FORMALIZED MATHEMATICS
Vol. 21, No. 3, Pages 163–170, 2013
DOI: 10.2478/forma-2013-0018

VERSITA
degruyter.com/view/j/forma

Double Sequences and Limits[1]

Noboru Endou
Gifu National College of Thechnology
Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. Double sequences are important extension of the ordinary notion of a sequence. In this article we formalized three types of limits of double sequences and the theory of these limits.

MSC: 54A20 03B35

Keywords: formalization of basic metric space; limits of double sequences

MML identifier: DBLSEQ_1, version: 8.1.02 5.19.1189

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

In this paper R, R_1, R_2 denote functions from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$, r_1, r_2 denote convergent sequences of real numbers, n, m, N, M denote natural numbers, and e, r denote real numbers.

Let us consider R. We say that R is p-convergent if and only if

(Def. 1) There exists a real number p such that for every real number e such that $0 < e$ there exists a natural number N such that for every natural numbers n, m such that $n \geqslant N$ and $m \geqslant N$ holds $|R(n, m) - p| < e$.

Assume R is p-convergent. The functor P-lim R yielding a real number is defined by

(Def. 2) Let us consider a real number e. Suppose $0 < e$. Then there exists a natural number N such that for every natural numbers n, m such that $n \geqslant N$ and $m \geqslant N$ holds $|R(n, m) - it| < e$.

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

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

We say that R is convergent in the first coordinate if and only if

(Def. 3) Let us consider an element m of $\mathbb{N}$. Then $\mathrm{curry}'(R, m)$ is convergent.

We say that R is convergent in the second coordinate if and only if

(Def. 4) Let us consider an element n of $\mathbb{N}$. Then $\mathrm{curry}(R, n)$ is convergent.

The lim in the first coordinate of R yielding a function from $\mathbb{N}$ into $\mathbb{R}$ is defined by

(Def. 5) Let us consider an element m of $\mathbb{N}$. Then $it(m) = \lim \mathrm{curry}'(R, m)$.

The lim in the second coordinate of R yielding a function from $\mathbb{N}$ into $\mathbb{R}$ is defined by

(Def. 6) Let us consider an element n of $\mathbb{N}$. Then $it(n) = \lim \mathrm{curry}(R, n)$.

Assume the lim in the first coordinate of R is convergent. The first coordinate major iterated lim of R yielding a real number is defined by

(Def. 7) Let us consider a real number e. Suppose $0 < e$. Then there exists a natural number M such that for every natural number m such that $m \geqslant M$ holds $|(\text{the lim in the first coordinate of } R)(m) - it| < e$.

Assume the lim in the second coordinate of R is convergent. The second coordinate major iterated lim of R yielding a real number is defined by

(Def. 8) Let us consider a real number e. Suppose $0 < e$. Then there exists a natural number N such that for every natural number n such that $n \geqslant N$ holds $|(\text{the lim in the second coordinate of } R)(n) - it| < e$.

Let R be a function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$. We say that R is uniformly convergent in the first coordinate if and only if

(Def. 9) (i) R is convergent in the first coordinate, and

(ii) for every real number e such that $e > 0$ there exists a natural number M such that for every natural number m such that $m \geqslant M$ for every natural number n, $|R(n, m) - (\text{the lim in the first coordinate of } R)(n)| < e$.

We say that R is uniformly convergent in the second coordinate if and only if

(Def. 10) (i) R is convergent in the second coordinate, and

(ii) for every real number e such that $e > 0$ there exists a natural number N such that for every natural number n such that $n \geqslant N$ for every natural number m, $|R(n, m) - (\text{the lim in the second coordinate of } R)(m)| < e$.

Let us consider R. We say that R is non-decreasing if and only if

(Def. 11) Let us consider natural numbers n_1, m_1, n_2, m_2. If $n_1 \geqslant n_2$ and $m_1 \geqslant m_2$, then $R(n_1, m_1) \geqslant R(n_2, m_2)$.

We say that R is non-increasing if and only if

(Def. 12) Let us consider natural numbers n_1, m_1, n_2, m_2. If $n_1 \geqslant n_2$ and $m_1 \geqslant m_2$, then $R(n_1, m_1) \leqslant R(n_2, m_2)$.

Now we state the proposition:

(1) Let us consider real numbers a, b, c. If $a \leqslant b \leqslant c$, then $|b| \leqslant |a|$ or $|b| \leqslant |c|$.

Note that every function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$ which is non-decreasing and p-convergent is also lower bounded and upper bounded and every function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$ which is non-increasing and p-convergent is also lower bounded and upper bounded.

