). Then $h = f + g$ if and only if for every vector x of X holds $h(x) = f(x) + g(x)$.

(21) Let X, Y be real linear spaces, f, h be vectors of RVectorSpaceOfLinearOperators(X,Y), and a be a real number. Then $h = a \cdot f$ if and only if for every vector x of X holds $h(x) = a \cdot f(x)$.

(22) For all real linear spaces X, Y holds $0_{\mathrm{RVectorSpaceOfLinearOperators}(X,Y)} =$ (the carrier of X) $\longmapsto 0_Y$.

(23) For all real linear spaces X, Y holds (the carrier of X) $\longmapsto 0_Y$ is a linear operator from X into Y.

3. Real Normed Linear Space of Bounded Linear Operators

One can prove the following proposition

(24) Let X be a real normed space, s_1 be a sequence of X, and g be a point of X. If s_1 is convergent and $\lim s_1 = g$, then $\|s_1\|$ is convergent and $\lim\|s_1\| = \|g\|$.

Let X, Y be real normed spaces and let I_1 be a linear operator from X into Y. We say that I_1 is bounded if and only if:

(Def. 9) There exists a real number K such that $0 \leqslant K$ and for every vector x of X holds $\|I_1(x)\| \leqslant K \cdot \|x\|$.

Next we state the proposition

(25) Let X, Y be real normed spaces and f be a linear operator from X into Y. If for every vector x of X holds $f(x) = 0_Y$, then f is bounded.

Let X, Y be real normed spaces. One can check that there exists a linear operator from X into Y which is bounded.

Let X, Y be real normed spaces. The functor BoundedLinearOperators(X, Y) yields a subset of RVectorSpaceOfLinearOperators(X, Y) and is defined by:

(Def. 10) For every set x holds $x \in$ BoundedLinearOperators(X, Y) iff x is a bounded linear operator from X into Y.

Let X, Y be real normed spaces. One can verify that BoundedLinearOperators (X, Y) is non empty.

One can prove the following two propositions:

(26) For all real normed spaces X, Y holds BoundedLinearOperators(X, Y) is linearly closed.

(27) For all real normed spaces X, Y holds $\langle$BoundedLinearOperators(X, Y), Zero_(BoundedLinearOperators(X, Y), RVectorSpaceOfLinearOperators (X, Y)), Add_(BoundedLinearOperators(X, Y), RVectorSpaceOfLinearOperators(X, Y)), Mult_(BoundedLinearOperators (X, Y), RVectorSpaceOfLinearOperators(X, Y))$\rangle$ is a subspace of RVectorSpaceOfLinearOperators(X, Y).

Let X, Y be real normed spaces.

Observe that $\langle$BoundedLinearOperators(X, Y), Zero_(BoundedLinearOperators(X, Y), RVectorSpaceOfLinearOperators(X, Y)), Add_(BoundedLinearOperators(X, Y), RVectorSpaceOfLinearOperators (X, Y)), Mult_(BoundedLinearOperators(X, Y), RVectorSpaceOfLinearOperators$(X, Y))\rangle$ is Abelian, add-associative, right zeroed, right complementable, and real linear space-like.

One can prove the following proposition

(28) For all real normed spaces X, Y holds $\langle$BoundedLinearOperators(X, Y), Zero_(BoundedLinearOperators(X, Y), RVectorSpaceOfLinearOperators $(X, Y))$, Add_(BoundedLinearOperators(X, Y), RVectorSpaceOfLinearOperators$(X, Y))$, Mult_(BoundedLinearOperators(X, Y), RVectorSpaceOfLinearOperators $(X, Y))\rangle$ is a real linear space.

Let X, Y be real normed spaces.

The functor RVectorSpaceOfBoundedLinearOperators(X, Y) yields a real linear space and is defined by:

(Def. 11) RVectorSpaceOfBoundedLinearOperators$(X, Y) =$ $\langle$BoundedLinearOperators(X, Y), Zero_(BoundedLinearOperators(X, Y), RVectorSpaceOfLinearOperators$(X, Y))$, Add_(BoundedLinearOperators (X, Y), RVectorSpaceOfLinearOperators$(X, Y))$, Mult_(BoundedLinearOperators(X, Y), RVectorSpaceOfLinearOperators $(X, Y))\rangle$.

Let X, Y be real normed spaces.

Observe that RVectorSpaceOfBoundedLinearOperators(X, Y) is strict.

Let X, Y be real normed spaces. Note that every element of RVectorSpaceOfBoundedLinearOperators(X, Y) is function-like and relation-like.

Let X, Y be real normed spaces, let f be an element of RVectorSpaceOfBoundedLinearOperators(X, Y), and let v be a vector of X. Then $f(v)$ is a vector of Y.

One can prove the following propositions:

(29) Let X, Y be real normed spaces and f, g, h be vectors of RVectorSpaceOfBoundedLinearOperators(X, Y). Then $h = f + g$ if and only if for every vector x of X holds $h(x) = f(x) + g(x)$.

(30) Let X, Y be real normed spaces, f, h be vectors of RVectorSpaceOfBoundedLinearOperators(X, Y), and a be a real number. Then $h = a \cdot f$ if and only if for every vector x of X holds $h(x) = a \cdot f(x)$.

(31) For all real normed spaces X, Y holds $0_{\mathrm{RVectorSpaceOfBoundedLinearOperators}(X,Y)} = (\text{the carrier of } X) \longmapsto 0_Y$.

Let X, Y be real normed spaces and let f be a set. Let us assume that $f \in$ BoundedLinearOperators(X, Y). The functor modetrans(f, X, Y) yields a bounded linear operator from X into Y and is defined by:

(Def. 12) modetrans$(f, X, Y) = f$.

Let X, Y be real normed spaces and let u be a linear operator from X into Y. The functor $\mathrm{PreNorms}(u)$ yielding a non empty subset of $\mathbb{R}$ is defined as follows:

(Def. 13) $\mathrm{PreNorms}(u) = \{\|u(t)\|; t$ ranges over vectors of X: $\|t\| \leqslant 1\}$.

We now state three propositions:

(32) Let X, Y be real normed spaces and g be a bounded linear operator from X into Y. Then $\mathrm{PreNorms}(g)$ is non empty and upper bounded.

(33) Let X, Y be real normed spaces and g be a linear operator from X into Y. Then g is bounded if and only if $\mathrm{PreNorms}(g)$ is upper bounded.

(34) Let X, Y be real normed spaces. Then there exists a function N_1 from $\mathrm{BoundedLinearOperators}(X,Y)$ into $\mathbb{R}$ such that for every set f if $f \in \mathrm{BoundedLinearOperators}(X,Y)$, then $N_1(f) = \sup \mathrm{PreNorms}(\mathrm{modetrans}(f,X,Y))$.

Let X, Y be real normed spaces. The functor BoundedLinearOperatorsNorm (X,Y) yielding a function from $\mathrm{BoundedLinearOperators}(X,Y)$ into $\mathbb{R}$ is defined as follows:

(Def. 14) For every set x such that $x \in \mathrm{BoundedLinearOperators}(X,Y)$ holds $(\mathrm{BoundedLinearOperatorsNorm}(X,Y))(x) = \sup \mathrm{PreNorms}(\mathrm{modetrans}(x, X,Y))$.

The following two propositions are true:

(35) For all real normed spaces X, Y and for every bounded linear operator f from X into Y holds $\mathrm{modetrans}(f,X,Y) = f$.

(36) For all real normed spaces X, Y and for every bounded linear operator f from X into Y holds $(\mathrm{BoundedLinearOperatorsNorm}(X,Y))(f) = \sup \mathrm{PreNorms}(f)$.

Let X, Y be real normed spaces.

The functor $\mathrm{RNormSpaceOfBoundedLinearOperators}(X,Y)$ yielding a non empty normed structure is defined as follows:

(Def. 15) $\mathrm{RNormSpaceOfBoundedLinearOperators}(X,Y) = \langle \mathrm{BoundedLinearOperators}(X,Y), \mathrm{Zero\_}(\mathrm{BoundedLinearOperators}(X,Y), \mathrm{RVectorSpaceOfLinearOperators}(X,Y)), \mathrm{Add\_}(\mathrm{BoundedLinearOperators}(X,Y), \mathrm{RVectorSpaceOfLinearOperators}(X,Y)), \mathrm{Mult\_}(\mathrm{BoundedLinearOperators}(X,Y), \mathrm{RVectorSpaceOfLinearOperators}(X,Y)), \mathrm{BoundedLinearOperatorsNorm}(X,Y)\rangle$.

The following propositions are true:

(37) For all real normed spaces X, Y holds (the carrier of X) $\longmapsto 0_Y = 0_{\mathrm{RNormSpaceOfBoundedLinearOperators}(X,Y)}$.

(38) Let X, Y be real normed spaces, f be a point

of RNormSpaceOfBoundedLinearOperators(X, Y), and g be a bounded linear operator from X into Y. If $g = f$, then for every vector t of X holds $\|g(t)\| \leqslant \|f\| \cdot \|t\|$.

(39) For all real normed spaces X, Y and for every point f of RNormSpaceOfBoundedLinearOperators(X, Y) holds $0 \leqslant \|f\|$.

(40) For all real normed spaces X, Y and for every point f of RNormSpaceOfBoundedLinearOperators(X, Y) such that $f = 0_{\mathrm{RNormSpaceOfBoundedLinearOperators}(X,Y)}$ holds $0 = \|f\|$.

Let X, Y be real normed spaces. Observe that every element of RNormSpaceOfBoundedLinearOperators(X, Y) is function-like and relation-like.

Let X, Y be real normed spaces, let f be an element of RNormSpaceOfBoundedLinearOperators(X, Y), and let v be a vector of X. Then $f(v)$ is a vector of Y.

The following propositions are true:

(41) Let X, Y be real normed spaces and f, g, h be points of RNormSpaceOfBoundedLinearOperators(X, Y). Then $h = f + g$ if and only if for every vector x of X holds $h(x) = f(x) + g(x)$.

(42) Let X, Y be real normed spaces, f, h be points of RNormSpaceOfBoundedLinearOperators(X, Y), and a be a real number. Then $h = a \cdot f$ if and only if for every vector x of X holds $h(x) = a \cdot f(x)$.

(43) Let X be a real normed space, Y be a real normed space, f, g be points of RNormSpaceOfBoundedLinearOperators(X, Y), and a be a real number. Then $\|f\| = 0$ iff $f = 0_{\mathrm{RNormSpaceOfBoundedLinearOperators}(X,Y)}$ and $\|a \cdot f\| = |a| \cdot \|f\|$ and $\|f + g\| \leqslant \|f\| + \|g\|$.

(44) For all real normed spaces X, Y holds RNormSpaceOfBoundedLinearOperators(X, Y) is real normed space-like.

(45) For all real normed spaces X, Y holds RNormSpaceOfBoundedLinearOperators(X, Y) is a real normed space.

Let X, Y be real normed spaces.

Note that RNormSpaceOfBoundedLinearOperators(X, Y) is real normed space-like, real linear space-like, Abelian, add-associative, right zeroed, and right complementable.

One can prove the following proposition

(46) Let X, Y be real normed spaces and f, g, h be points of RNormSpaceOfBoundedLinearOperators(X, Y). Then $h = f - g$ if and only if for every vector x of X holds $h(x) = f(x) - g(x)$.

4. Real Banach Space of Bounded Linear Operators

Let X be a real normed space. We say that X is complete if and only if:

(Def. 16) For every sequence s_1 of X such that s_1 is Cauchy sequence by norm holds s_1 is convergent.

Let us note that there exists a real normed space which is complete.

A real Banach space is a complete real normed space.

We now state three propositions:

(47) Let X be a real normed space and s_1 be a sequence of X. If s_1 is convergent, then $\|s_1\|$ is convergent and $\lim\|s_1\| = \|\lim s_1\|$.

(48) Let X, Y be real normed spaces. Suppose Y is complete. Let s_1 be a sequence of RNormSpaceOfBoundedLinearOperators(X, Y). If s_1 is Cauchy sequence by norm, then s_1 is convergent.

(49) For every real normed space X and for every real Banach space Y holds RNormSpaceOfBoundedLinearOperators(X, Y) is a real Banach space.

Let X be a real normed space and let Y be a real Banach space. Observe that RNormSpaceOfBoundedLinearOperators(X, Y) is complete.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[2] Grzegorz Bancerek. Sequences of ordinal numbers. *Formalized Mathematics*, 1(**2**):281–290, 1990.
[3] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[7] Czesław Byliński and Piotr Rudnicki. Bounding boxes for compact sets in $\mathcal{E}^2$. *Formalized Mathematics*, 6(**3**):427–440, 1997.
[8] Noboru Endou, Yasumasa Suzuki, and Yasunari Shidama. Real linear space of real sequences. *Formalized Mathematics*, 11(**3**):249–253, 2003.
[9] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[10] Jarosław Kotowicz. Convergent real sequences. Upper and lower bound of sets of real numbers. *Formalized Mathematics*, 1(**3**):477–481, 1990.
[11] Jarosław Kotowicz. Convergent sequences and the limit of sequences. *Formalized Mathematics*, 1(**2**):273–275, 1990.
[12] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.
[13] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[14] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[15] Henryk Oryszczyszyn and Krzysztof Prażmowski. Real functions spaces. *Formalized Mathematics*, 1(**3**):555–561, 1990.
[16] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.

[17] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.
[18] Jan Popiołek. Introduction to Banach and Hilbert spaces - part I. *Formalized Mathematics*, 2(**4**):511–516, 1991.
[19] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[20] Yasumasa Suzuki, Noboru Endou, and Yasunari Shidama. Banach space of absolute summable real sequences. *Formalized Mathematics*, 11(**4**):377–380, 2003.
[21] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*
[22] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[23] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[24] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[25] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.
[26] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[27] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[28] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[29] Wojciech A. Trybulec. Subspaces and cosets of subspaces in real linear space. *Formalized Mathematics*, 1(**2**):297–301, 1990.
[30] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[33] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received December 22, 2003

FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

Little Bezout Theorem (Factor Theorem)[1]

Piotr Rudnicki
University of Alberta
Edmonton

Summary. We present a formalization of the factor theorem for univariate polynomials, also called the (little) Bezout theorem: Let r belong to a commutative ring L and $p(x)$ be a polynomial over L. Then $x-r$ divides $p(x)$ iff $p(r)=0$. We also prove some consequences of this theorem like that any non zero polynomial of degree n over an algebraically closed integral domain has n (non necessarily distinct) roots.

MML Identifier: UPROOTS.

The articles [28], [37], [26], [10], [2], [27], [36], [15], [20], [38], [7], [8], [3], [6], [35], [32], [24], [23], [11], [21], [16], [19], [17], [18], [1], [12], [33], [29], [22], [9], [34], [4], [25], [39], [13], [30], [14], [31], and [5] provide the notation and terminology for this paper.

1. Preliminaries

One can prove the following propositions:

(1) For every natural number n holds n is non empty iff $n=1$ or $n>1$.

(2) Let f be a finite sequence of elements of $\mathbb{N}$. Suppose that for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i) \neq 0$. Then $\sum f = \operatorname{len} f$ if and only if $f = \operatorname{len} f \mapsto 1$.

The scheme *IndFinSeq0* deals with a finite sequence $\mathcal{A}$ and a binary predicate $\mathcal{P}$, and states that:

For every natural number i such that $1 \leqslant i$ and $i \leqslant \operatorname{len} \mathcal{A}$ holds $\mathcal{P}[i, \mathcal{A}(i)]$

[1]This work has been supported by NSERC Grant OGP9207.

ISSN 1426–2630

provided the parameters meet the following requirements:

- $\mathcal{P}[1, \mathcal{A}(1)]$, and
- For every natural number i such that $1 \leqslant i$ and $i < \operatorname{len} \mathcal{A}$ holds if $\mathcal{P}[i, \mathcal{A}(i)]$, then $\mathcal{P}[i+1, \mathcal{A}(i+1)]$.

We now state the proposition

(3) Let L be an add-associative right zeroed right complementable non empty loop structure and r be a finite sequence of elements of L. Suppose $\operatorname{len} r \geqslant 2$ and for every natural number k such that $2 < k$ and $k \in \operatorname{dom} r$ holds $r(k) = 0_L$. Then $\sum r = r_1 + r_2$.

2. Canonical Ordering of a Finite Set

Let A be a finite set. The functor $\mathrm{CFS}(A)$ yielding a finite sequence of elements of A is defined by the conditions (Def. 1).

(Def. 1)(i) $\operatorname{len} \mathrm{CFS}(A) = \operatorname{card} A$, and

(ii) there exists a finite sequence f such that $\operatorname{len} f = \operatorname{card} A$ and $f(1) = \langle\!\langle \mathrm{choose}(A), A \setminus \{\mathrm{choose}(A)\} \rangle\!\rangle$ or $\operatorname{card} A = 0$ and for every natural number i such that $1 \leqslant i$ and $i < \operatorname{card} A$ and for every set x such that $f(i) = x$ holds $f(i+1) = \langle\!\langle \mathrm{choose}(x_{\mathbf{2}}), x_{\mathbf{2}} \setminus \{\mathrm{choose}(x_{\mathbf{2}})\} \rangle\!\rangle$ and for every natural number i such that $i \in \operatorname{dom} \mathrm{CFS}(A)$ holds $(\mathrm{CFS}(A))(i) = f(i)_{\mathbf{1}}$.

The following four propositions are true:

(4) For every finite set A holds $\mathrm{CFS}(A)$ is one-to-one.

(5) For every finite set A holds $\operatorname{rng} \mathrm{CFS}(A) = A$.

(6) For every set a holds $\mathrm{CFS}(\{a\}) = \langle a \rangle$.

(7) For every finite set A holds $(\mathrm{CFS}(A))^{-1}$ is a function from A into $\operatorname{Seg} \operatorname{card} A$.

3. More about Bags

Let X be a set, let S be a finite subset of X, and let n be a natural number. The functor (S, n)-bag yields an element of $\operatorname{Bags} X$ and is defined by:

(Def. 2) $(S, n)\text{-bag} = \operatorname{EmptyBag} X {+\cdot} (S \longmapsto n)$.

We now state several propositions:

(8) Let X be a set, S be a finite subset of X, n be a natural number, and i be a set. If $i \notin S$, then $((S, n)\text{-bag})(i) = 0$.

(9) Let X be a set, S be a finite subset of X, n be a natural number, and i be a set. If $i \in S$, then $((S, n)\text{-bag})(i) = n$.