Let r be an element of $\mathbb{R}$. Let us note that $\mathbb{N} \times \mathbb{N} \longmapsto r$ is p-convergent convergent in the first coordinate and convergent in the second coordinate as a function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$.

Now we state the proposition:

(2) Let us consider an element r of $\mathbb{R}$. Then P-lim$(\mathbb{N} \times \mathbb{N} \longmapsto r) = r$. Proof: Set $R = \mathbb{N} \times \mathbb{N} \longmapsto r$. For every natural numbers n, m, $R(n, m) = r$ by [15, (70)]. □

Note that there exists a function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$ which is p-convergent, convergent in the first coordinate, and convergent in the second coordinate.

In this paper P_1 denotes a p-convergent function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$.

Let P_4 be a p-convergent convergent in the second coordinate function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$. Note that the lim in the second coordinate of P_4 is convergent.

Now we state the proposition:

(3) Suppose R is p-convergent and convergent in the second coordinate. Then P-lim R = the second coordinate major iterated lim of R. Proof: Consider z being a real number such that for every e such that $0 < e$ there exists a natural number N_1 such that for every n and m such that $n \geqslant N_1$ and $m \geqslant N_1$ holds $|R(n, m) - z| < e$. For every e such that $0 < e$ there exists N such that for every n such that $n \geqslant N$ holds |(the lim in the second coordinate of $R)(n) - z| < e$ by [4, (63), (60)]. For every e such that $0 < e$ there exists N such that for every n such that $n \geqslant N$ holds |(the lim in the second coordinate of $R)(n) -$ P-lim $R| < e$ by [4, (60), (63)]. □

Let P_3 be a p-convergent convergent in the first coordinate function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$. Let us note that the lim in the first coordinate of P_3 is convergent.

Now we state the proposition:

(4) Suppose R is p-convergent and convergent in the first coordinate. Then P-lim R = the first coordinate major iterated lim of R. Proof: Consider z being a real number such that for every e such that $0 < e$ there exists a natural number N_1 such that for every n and m such that $n \geqslant N_1$ and $m \geqslant N_1$ holds $|R(n, m) - z| < e$. For every e such that $0 < e$ there exists N such that for every n such that $n \geqslant N$ holds |(the lim in the first coordinate of $R)(n) - z| < e$ by [4, (63), (60)]. For every e such that $0 < e$

there exists N such that for every n such that $n \geqslant N$ holds |(the lim in the first coordinate of $R)(n) - \text{P-lim}\, R| < e$ by [4, (60), (63)]. □

One can verify that every function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$ which is non-decreasing and upper bounded is also p-convergent convergent in the first coordinate and convergent in the second coordinate and every function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$ which is non-increasing and lower bounded is also p-convergent convergent in the first coordinate and convergent in the second coordinate.

Now we state the propositions:

(5) Suppose R is uniformly convergent in the first coordinate and the lim in the first coordinate of R is convergent. Then

(i) R is p-convergent, and

(ii) $\text{P-lim}\, R =$ the first coordinate major iterated lim of R.

(6) Suppose R is uniformly convergent in the second coordinate and the lim in the second coordinate of R is convergent. Then

(i) R is p-convergent, and

(ii) $\text{P-lim}\, R =$ the second coordinate major iterated lim of R.

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

(Def. 13) Let us consider a real number e. Suppose $e > 0$. Then there exists a natural number N such that for every natural numbers n_1, n_2, m_1, m_2 such that $N \leqslant n_1 \leqslant n_2$ and $N \leqslant m_1 \leqslant m_2$ holds $|R(n_2, m_2) - R(n_1, m_1)| < e$.

Now we state the propositions:

(7) R is p-convergent if and only if R is Cauchy. Proof: Define $\mathcal{R}$(element of $\mathbb{N}) = R(\$_1, \$_1)$. Consider s_1 being a function from $\mathbb{N}$ into $\mathbb{R}$ such that for every element n of $\mathbb{N}$, $s_1(n) = \mathcal{R}(n)$ from [7, Sch. 4]. Reconsider $z = \lim s_1$ as a complex number. For every e such that $0 < e$ there exists N such that for every n and m such that $n \geqslant N$ and $m \geqslant N$ holds $|R(n, m) - z| < e$ by [4, (63)]. □

(8) Let us consider a function R from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$. Suppose

(i) R is non-decreasing, or

(ii) R is non-increasing.

Then R is p-convergent if and only if R is lower bounded and upper bounded.