(10) For every set X and for every finite subset S of X and for every natural number n such that $n \neq 0$ holds $\operatorname{support}(S, n)\text{-bag} = S$.

(11) Let X be a set, S be a finite subset of X, and n be a natural number. If S is empty or $n = 0$, then (S, n)-bag $=$ EmptyBag X.

(12) Let X be a set, S, T be finite subsets of X, and n be a natural number. If S misses T, then $(S \cup T, n)$-bag $= (S, n)$-bag $+ (T, n)$-bag.

Let A be a set and let b be a bag of A. The functor degree(b) yielding a natural number is defined as follows:

(Def. 3) There exists a finite sequence f of elements of $\mathbb{N}$ such that degree$(b) = \sum f$ and $f = b \cdot \mathrm{CFS}(\mathrm{support}\, b)$.

We now state several propositions:

(13) For every set A and for every bag b of A holds $b =$ EmptyBag A iff degree$(b) = 0$.

(14) Let A be a set, S be a finite subset of A, and b be a bag of A. Then $S = \mathrm{support}\, b$ and degree$(b) = \mathrm{card}\, S$ if and only if $b = (S, 1)$-bag.

(15) Let A be a set, S be a finite subset of A, and b be a bag of A. Suppose $\mathrm{support}\, b \subseteq S$. Then there exists a finite sequence f of elements of $\mathbb{N}$ such that $f = b \cdot \mathrm{CFS}(S)$ and degree$(b) = \sum f$.

(16) For every set A and for all bags b, b_1, b_2 of A such that $b = b_1 + b_2$ holds degree$(b) =$ degree$(b_1) +$ degree(b_2).

(17) Let L be an associative commutative unital non empty groupoid, f, g be finite sequences of elements of L, and p be a permutation of dom f. If $g = f \cdot p$, then $\prod g = \prod f$.

4. More on Polynomials

Let L be a non empty zero structure and let p be a polynomial of L. We say that p is non-zero if and only if:

(Def. 4) $p \neq \mathbf{0}.\, L$.

One can prove the following proposition

(18) For every non empty zero structure L and for every polynomial p of L holds p is non-zero iff $\mathrm{len}\, p > 0$.

Let L be a non trivial non empty zero structure. Note that there exists a polynomial of L which is non-zero.

Let L be a non degenerated non empty multiplicative loop with zero structure and let x be an element of L. Note that $\langle x, \mathbf{1}_L \rangle$ is non-zero.

Next we state three propositions:

(19) For every non empty zero structure L and for every polynomial p of L such that $\mathrm{len}\, p > 0$ holds $p(\mathrm{len}\, p -' 1) \neq 0_L$.

(20) Let L be a non empty zero structure and p be an algebraic sequence of L. If $\mathrm{len}\, p = 1$, then $p = \langle p(0) \rangle$ and $p(0) \neq 0_L$.

(21) Let L be an add-associative right zeroed right complementable right distributive non empty double loop structure and p be a polynomial of L. Then $p * \mathbf{0}. L = \mathbf{0}. L$.

Let us mention that there exists a well unital non empty double loop structure which is algebraic-closed, add-associative, right zeroed, right complementable, Abelian, commutative, associative, distributive, integral domain-like, and non degenerated.

We now state the proposition

(22) Let L be an add-associative right zeroed right complementable distributive integral domain-like non empty double loop structure and p, q be polynomials of L. If $p * q = \mathbf{0}. L$, then $p = \mathbf{0}. L$ or $q = \mathbf{0}. L$.

Let L be an add-associative right zeroed right complementable distributive integral domain-like non empty double loop structure. Observe that Polynom-Ring L is integral domain-like.

Let L be an integral domain and let p, q be non-zero polynomials of L. One can check that $p * q$ is non-zero.

We now state a number of propositions:

(23) For every non degenerated commutative ring L and for all polynomials p, q of L holds $\mathrm{Roots}\, p \cup \mathrm{Roots}\, q \subseteq \mathrm{Roots}(p * q)$.

(24) For every integral domain L and for all polynomials p, q of L holds $\mathrm{Roots}(p * q) = \mathrm{Roots}\, p \cup \mathrm{Roots}\, q$.

(25) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure, p be a polynomial of L, and p_1 be an element of Polynom-Ring L. If $p = p_1$, then $-p = -p_1$.

(26) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure, p, q be polynomials of L, and p_1, q_1 be elements of Polynom-Ring L. If $p = p_1$ and $q = q_1$, then $p - q = p_1 - q_1$.

(27) Let L be an Abelian add-associative right zeroed right complementable distributive non empty double loop structure and p, q, r be polynomials of L. Then $p * q - p * r = p * (q - r)$.

(28) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure and p, q be polynomials of L. If $p - q = \mathbf{0}. L$, then $p = q$.

(29) Let L be an Abelian add-associative right zeroed right complementable distributive integral domain-like non empty double loop structure and p, q, r be polynomials of L. If $p \neq \mathbf{0}. L$ and $p * q = p * r$, then $q = r$.

(30) Let L be an integral domain, n be a natural number, and p be a polynomial of L. If $p \neq \mathbf{0}. L$, then $p^n \neq \mathbf{0}. L$.

(31) For every commutative ring L and for all natural numbers i, j and for every polynomial p of L holds $p^i * p^j = p^{i+j}$.

(32) For every non empty multiplicative loop with zero structure L holds $\mathbf{1}.\,L = \langle \mathbf{1}_L \rangle$.

(33) Let L be an add-associative right zeroed right complementable right unital right distributive non empty double loop structure and p be a polynomial of L. Then $p * \langle \mathbf{1}_L \rangle = p$.

(34) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure and p, q be polynomials of L. If $\operatorname{len} p = 0$ or $\operatorname{len} q = 0$, then $\operatorname{len}(p * q) = 0$.

(35) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure and p, q be polynomials of L. If $p * q$ is non-zero, then p is non-zero and q is non-zero.

(36) Let L be an add-associative right zeroed right complementable distributive commutative associative left unital non empty double loop structure and p, q be polynomials of L. If $p(\operatorname{len} p -' 1) \cdot q(\operatorname{len} q -' 1) \neq 0_L$, then $0 < \operatorname{len}(p * q)$.

(37) Let L be an add-associative right zeroed right complementable distributive commutative associative left unital integral domain-like non empty double loop structure and p, q be polynomials of L. If $1 < \operatorname{len} p$ and $1 < \operatorname{len} q$, then $\operatorname{len} p < \operatorname{len}(p * q)$.

(38) Let L be an add-associative right zeroed right complementable left distributive non empty double loop structure, a, b be elements of L, and p be a polynomial of L. Then $(\langle a, b \rangle * p)(0) = a \cdot p(0)$ and for every natural number i holds $(\langle a, b \rangle * p)(i + 1) = a \cdot p(i + 1) + b \cdot p(i)$.

(39) Let L be an add-associative right zeroed right complementable distributive well unital commutative associative non degenerated non empty double loop structure, r be an element of L, and q be a non-zero polynomial of L. Then $\operatorname{len}(\langle r, \mathbf{1}_L \rangle * q) = \operatorname{len} q + 1$.

(40) Let L be a non degenerated commutative ring, x be an element of L, and i be a natural number. Then $\operatorname{len}(\langle x, \mathbf{1}_L \rangle^i) = i + 1$.

Let L be a non degenerated commutative ring, let x be an element of L, and let n be a natural number. Note that $\langle x, \mathbf{1}_L \rangle^n$ is non-zero.

Next we state two propositions:

(41) Let L be a non degenerated commutative ring, x be an element of L, q be a non-zero polynomial of L, and i be a natural number. Then $\operatorname{len}(\langle x, \mathbf{1}_L \rangle^i * q) = i + \operatorname{len} q$.

(42) Let L be an add-associative right zeroed right complementable distributive well unital commutative associative non degenerated non empty double loop structure, r be an element of L, and p, q be polynomials of L. If $p = \langle r, \mathbf{1}_L \rangle * q$ and $p(\operatorname{len} p -' 1) = \mathbf{1}_L$, then $q(\operatorname{len} q -' 1) = \mathbf{1}_L$.

5. Little Bezout Theorem

Let L be a non empty zero structure, let p be a polynomial of L, and let n be a natural number. The functor $\mathrm{poly\_shift}(p, n)$ yields a polynomial of L and is defined by:

(Def. 5) For every natural number i holds $(\mathrm{poly\_shift}(p, n))(i) = p(n + i)$.

We now state several propositions:

(43) For every non empty zero structure L and for every polynomial p of L holds $\mathrm{poly\_shift}(p, 0) = p$.

(44) Let L be a non empty zero structure, n be a natural number, and p be a polynomial of L. If $n \geqslant \mathrm{len}\, p$, then $\mathrm{poly\_shift}(p, n) = \mathbf{0}.\, L$.

(45) Let L be a non degenerated non empty multiplicative loop with zero structure, n be a natural number, and p be a polynomial of L. If $n \leqslant \mathrm{len}\, p$, then $\mathrm{len}\,\mathrm{poly\_shift}(p, n) + n = \mathrm{len}\, p$.

(46) Let L be a non degenerated commutative ring, x be an element of L, n be a natural number, and p be a polynomial of L. If $n < \mathrm{len}\, p$, then $\mathrm{eval}(\mathrm{poly\_shift}(p, n), x) = x \cdot \mathrm{eval}(\mathrm{poly\_shift}(p, n + 1), x) + p(n)$.

(47) For every non degenerated commutative ring L and for every polynomial p of L such that $\mathrm{len}\, p = 1$ holds $\mathrm{Roots}\, p = \emptyset$.

Let L be a non degenerated commutative ring, let r be an element of L, and let p be a polynomial of L. Let us assume that r is a root of p. The functor $\mathrm{poly\_quotient}(p, r)$ yielding a polynomial of L is defined as follows:

(Def. 6)(i) $\mathrm{len}\,\mathrm{poly\_quotient}(p, r) + 1 = \mathrm{len}\, p$ and for every natural number i holds $(\mathrm{poly\_quotient}(p, r))(i) = \mathrm{eval}(\mathrm{poly\_shift}(p, i + 1), r)$ if $\mathrm{len}\, p > 0$,

(ii) $\mathrm{poly\_quotient}(p, r) = \mathbf{0}.\, L$, otherwise.

Next we state several propositions:

(48) Let L be a non degenerated commutative ring, r be an element of L, and p be a non-zero polynomial of L. If r is a root of p, then $\mathrm{len}\,\mathrm{poly\_quotient}(p, r) > 0$.

(49) Let L be an add-associative right zeroed right complementable left distributive well unital non empty double loop structure and x be an element of L. Then $\mathrm{Roots}\langle -x, \mathbf{1}_L \rangle = \{x\}$.

(50) Let L be a non trivial commutative ring, x be an element of L, and p, q be polynomials of L. If $p = \langle -x, \mathbf{1}_L \rangle * q$, then x is a root of p.

(51) Let L be a non degenerated commutative ring, r be an element of L, and p be a polynomial of L. If r is a root of p, then $p = \langle -r, \mathbf{1}_L \rangle * \mathrm{poly\_quotient}(p, r)$.

(52) Let L be a non degenerated commutative ring, r be an element of L, and p, q be polynomials of L. If $p = \langle -r, \mathbf{1}_L \rangle * q$, then r is a root of p.

6. Polynomials Defined by Roots

Let L be an integral domain and let p be a non-zero polynomial of L. One can verify that $\mathrm{Roots}\, p$ is finite.

Let L be a non degenerated commutative ring, let x be an element of L, and let p be a non-zero polynomial of L. The functor $\mathrm{multiplicity}(p, x)$ yields a natural number and is defined by the condition (Def. 7).

(Def. 7) There exists a finite non empty subset F of $\mathbb{N}$ such that $F = \{k; k$ ranges over natural numbers: $\bigvee_{q:\text{polynomial of } L}\ p = \langle -x, \mathbf{1}_L \rangle^k * q\}$ and $\mathrm{multiplicity}(p, x) = \max F$.

Next we state two propositions:

(53) Let L be a non degenerated commutative ring, p be a non-zero polynomial of L, and x be an element of L. Then x is a root of p if and only if $\mathrm{multiplicity}(p, x) \geqslant 1$.

(54) For every non degenerated commutative ring L and for every element x of L holds $\mathrm{multiplicity}(\langle -x, \mathbf{1}_L \rangle, x) = 1$.

Let L be an integral domain and let p be a non-zero polynomial of L. The functor $\mathrm{BRoots}(p)$ yields a bag of the carrier of L and is defined as follows:

(Def. 8) $\mathrm{support}\, \mathrm{BRoots}(p) = \mathrm{Roots}\, p$ and for every element x of L holds $(\mathrm{BRoots}(p))(x) = \mathrm{multiplicity}(p, x)$.

Next we state several propositions:

(55) For every integral domain L and for every element x of L holds $\mathrm{BRoots}(\langle -x, \mathbf{1}_L \rangle) = (\{x\}, 1)\text{-bag}$.

(56) Let L be an integral domain, x be an element of L, and p, q be non-zero polynomials of L. Then $\mathrm{multiplicity}(p * q, x) = \mathrm{multiplicity}(p, x) + \mathrm{multiplicity}(q, x)$.

(57) For every integral domain L and for all non-zero polynomials p, q of L holds $\mathrm{BRoots}(p * q) = \mathrm{BRoots}(p) + \mathrm{BRoots}(q)$.

(58) For every integral domain L and for every non-zero polynomial p of L such that $\mathrm{len}\, p = 1$ holds $\mathrm{degree}(\mathrm{BRoots}(p)) = 0$.

(59) For every integral domain L and for every element x of L and for every natural number n holds $\mathrm{degree}(\mathrm{BRoots}(\langle -x, \mathbf{1}_L \rangle^n)) = n$.

(60) For every algebraic-closed integral domain L and for every non-zero polynomial p of L holds $\mathrm{degree}(\mathrm{BRoots}(p)) = \mathrm{len}\, p -' 1$.

Let L be an add-associative right zeroed right complementable distributive non empty double loop structure, let c be an element of L, and let n be a natural number. The functor $\mathrm{fpoly\_mult\_root}(c, n)$ yielding a finite sequence of elements of Polynom-Ring L is defined as follows:

(Def. 9) $\mathrm{len}\, \mathrm{fpoly\_mult\_root}(c, n) = n$ and for every natural number i such that $i \in \mathrm{dom}\, \mathrm{fpoly\_mult\_root}(c, n)$ holds $(\mathrm{fpoly\_mult\_root}(c, n))(i) = \langle -c, \mathbf{1}_L \rangle$.

Let L be an add-associative right zeroed right complementable distributive non empty double loop structure and let b be a bag of the carrier of L. The functor poly_with_roots(b) yields a polynomial of L and is defined by the condition (Def. 10).

(Def. 10) There exists a finite sequence f of elements of (the carrier of Polynom-Ring $L)^*$ and there exists a finite sequence s of elements of L such that $\operatorname{len} f = \operatorname{card} \operatorname{support} b$ and $s = \mathrm{CFS}(\operatorname{support} b)$ and for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i) =$ fpoly_mult_root$(s_i, b(s_i))$ and poly_with_roots$(b) = \prod \mathrm{Flat}(f)$.

The following propositions are true:

(61) Let L be an Abelian add-associative right zeroed right complementable commutative distributive right unital non empty double loop structure. Then poly_with_roots(EmptyBag (the carrier of L)) $= \langle \mathbf{1}_L \rangle$.

(62) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure and c be an element of L. Then poly_with_roots$((\{c\}, 1)$-bag$) = \langle -c, \mathbf{1}_L \rangle$.

(63) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure, b be a bag of the carrier of L, f be a finite sequence of elements of (the carrier of Polynom-Ring $L)^*$, and s be a finite sequence of elements of L. Suppose $\operatorname{len} f = \operatorname{card} \operatorname{support} b$ and $s = \mathrm{CFS}(\operatorname{support} b)$ and for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i) =$ fpoly_mult_root$(s_i, b(s_i))$. Then $\operatorname{len} \mathrm{Flat}(f) = \operatorname{degree}(b)$.

(64) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure, b be a bag of the carrier of L, f be a finite sequence of elements of (the carrier of Polynom-Ring $L)^*$, s be a finite sequence of elements of L, and c be an element of L such that $\operatorname{len} f = \operatorname{card} \operatorname{support} b$ and $s = \mathrm{CFS}(\operatorname{support} b)$ and for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i) =$ fpoly_mult_root$(s_i, b(s_i))$. Then

(i) if $c \in \operatorname{support} b$, then $\operatorname{card}(\mathrm{Flat}(f)^{-1}(\{\langle -c, \mathbf{1}_L \rangle\})) = b(c)$, and

(ii) if $c \notin \operatorname{support} b$, then $\operatorname{card}(\mathrm{Flat}(f)^{-1}(\{\langle -c, \mathbf{1}_L \rangle\})) = 0$.

(65) For every commutative ring L and for all bags b_1, b_2 of the carrier of L holds poly_with_roots$(b_1 + b_2) =$ poly_with_roots$(b_1) *$ poly_with_roots(b_2).

(66) Let L be an algebraic-closed integral domain and p be a non-zero polynomial of L. If $p(\operatorname{len} p -' 1) = \mathbf{1}_L$, then $p =$ poly_with_roots(BRoots(p)).

(67) Let L be a commutative ring, s be a non empty finite subset of L, and f be a finite sequence of elements of Polynom-Ring L. Suppose $\operatorname{len} f = \operatorname{card} s$ and for every natural number i and for every element c of L such that $i \in \operatorname{dom} f$ and $c = (\mathrm{CFS}(s))(i)$ holds $f(i) = \langle -c, \mathbf{1}_L \rangle$. Then poly_with_roots$((s, 1)$-bag$) = \prod f$.

(68) Let L be a non trivial commutative ring, s be a non empty finite subset

of L, x be an element of L, and f be a finite sequence of elements of L. Suppose $\operatorname{len} f = \operatorname{card} s$ and for every natural number i and for every element c of L such that $i \in \operatorname{dom} f$ and $c = (\mathrm{CFS}(s))(i)$ holds $f(i) = \mathrm{eval}(\langle -c, \mathbf{1}_L \rangle, x)$. Then $\mathrm{eval}(\mathrm{poly\_with\_roots}((s,1)\text{-bag}), x) = \prod f$.