Let X, Y be non empty sets, H be a binary operation on Y, and f, g be functions from X into Y. Observe that the functor $H_{f,g}$ yields a function from $X \times X$ into Y. Now we state the propositions:

(9) (i) $\cdot_{\mathbb{R}_{r_1, r_2}}$ is convergent in the first coordinate and convergent in the second coordinate, and

(ii) the lim in the first coordinate of $\cdot_{\mathbb{R}_{r_1, r_2}}$ is convergent, and

(iii) the first coordinate major iterated lim of $\cdot_{\mathbb{R}\, r_1, r_2} = \lim r_1 \cdot \lim r_2$, and

(iv) the lim in the second coordinate of $\cdot_{\mathbb{R} r_1, r_2}$ is convergent, and

(v) the second coordinate major iterated lim of $\cdot_{\mathbb{R}\, r_1, r_2} = \lim r_1 \cdot \lim r_2$, and

(vi) $\cdot_{\mathbb{R} r_1, r_2}$ is p-convergent, and

(vii) P-lim $\cdot_{\mathbb{R} r_1, r_2} = \lim r_1 \cdot \lim r_2$.

Proof: Set $R = \cdot_{\mathbb{R} r_1, r_2}$. For every n and m, $R(n,m) = r_1(n) \cdot r_2(m)$ by [5, (77)]. For every element m of $\mathbb{N}$ and for every real number e such that $0 < e$ there exists N such that for every n such that $n \geqslant N$ holds $|(\text{curry}'(R,m))(n) - \lim r_1 \cdot r_2(m)| < e$ by [4, (47), (65), (44)]. For every element m of $\mathbb{N}$, curry$'(R,m)$ is convergent. For every element m of $\mathbb{N}$ and for every real number e such that $0 < e$ there exists N such that for every n such that $n \geqslant N$ holds $|(\text{curry}(R,m))(n) - r_1(m) \cdot \lim r_2| < e$ by [4, (47), (65), (44)]. For every element m of $\mathbb{N}$, curry(R,m) is convergent. For every e such that $0 < e$ there exists N such that for every n such that $n \geqslant N$ holds $|(\text{the lim in the first coordinate of } R)(n) - \lim r_1 \cdot \lim r_2| < e$ by [4, (46), (65)]. For every e such that $0 < e$ there exists N such that for every n such that $n \geqslant N$ holds $|(\text{the lim in the second coordinate of } R)(n) - \lim r_1 \cdot \lim r_2| < e$ by [4, (46), (65)]. For every e such that $0 < e$ there exists N such that for every n and m such that $n \geqslant N$ and $m \geqslant N$ holds $|R(n,m) - \lim r_1 \cdot \lim r_2| < e$ by [12, (3)], [4, (63), (46), (65)]. □

(10) (i) $+_{\mathbb{R} r_1, r_2}$ is convergent in the first coordinate and convergent in the second coordinate, and

(ii) the lim in the first coordinate of $+_{\mathbb{R} r_1, r_2}$ is convergent, and

(iii) the first coordinate major iterated lim of $+_{\mathbb{R}\, r_1, r_2} = \lim r_1 + \lim r_2$, and

(iv) the lim in the second coordinate of $+_{\mathbb{R} r_1, r_2}$ is convergent, and

(v) the second coordinate major iterated lim of $+_{\mathbb{R}\, r_1, r_2} = \lim r_1 + \lim r_2$, and

(vi) $+_{\mathbb{R} r_1, r_2}$ is p-convergent, and

(vii) P-lim $+_{\mathbb{R} r_1, r_2} = \lim r_1 + \lim r_2$.

Proof: Set $R = +_{\mathbb{R} r_1, r_2}$. For every n and m, $R(n,m) = r_1(n) + r_2(m)$ by [5, (77)]. For every element m of $\mathbb{N}$ and for every real number e such that $0 < e$ there exists a natural number N such that for every natural number n such that $n \geqslant N$ holds $|(\text{curry}'(R,m))(n) - (\lim r_1 + r_2(m))| < e$. For every element m of $\mathbb{N}$, curry$'(R,m)$ is convergent. For every element m of $\mathbb{N}$ and for every real number e such that $0 < e$ there exists N such that for every n such that $n \geqslant N$ holds $|(\text{curry}(R,m))(n) - (r_1(m) + \lim r_2)| < e$. For every element m of $\mathbb{N}$, curry(R,m) is convergent. For every e such that $0 < e$ there exists N such that for every n such that $n \geqslant N$ holds $|(\text{the lim in the first coordinate of } R)(n) - (\lim r_1 + \lim r_2)| < e$. For every e such that $0 < e$ there exists N such that for every n such that $n \geqslant N$ holds $|(\text{the lim in the second coordinate of } R)(n) - (\lim r_1 + \lim r_2)| < e$. For every e such that $0 < e$ there exists N such that for every n and m such that $n \geqslant N$ and $m \geqslant N$ holds $|R(n,m) - (\lim r_1 + \lim r_2)| < e$ by [4, (56)]. □

(11) Suppose R_1 is p-convergent and R_2 is p-convergent. Then

(i) $R_1 + R_2$ is p-convergent, and

(ii) $\text{P-lim}(R_1 + R_2) = \text{P-lim}\, R_1 + \text{P-lim}\, R_2$.