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 and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Grzegorz Bancerek and Piotr Rudnicki. On defining functions on trees. *Formalized Mathematics*, 4(**1**):91–101, 1993.
[5] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 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. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 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. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[13] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.
[14] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.
[15] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[16] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(**2**):265–269, 2001.
[17] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.
[18] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.
[19] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.
[20] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[21] 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.
[22] Yatsuka Nakamura, Piotr Rudnicki, Andrzej Trybulec, and Pauline N. Kawamoto. Preliminaries to circuits, I. *Formalized Mathematics*, 5(**2**):167–172, 1996.
[23] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[24] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[25] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[26] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*
[27] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.
[28] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[29] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[30] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[31] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[32] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.
[33] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[34] Wojciech A. Trybulec. Linear combinations in real linear space. *Formalized Mathematics*, 1(**3**):581–588, 1990.
[35] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[36] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[37] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[38] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[39] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.

Received December 30, 2003

FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

Primitive Roots of Unity and Cyclotomic Polynomials[1]

Broderick Arneson
University of Alberta
Edmonton

Piotr Rudnicki
University of Alberta
Edmonton

Summary. We present a formalization of roots of unity, define cyclotomic polynomials and demonstrate the relationship between cyclotomic polynomials and unital polynomials.

MML Identifier: `UNIROOTS`.

The papers [34], [42], [32], [31], [11], [14], [35], [17], [2], [26], [41], [16], [24], [5], [43], [8], [9], [4], [15], [7], [39], [36], [10], [6], [27], [12], [25], [18], [19], [22], [20], [21], [23], [1], [40], [44], [28], [13], [37], [33], [3], [38], [30], [45], and [29] provide the notation and terminology for this paper.

1. Preliminaries

One can prove the following proposition

(1) For every natural number n holds $n = 0$ or $n = 1$ or $n \geqslant 2$.

The scheme *Comp Ind NE* concerns a unary predicate $\mathcal{P}$, and states that:

For every non empty natural number k holds $\mathcal{P}[k]$

provided the parameters satisfy the following condition:

- For every non empty natural number k such that for every non empty natural number n such that $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$.

Next we state the proposition

(2) For every finite sequence f such that $1 \leqslant \operatorname{len} f$ holds $f \restriction \operatorname{Seg} 1 = \langle f(1) \rangle$.

The following propositions are true:

[1]This work has been supported by NSERC Grant OGP9207.

ISSN 1426–2630

(3) Let f be a finite sequence of elements of $\mathbb{C}_{\mathrm{F}}$ and g be a finite sequence of elements of $\mathbb{R}$. Suppose $\operatorname{len} f = \operatorname{len} g$ and for every natural number i such that $i \in \operatorname{dom} f$ holds $|f_i| = g(i)$. Then $|\prod f| = \prod g$.

(4) Let s be a non empty finite subset of $\mathbb{C}_{\mathrm{F}}$, x be an element of $\mathbb{C}_{\mathrm{F}}$, and r be a finite sequence of elements of $\mathbb{R}$. Suppose $\operatorname{len} r = \operatorname{card} s$ and for every natural number i and for every element c of $\mathbb{C}_{\mathrm{F}}$ such that $i \in \operatorname{dom} r$ and $c = (\mathrm{CFS}(s))(i)$ holds $r(i) = |x - c|$. Then $|\mathrm{eval}(\mathrm{poly\_with\_roots}((s, 1)\text{-bag}), x)| = \prod r$.

(5) Let f be a finite sequence of elements of $\mathbb{C}_{\mathrm{F}}$. Suppose that for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i)$ is integer. Then $\sum f$ is integer.

(6) For every real number r there exists an element z of $\mathbb{C}$ such that $z = r$ and $z = r + 0i$.

(7) For all elements x, y of $\mathbb{C}_{\mathrm{F}}$ and for all real numbers r_1, r_2 such that $r_1 = x$ and $r_2 = y$ holds $r_1 \cdot r_2 = x \cdot y$ and $r_1 + r_2 = x + y$.

(8) Let q be a real number. Suppose q is an integer and $q > 0$. Let r be an element of $\mathbb{C}_{\mathrm{F}}$. If $|r| = 1$ and $r \neq 1 + 0i_{\mathbb{C}_{\mathrm{F}}}$, then $|(q + 0i_{\mathbb{C}_{\mathrm{F}}}) - r| > q - 1$.

(9) Let p_1 be a non empty finite sequence of elements of $\mathbb{R}$ and x be a real number. Suppose $x \geqslant 1$ and for every natural number i such that $i \in \operatorname{dom} p_1$ holds $p_1(i) > x$. Then $\prod p_1 > x$.

(10) For every natural number n holds $\mathbf{1}_{\mathbb{C}_{\mathrm{F}}} = \mathrm{power}_{\mathbb{C}_{\mathrm{F}}}(\mathbf{1}_{\mathbb{C}_{\mathrm{F}}}, n)$.

(11) Let n be a non empty natural number and i be a natural number. Then $\cos(\frac{2 \cdot \pi \cdot i}{n}) = \cos(\frac{2 \cdot \pi \cdot (i \bmod n)}{n})$ and $\sin(\frac{2 \cdot \pi \cdot i}{n}) = \sin(\frac{2 \cdot \pi \cdot (i \bmod n)}{n})$.

(12) For every non empty natural number n and for every natural number i holds $\cos(\frac{2 \cdot \pi \cdot i}{n}) + \sin(\frac{2 \cdot \pi \cdot i}{n}) i_{\mathbb{C}_{\mathrm{F}}} = \cos(\frac{2 \cdot \pi \cdot (i \bmod n)}{n}) + \sin(\frac{2 \cdot \pi \cdot (i \bmod n)}{n}) i_{\mathbb{C}_{\mathrm{F}}}$.

(13) Let n be a non empty natural number and i, j be natural numbers. Then $(\cos(\frac{2 \cdot \pi \cdot i}{n}) + \sin(\frac{2 \cdot \pi \cdot i}{n}) i_{\mathbb{C}_{\mathrm{F}}}) \cdot (\cos(\frac{2 \cdot \pi \cdot j}{n}) + \sin(\frac{2 \cdot \pi \cdot j}{n}) i_{\mathbb{C}_{\mathrm{F}}}) = \cos(\frac{2 \cdot \pi \cdot ((i+j) \bmod n)}{n}) + \sin(\frac{2 \cdot \pi \cdot ((i+j) \bmod n)}{n}) i_{\mathbb{C}_{\mathrm{F}}}$.

(14) Let L be a unital associative non empty groupoid, x be an element of L, and n, m be natural numbers. Then $\mathrm{power}_L(x, n \cdot m) = \mathrm{power}_L(\mathrm{power}_L(x, n), m)$.

(15) For every natural number n and for every element x of $\mathbb{C}_{\mathrm{F}}$ such that x is an integer holds $\mathrm{power}_{\mathbb{C}_{\mathrm{F}}}(x, n)$ is an integer.

(16) Let F be a finite sequence of elements of $\mathbb{C}_{\mathrm{F}}$. Suppose that for every natural number i such that $i \in \operatorname{dom} F$ holds $F(i)$ is an integer. Then $\sum F$ is an integer.

(17) For every real number a such that $0 \leqslant a$ and $a < 2 \cdot \pi$ and $\cos a = 1$ holds $a = 0$.

Let us note that there exists a field which is finite and there exists a skew field which is finite.

2. Multiplicative Group of a Skew Field

Let R be a skew field. The functor MultGroup(R) yields a strict group and is defined by the conditions (Def. 1).

(Def. 1)(i) The carrier of MultGroup(R) = (the carrier of R) $\setminus \{0_R\}$, and

(ii) the multiplication of MultGroup(R) = (the multiplication of R)$\restriction$[: the carrier of MultGroup(R), the carrier of MultGroup(R) :].

Next we state three propositions:

(18) For every skew field R holds the carrier of R = (the carrier of MultGroup(R)) $\cup \{0_R\}$.

(19) Let R be a skew field, a, b be elements of R, and c, d be elements of MultGroup(R). If $a = c$ and $b = d$, then $c \cdot d = a \cdot b$.

(20) For every skew field R holds $\mathbf{1}_R = 1_{\mathrm{MultGroup}(R)}$.

Let R be a finite skew field. Observe that MultGroup(R) is finite.

We now state three propositions:

(21) For every finite skew field R holds ord(MultGroup(R)) = card (the carrier of R) $- 1$.

(22) For every skew field R and for every set s such that $s \in$ the carrier of MultGroup(R) holds $s \in$ the carrier of R.

(23) For every skew field R holds the carrier of MultGroup(R) $\subseteq$ the carrier of R.

3. Roots of Unity

Let n be a non empty natural number. The functor n-roots_of_1 yielding a subset of $\mathbb{C}_{\mathrm{F}}$ is defined by:

(Def. 2) n-roots_of_1 = $\{x; x$ ranges over elements of $\mathbb{C}_{\mathrm{F}}$: x is a complex root of n, $\mathbf{1}_{\mathbb{C}_{\mathrm{F}}}\}$.

We now state several propositions:

(24) Let n be a non empty natural number and x be an element of $\mathbb{C}_{\mathrm{F}}$. Then $x \in n$-roots_of_1 if and only if x is a complex root of n, $\mathbf{1}_{\mathbb{C}_{\mathrm{F}}}$.

(25) For every non empty natural number n holds $\mathbf{1}_{\mathbb{C}_{\mathrm{F}}} \in n$-roots_of_1 .

(26) For every non empty natural number n and for every element x of $\mathbb{C}_{\mathrm{F}}$ such that $x \in n$-roots_of_1 holds $|x| = 1$.

(27) Let n be a non empty natural number and x be an element of $\mathbb{C}_{\mathrm{F}}$. Then $x \in n$-roots_of_1 if and only if there exists a natural number k such that $x = \cos(\frac{2 \cdot \pi \cdot k}{n}) + \sin(\frac{2 \cdot \pi \cdot k}{n}) i_{\mathbb{C}_{\mathrm{F}}}$.

(28) For every non empty natural number n and for all elements x, y of $\mathbb{C}$ such that $x \in n$-roots_of_1 and $y \in n$-roots_of_1 holds $x \cdot y \in n$-roots_of_1.

(29) For every non empty natural number n holds n-roots_of_1 $=$ $\{\cos(\frac{2 \cdot \pi \cdot k}{n}) + \sin(\frac{2 \cdot \pi \cdot k}{n}) i_{\mathbb{C}_{\mathrm{F}}}; k$ ranges over natural numbers: $k < n\}$.

(30) For every non empty natural number n holds $\overline{\overline{n\text{-roots\_of\_1}}} = n$.

Let n be a non empty natural number. One can check that n-roots_of_1 is non empty and n-roots_of_1 is finite.

Next we state several propositions:

(31) For all non empty natural numbers n, n_1 such that $n_1 \mid n$ holds n_1-roots_of_1 $\subseteq$ n-roots_of_1.

(32) Let R be a skew field, x be an element of MultGroup(R), and y be an element of R. If $y = x$, then for every natural number k holds $\mathrm{power}_{\mathrm{MultGroup}(R)}(x, k) = \mathrm{power}_R(y, k)$.

(33) For every non empty natural number n and for every element x of MultGroup($\mathbb{C}_{\mathrm{F}}$) such that $x \in n$-roots_of_1 holds x is not of order 0.

(34) Let n be a non empty natural number, k be a natural number, and x be an element of MultGroup($\mathbb{C}_{\mathrm{F}}$). If $x = \cos(\frac{2 \cdot \pi \cdot k}{n}) + \sin(\frac{2 \cdot \pi \cdot k}{n}) i_{\mathbb{C}_{\mathrm{F}}}$, then $\mathrm{ord}(x) = n \div (k \gcd n)$.

(35) For every non empty natural number n holds n-roots_of_1 $\subseteq$ the carrier of MultGroup($\mathbb{C}_{\mathrm{F}}$).

(36) For every non empty natural number n there exists an element x of MultGroup($\mathbb{C}_{\mathrm{F}}$) such that $\mathrm{ord}(x) = n$.

(37) For every non empty natural number n and for every element x of MultGroup($\mathbb{C}_{\mathrm{F}}$) holds $\mathrm{ord}(x) \mid n$ iff $x \in n$-roots_of_1.

(38) For every non empty natural number n holds n-roots_of_1 $= \{x; x$ ranges over elements of MultGroup($\mathbb{C}_{\mathrm{F}}$): $\mathrm{ord}(x) \mid n\}$.

(39) Let n be a non empty natural number and x be a set. Then $x \in$ n-roots_of_1 if and only if there exists an element y of MultGroup($\mathbb{C}_{\mathrm{F}}$) such that $x = y$ and $\mathrm{ord}(y) \mid n$.

Let n be a non empty natural number. The functor n-th_roots_of_1 yielding a strict group is defined as follows:

(Def. 3) The carrier of n-th_roots_of_1 $=$ n-roots_of_1 and the multiplication of n-th_roots_of_1 $=$ (the multiplication of $\mathbb{C}_{\mathrm{F}}$)$\restriction [\![n$-roots_of_1, n-roots_of_1 $]\!]$.

One can prove the following proposition

(40) For every non empty natural number n holds n-th_roots_of_1 is a subgroup of MultGroup($\mathbb{C}_{\mathrm{F}}$).

4. The Unital Polynomial $x^n - 1$

Let n be a non empty natural number and let L be a left unital non empty double loop structure. The functor unital_poly(L, n) yields a polynomial of L and is defined as follows:

(Def. 4) unital_poly$(L, n) = \mathbf{0}.\, L +\cdot (0, -\mathbf{1}_L) +\cdot (n, \mathbf{1}_L)$.

Next we state four propositions:

(41) unital_poly$(\mathbb{C}_{\rm F}, 1) = \langle -\mathbf{1}_{\mathbb{C}_{\rm F}}, \mathbf{1}_{\mathbb{C}_{\rm F}} \rangle$.

(42) Let L be a left unital non empty double loop structure and n be a non empty natural number. Then (unital_poly$(L, n))(0) = -\mathbf{1}_L$ and (unital_poly$(L, n))(n) = \mathbf{1}_L$.

(43) Let L be a left unital non empty double loop structure, n be a non empty natural number, and i be a natural number. If $i \neq 0$ and $i \neq n$, then (unital_poly$(L, n))(i) = 0_L$.

(44) Let L be a non degenerated left unital non empty double loop structure and n be a non empty natural number. Then len unital_poly$(L, n) = n+1$.

Let L be a non degenerated left unital non empty double loop structure and let n be a non empty natural number. Observe that unital_poly(L, n) is non-zero.

The following propositions are true:

(45) For every non empty natural number n and for every element x of $\mathbb{C}_{\rm F}$ holds eval(unital_poly$(\mathbb{C}_{\rm F}, n), x) = \mathrm{power}_{\mathbb{C}_{\rm F}}(x, n) - 1$.

(46) For every non empty natural number n holds Roots unital_poly$(\mathbb{C}_{\rm F}, n) =$ n-roots_of_1 .

(47) Let n be a natural number and z be an element of $\mathbb{C}_{\rm F}$. Suppose z is a real number. Then there exists a real number x such that $x = z$ and $\mathrm{power}_{\mathbb{C}_{\rm F}}(z, n) = x^n$.

(48) Let n be a non empty natural number and x be a real number. Then there exists an element y of $\mathbb{C}_{\rm F}$ such that $y = x$ and eval(unital_poly$(\mathbb{C}_{\rm F}, n), y) =$ $x^n - 1$.

(49) For every non empty natural number n holds BRoots(unital_poly$(\mathbb{C}_{\rm F}, n)) =$ (n-roots_of_1, 1) -bag .

(50) For every non empty natural number n holds unital_poly$(\mathbb{C}_{\rm F}, n) =$ poly_with_roots((n-roots_of_1, 1) -bag).

Let i be an integer and let n be a natural number. Then i^n is an integer.

The following proposition is true

(51) For every non empty natural number n and for every element i of $\mathbb{C}_{\rm F}$ such that i is an integer holds eval(unital_poly$(\mathbb{C}_{\rm F}, n), i)$ is an integer.

5. Cyclotomic Polynomials

Let d be a non empty natural number. The functor cyclotomic_poly(d) yields a polynomial of $\mathbb{C}_{\mathrm{F}}$ and is defined by:

(Def. 5) There exists a non empty finite subset s of $\mathbb{C}_{\mathrm{F}}$ such that $s = \{y; y$ ranges over elements of MultGroup($\mathbb{C}_{\mathrm{F}}$): $\mathrm{ord}(y) = d\}$ and cyclotomic_poly(d) = poly_with_roots((s, 1)-bag).

The following propositions are true:

(52) cyclotomic_poly(1) $= \langle -\mathbf{1}_{\mathbb{C}_{\mathrm{F}}}, \mathbf{1}_{\mathbb{C}_{\mathrm{F}}} \rangle$.

(53) Let n be a non empty natural number and f be a finite sequence of elements of the carrier of Polynom-Ring($\mathbb{C}_{\mathrm{F}}$). Suppose $\mathrm{len}\, f = n$ and for every non empty natural number i such that $i \in \mathrm{dom}\, f$ holds if $i \nmid n$, then $f(i) = \langle \mathbf{1}_{\mathbb{C}_{\mathrm{F}}} \rangle$ and if $i \mid n$, then $f(i) =$ cyclotomic_poly(i). Then unital_poly($\mathbb{C}_{\mathrm{F}}, n$) $= \prod f$.

(54) Let n be a non empty natural number. Then there exists a finite sequence f of elements of the carrier of Polynom-Ring($\mathbb{C}_{\mathrm{F}}$) and there exists a polynomial p of $\mathbb{C}_{\mathrm{F}}$ such that

(i) $p = \prod f$,

(ii) $\mathrm{dom}\, f = \mathrm{Seg}\, n$,

(iii) for every non empty natural number i such that $i \in \mathrm{Seg}\, n$ holds if $i \nmid n$ or $i = n$, then $f(i) = \langle \mathbf{1}_{\mathbb{C}_{\mathrm{F}}} \rangle$ and if $i \mid n$ and $i \neq n$, then $f(i) =$ cyclotomic_poly(i), and

(iv) unital_poly($\mathbb{C}_{\mathrm{F}}, n$) = cyclotomic_poly($n$) $* p$.

(55) For every non empty natural number d and for every natural number i holds (cyclotomic_poly(d))(0) $= 1$ or (cyclotomic_poly(d))(0) $= -1$ but (cyclotomic_poly(d))(i) is integer.

(56) For every non empty natural number d and for every element z of $\mathbb{C}_{\mathrm{F}}$ such that z is an integer holds eval(cyclotomic_poly(d), z) is an integer.

(57) Let n, n_1 be non empty natural numbers, f be a finite sequence of elements of the carrier of Polynom-Ring($\mathbb{C}_{\mathrm{F}}$), and s be a finite subset of $\mathbb{C}_{\mathrm{F}}$. Suppose that

(i) $s = \{y; y$ ranges over elements of MultGroup($\mathbb{C}_{\mathrm{F}}$): $\mathrm{ord}(y) \mid n \wedge \mathrm{ord}(y) \nmid n_1 \wedge \mathrm{ord}(y) \neq n\}$,

(ii) $\mathrm{dom}\, f = \mathrm{Seg}\, n$, and

(iii) for every non empty natural number i such that $i \in \mathrm{dom}\, f$ holds if $i \nmid n$ or $i \mid n_1$ or $i = n$, then $f(i) = \langle \mathbf{1}_{\mathbb{C}_{\mathrm{F}}} \rangle$ and if $i \mid n$ and $i \nmid n_1$ and $i \neq n$, then $f(i) =$ cyclotomic_poly(i).

Then $\prod f$ = poly_with_roots((s, 1)-bag).

(58) Let n, n_1 be non empty natural numbers. Suppose $n_1 < n$ and $n_1 \mid n$. Then there exists a finite sequence f of elements of the carrier of Polynom-Ring($\mathbb{C}_{\mathrm{F}}$) and there exists a polynomial p of $\mathbb{C}_{\mathrm{F}}$ such that

(i) $p = \prod f$,

(ii) $\operatorname{dom} f = \operatorname{Seg} n$,

(iii) for every non empty natural number i such that $i \in \operatorname{Seg} n$ holds if $i \nmid n$ or $i \mid n_1$ or $i = n$, then $f(i) = \langle \mathbf{1}_{\mathbb{C}_\mathrm{F}} \rangle$ and if $i \mid n$ and $i \nmid n_1$ and $i \neq n$, then $f(i) = \text{cyclotomic\_poly}(i)$, and

(iv) $\text{unital\_poly}(\mathbb{C}_\mathrm{F}, n) = \text{unital\_poly}(\mathbb{C}_\mathrm{F}, n_1) * \text{cyclotomic\_poly}(n) * p$.

(59) Let i be an integer, c be an element of $\mathbb{C}_\mathrm{F}$, f be a finite sequence of elements of the carrier of Polynom-Ring($\mathbb{C}_\mathrm{F}$), and p be a polynomial of $\mathbb{C}_\mathrm{F}$. Suppose $p = \prod f$ and $c = i$ and for every non empty natural number i such that $i \in \operatorname{dom} f$ holds $f(i) = \langle \mathbf{1}_{\mathbb{C}_\mathrm{F}} \rangle$ or $f(i) = \text{cyclotomic\_poly}(i)$. Then $\text{eval}(p, c)$ is integer.

(60) Let n be a non empty natural number, j, k, q be integers, and q_1 be an element of $\mathbb{C}_\mathrm{F}$. If $q_1 = q$ and $j = \text{eval}(\text{cyclotomic\_poly}(n), q_1)$ and $k = \text{eval}(\text{unital\_poly}(\mathbb{C}_\mathrm{F}, n), q_1)$, then $j \mid k$.

(61) Let n, n_1 be non empty natural numbers and q be an integer. Suppose $n_1 < n$ and $n_1 \mid n$. Let q_1 be an element of c_1. Suppose $q_1 = q$. Let j, k, l be integers. If $j = \text{eval}(\text{cyclotomic\_poly}(n), q_1)$ and $k = \text{eval}(\text{unital\_poly}(\mathbb{C}_\mathrm{F}, n), q_1)$ and $l = \text{eval}(\text{unital\_poly}(\mathbb{C}_\mathrm{F}, n_1), q_1)$, then $j \mid k \div l$, where $c_1 =$ the carrier of $\mathbb{C}_\mathrm{F}$.

(62) Let n, q be non empty natural numbers and q_1 be an element of $\mathbb{C}_\mathrm{F}$. If $q_1 = q$, then for every integer j such that $j = \text{eval}(\text{cyclotomic\_poly}(n), q_1)$ holds $j \mid q^n - 1$.

(63) Let n, n_1, q be non empty natural numbers. Suppose $n_1 < n$ and $n_1 \mid n$. Let q_1 be an element of $\mathbb{C}_\mathrm{F}$. If $q_1 = q$, then for every integer j such that $j = \text{eval}(\text{cyclotomic\_poly}(n), q_1)$ holds $j \mid (q^n - 1) \div (q^{n_1} - 1)$.

(64) Let n be a non empty natural number. Suppose $1 < n$. Let q be a natural number. Suppose $1 < q$. Let q_1 be an element of $\mathbb{C}_\mathrm{F}$. If $q_1 = q$, then for every integer i such that $i = \text{eval}(\text{cyclotomic\_poly}(n), q_1)$ holds $|i| > q - 1$.

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. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

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

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

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

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

[11] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[12] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[13] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[14] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[15] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**):841–845, 1990.
[16] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[17] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[18] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(**2**):265–269, 2001.
[19] Anna Justyna Milewska. The Hahn Banach theorem in the vector space over the field of complex numbers. *Formalized Mathematics*, 9(**2**):363–371, 2001.
[20] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.
[21] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.
[22] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.
[23] Robert Milewski. Trigonometric form of complex numbers. *Formalized Mathematics*, 9(**3**):455–460, 2001.
[24] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[25] 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.
[26] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.
[27] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[28] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.
[29] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**):49–58, 2004.
[30] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[31] Andrzej Trybulec. Introduction to arithmetics. *To appear in Formalized Mathematics.*
[32] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*
[33] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[34] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[35] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[36] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.
[37] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[38] Wojciech A. Trybulec. Linear combinations in real linear space. *Formalized Mathematics*, 1(**3**):581–588, 1990.
[39] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[40] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.
[41] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[42] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[43] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[44] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

[45] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.

Received December 30, 2003

FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

Witt's Proof of the Wedderburn Theorem[1]

Broderick Arneson
University of Alberta
Edmonton

Matthias Baaz
Technische Universität Wien

Piotr Rudnicki
University of Alberta
Edmonton

Summary. We present a formalization of Witt's proof of the Wedderburn theorem following Chapter 5 of *Proofs from THE BOOK* by Martin Aigner and Günter M. Ziegler, 2nd ed., Springer 1999.

MML Identifier: `WEDDWITT`.

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

1. Preliminaries

The following propositions are true:

(1) For every natural number a and for every real number q such that $1 < q$ and $q^a = 1$ holds $a = 0$.

(2) For all natural numbers a, k, r and for every real number x such that $1 < x$ and $0 < k$ holds $x^{a \cdot k + r} = x^a \cdot x^{a \cdot (k -' 1) + r}$.

(3) For all natural numbers q, a, b such that $0 < a$ and $1 < q$ and $q^a -' 1 \mid q^b -' 1$ holds $a \mid b$.

(4) For all natural numbers n, q such that $0 < q$ holds $\overline{\overline{q^n}} = q^n$.

[1]This work has been supported by NSERC Grant OGP9207.

ISSN 1426–2630

(5) Let f be a finite sequence of elements of $\mathbb{N}$ and i be a natural number. If for every natural number j such that $j \in \operatorname{dom} f$ holds $i \mid f_j$, then $i \mid \sum f$.

(6) Let X be a finite set, Y be a partition of X, and f be a finite sequence of elements of Y. Suppose f is one-to-one and $\operatorname{rng} f = Y$. Let c be a finite sequence of elements of $\mathbb{N}$. Suppose $\operatorname{len} c = \operatorname{len} f$ and for every natural number i such that $i \in \operatorname{dom} c$ holds $c(i) = \overline{\overline{f(i)}}$. Then $\operatorname{card} X = \sum c$.

2. Class Formula for Groups

Let us observe that there exists a group which is finite.

Let G be a finite group. Observe that $\mathrm{Z}(G)$ is finite.

Let G be a group and let a be an element of G. The functor Centralizer(a) yields a strict subgroup of G and is defined by:

(Def. 1) The carrier of Centralizer(a) $= \{b; b$ ranges over elements of G: $a \cdot b = b \cdot a\}$.

Let G be a finite group and let a be an element of G. Observe that Centralizer(a) is finite.

Next we state two propositions:

(7) For every group G and for every element a of G and for every set x such that $x \in$ Centralizer(a) holds $x \in G$.

(8) For every group G and for all elements a, x of G holds $a \cdot x = x \cdot a$ iff x is an element of Centralizer(a).

Let G be a group and let a be an element of G. One can verify that $a^\bullet$ is non empty.

Let G be a group and let a be an element of G. The functor a-con_map yields a function from the carrier of G into $a^\bullet$ and is defined by:

(Def. 2) For every element x of G holds $(a\text{-con\_map})(x) = a^x$.

One can prove the following propositions:

(9) For every finite group G and for every element a of G and for every element x of $a^\bullet$ holds $\operatorname{card}((a\text{-con\_map})^{-1}(\{x\})) = \operatorname{ord}(\text{Centralizer}(a))$.

(10) Let G be a group, a be an element of G, and x, y be elements of $a^\bullet$. If $x \neq y$, then $(a\text{-con\_map})^{-1}(\{x\})$ misses $(a\text{-con\_map})^{-1}(\{y\})$.

(11) Let G be a group and a be an element of G. Then $\{(a\text{-con\_map})^{-1}(\{x\}) :$ x ranges over elements of $a^\bullet\}$ is a partition of the carrier of G.

(12) For every finite group G and for every element a of G holds $\overline{\overline{\{(a\text{-con\_map})^{-1}(\{x\}) : x \text{ ranges over elements of } a^\bullet\}}} = \operatorname{card} a^\bullet$.

(13) For every finite group G and for every element a of G holds $\operatorname{ord}(G) = \operatorname{card} a^\bullet \cdot \operatorname{ord}(\text{Centralizer}(a))$.

Let G be a group. The functor conjugate_Classes(G) yielding a partition of the carrier of G is defined by:

(Def. 3) conjugate_Classes$(G) = \{S; S$ ranges over subsets of G: $\bigvee_{a\,:\,\mathrm{element\ of}\ G}\ S = a^{\bullet}\}$.

The following two propositions are true:

(14) For every group G and for every set x holds $x \in$ conjugate_Classes(G) iff there exists an element a of G such that $a^{\bullet} = x$.

(15) Let G be a finite group and f be a finite sequence of elements of conjugate_Classes(G). Suppose f is one-to-one and $\mathrm{rng}\, f =$ conjugate_Classes(G). Let c be a finite sequence of elements of $\mathbb{N}$. Suppose $\mathrm{len}\, c = \mathrm{len}\, f$ and for every natural number i such that $i \in \mathrm{dom}\, c$ holds $c(i) = \overline{\overline{f(i)}}$. Then $\mathrm{ord}(G) = \sum c$.

3. Centers and Centralizers of Skew Fields

We now state the proposition

(16) Let F be a finite field, V be a vector space over F, and n, q be natural numbers. Suppose V is finite dimensional and $n = \dim(V)$ and $q = \overline{\overline{\text{the carrier of } F}}$. Then $\overline{\overline{\text{the carrier of } V}} = q^n$.

Let R be a skew field. The functor $\mathrm{Z}(R)$ yielding a strict field is defined by the conditions (Def. 4).

(Def. 4)(i) The carrier of $\mathrm{Z}(R) = \{x; x$ ranges over elements of R: $\bigwedge_{s\,:\,\mathrm{element\ of}\ R}\ x \cdot s = s \cdot x\}$,

(ii) the addition of $\mathrm{Z}(R) =$ (the addition of R)$\restriction[\!:$ the carrier of $\mathrm{Z}(R)$, the carrier of $\mathrm{Z}(R)\,:\!]$,

(iii) the multiplication of $\mathrm{Z}(R) =$ (the multiplication of R)$\restriction[\!:$ the carrier of $\mathrm{Z}(R)$, the carrier of $\mathrm{Z}(R)\,:\!]$,

(iv) the zero of $\mathrm{Z}(R) =$ the zero of R, and

(v) the unity of $\mathrm{Z}(R) =$ the unity of R.

The following proposition is true

(17) For every skew field R holds the carrier of $\mathrm{Z}(R) \subseteq$ the carrier of R.

Let R be a finite skew field. Note that $\mathrm{Z}(R)$ is finite.

We now state several propositions:

(18) Let R be a skew field and y be an element of R. Then $y \in \mathrm{Z}(R)$ if and only if for every element s of R holds $y \cdot s = s \cdot y$.

(19) For every skew field R holds $0_R \in \mathrm{Z}(R)$.

(20) For every skew field R holds $\mathbf{1}_R \in \mathrm{Z}(R)$.

(21) For every finite skew field R holds $1 < \mathrm{card}$ (the carrier of $\mathrm{Z}(R)$).

(22) For every finite skew field R holds card (the carrier of $\mathrm{Z}(R)$) = card (the carrier of R) iff R is commutative.

(23) For every skew field R holds the carrier of $\mathrm{Z}(R)$ = (the carrier of $\mathrm{Z}(\mathrm{MultGroup}(R))) \cup \{0_R\}$.

Let R be a skew field and let s be an element of R. The functor centralizer(s) yields a strict skew field and is defined by the conditions (Def. 5).

(Def. 5)(i) The carrier of centralizer(s) = $\{x; x$ ranges over elements of R: $x \cdot s = s \cdot x\}$,

(ii) the addition of centralizer(s) = (the addition of R)$\restriction$[: the carrier of centralizer(s), the carrier of centralizer(s) :],

(iii) the multiplication of centralizer(s) = (the multiplication of R)$\restriction$[: the carrier of centralizer(s), the carrier of centralizer(s) :],

(iv) the zero of centralizer(s) = the zero of R, and

(v) the unity of centralizer(s) = the unity of R.

Next we state several propositions:

(24) For every skew field R and for every element s of R holds the carrier of centralizer(s) $\subseteq$ the carrier of R.

(25) For every skew field R and for all elements s, a of R holds $a \in$ the carrier of centralizer(s) iff $a \cdot s = s \cdot a$.

(26) For every skew field R and for every element s of R holds the carrier of $\mathrm{Z}(R) \subseteq$ the carrier of centralizer(s).

(27) Let R be a skew field and s, a, b be elements of R. Suppose $a \in$ the carrier of $\mathrm{Z}(R)$ and $b \in$ the carrier of centralizer(s). Then $a \cdot b \in$ the carrier of centralizer(s).

(28) For every skew field R and for every element s of R holds 0_R is an element of centralizer(s) and $\mathbf{1}_R$ is an element of centralizer(s).

Let R be a finite skew field and let s be an element of R. Observe that centralizer(s) is finite.

Next we state three propositions:

(29) For every finite skew field R and for every element s of R holds $1 <$ card (the carrier of centralizer(s)).

(30) Let R be a skew field, s be an element of R, and t be an element of MultGroup(R). If $t = s$, then the carrier of centralizer(s) = (the carrier of Centralizer(t)) $\cup \{0_R\}$.

(31) Let R be a finite skew field, s be an element of R, and t be an element of MultGroup(R). If $t = s$, then ord(Centralizer(t)) = card (the carrier of centralizer(s)) $- 1$.

4. Vector Spaces over Centers of Skew Fields

Let R be a skew field. The functor VectSp_over Z(R) yielding a strict vector space over Z(R) is defined by the conditions (Def. 6).

(Def. 6)(i) The loop structure of VectSp_over Z(R) = the loop structure of R, and

(ii) the left multiplication of VectSp_over Z(R) = (the multiplication of R)$\restriction$[: the carrier of Z(R), the carrier of R :].

We now state two propositions:

(32) For every finite skew field R holds card (the carrier of R) = (card (the carrier of Z(R)))$^{\dim(\mathrm{VectSp\_over}\ \mathrm{Z}(R))}$.

(33) For every finite skew field R holds $0 <$ dim(VectSp_over Z(R)).

Let R be a skew field and let s be an element of R. The functor VectSp_over Z(s) yields a strict vector space over Z(R) and is defined by the conditions (Def. 7).

(Def. 7)(i) The loop structure of VectSp_over Z(s) = the loop structure of centralizer(s), and

(ii) the left multiplication of VectSp_over Z(s) = (the multiplication of R)$\restriction$[: the carrier of Z(R), the carrier of centralizer(s) :].

The following propositions are true:

(34) For every finite skew field R and for every element s of R holds card (the carrier of centralizer(s)) = (card (the carrier of Z(R)))$^{\dim(\mathrm{VectSp\_over}\ \mathrm{Z}(s))}$.

(35) For every finite skew field R and for every element s of R holds $0 <$ dim(VectSp_over Z(s)).

(36) Let R be a finite skew field and r be an element of R. Suppose r is an element of MultGroup(R).
Then (card (the carrier of Z(R)))$^{\dim(\mathrm{VectSp\_over}\ \mathrm{Z}(r))} - 1 \mid$ (card (the carrier of Z(R)))$^{\dim(\mathrm{VectSp\_over}\ \mathrm{Z}(R))} - 1$.

(37) For every finite skew field R and for every element s of R such that s is an element of MultGroup(R) holds dim(VectSp_over Z(s)) $\mid$ dim(VectSp_over Z(R)).

(38) For every finite skew field R holds
card (the carrier of Z(MultGroup(R))) = card (the carrier of Z(R)) $- 1$.

5. Witt's Proof of Wedderburn's Theorem

One can prove the following proposition

(39) Every finite skew field is commutative.

References

[1] Broderick Arneson and Piotr Rudnicki. Primitive roots of unity and cyclotomic polynomials.*FormalizedMathematics*,12(**1**):59–67,2004.
[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[9] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[11] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Formalized Mathematics*, 7(**1**):123–126, 1998.
[12] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[13] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.
[14] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[15] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(**2**):265–269, 2001.
[16] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[17] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[18] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.
[19] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.
[20] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*
[21] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[22] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.
[23] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[24] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[25] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.
[26] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[27] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[28] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.
[29] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[30] Wojciech A. Trybulec. Commutator and center of a group. *Formalized Mathematics*, 2(**4**):461–466, 1991.
[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[33] Mariusz Żynel. The Steinitz theorem and the dimension of a vector space. *Formalized Mathematics*, 5(**3**):423–428, 1996.

Received December 30, 2003

Contents

Formaliz. Math. 12 (**1**)

Continued on inside back cover