(12) Suppose R_1 is p-convergent and R_2 is p-convergent. Then

(i) $R_1 - R_2$ is p-convergent, and

(ii) $\text{P-lim}(R_1 - R_2) = \text{P-lim}\, R_1 - \text{P-lim}\, R_2$.

(13) Let us consider a function R from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$ and a real number r. Suppose R is p-convergent. Then

(i) $r \cdot R$ is p-convergent, and

(ii) $\text{P-lim}(r \cdot R) = r \cdot \text{P-lim}\, R$.

(14) If R is p-convergent and for every natural numbers n, m, $R(n,m) \geqslant r$, then $\text{P-lim}\, R \geqslant r$.

(15) Suppose R_1 is p-convergent and R_2 is p-convergent and for every natural numbers n, m, $R_1(n,m) \leqslant R_2(n,m)$. Then $\text{P-lim}\, R_1 \leqslant \text{P-lim}\, R_2$. The theorem is a consequence of (12) and (14).

(16) Suppose R_1 is p-convergent and R_2 is p-convergent and $\text{P-lim}\, R_1 = \text{P-lim}\, R_2$ and for every natural numbers n, m, $R_1(n,m) \leqslant R(n,m) \leqslant R_2(n,m)$. Then

(i) R is p-convergent, and

(ii) $\text{P-lim}\, R = \text{P-lim}\, R_1$.

PROOF: For every e such that $0 < e$ there exists N such that for every n and m such that $n \geqslant N$ and $m \geqslant N$ holds $|R(n,m) - \text{P-lim}\, R_1| < e$ by [14, (4), (5), (1)]. □

Let X be a non empty set and s_1 be a function from $\mathbb{N} \times \mathbb{N}$ into X. A subsequence of s_1 is a function from $\mathbb{N} \times \mathbb{N}$ into X and is defined by

(Def. 14) There exist increasing sequences N, M of $\mathbb{N}$ such that for every natural numbers n, m, $it(n,m) = s_1(N(n), M(m))$.

Let us consider P_1. Observe that every subsequence of P_1 is p-convergent.

Now we state the proposition:

(17) Let us consider a subsequence P_2 of P_1. Then $\text{P-lim}\, P_2 = \text{P-lim}\, P_1$.

Let R be a convergent in the first coordinate function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$. Note that every subsequence of R is convergent in the first coordinate.

Now we state the proposition:

(18) Let us consider a subsequence R_1 of R. Suppose

(i) R is convergent in the first coordinate, and

(ii) the lim in the first coordinate of R is convergent.

Then

(iii) the lim in the first coordinate of R_1 is convergent, and

(iv) the first coordinate major iterated lim of R_1 = the first coordinate major iterated lim of R.

PROOF: Consider I_1, I_2 being increasing sequences of $\mathbb{N}$ such that for every natural numbers n, m, $R_1(n, m) = R(I_1(n), I_2(m))$. For every e such that $0 < e$ there exists N such that for every m such that $m \geqslant N$ holds $|$(the lim in the first coordinate of $R_1)(m)$ − the first coordinate major iterated lim of $R| < e$. $\square$

Let R be a convergent in the second coordinate function from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{R}$. One can check that every subsequence of R is convergent in the second coordinate.

Now we state the proposition:

(19) Let us consider a subsequence R_1 of R. Suppose

(i) R is convergent in the second coordinate, and

(ii) the lim in the second coordinate of R is convergent.

Then

(iii) the lim in the second coordinate of R_1 is convergent, and

(iv) the second coordinate major iterated lim of R_1 = the second coordinate major iterated lim of R.

PROOF: Consider I_1, I_2 being increasing sequences of $\mathbb{N}$ such that for every n and m, $R_1(n, m) = R(I_1(n), I_2(m))$. For every e such that $0 < e$ there exists N such that for every m such that $m \geqslant N$ holds $|$(the lim in the second coordinate of $R_1)(m)$ − the second coordinate major iterated lim of $R| < e$. $\square$

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

[5] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 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] Noboru Endou, Keiko Narita, and Yasunari Shidama. The Lebesgue monotone convergence theorem. *Formalized Mathematics*, 16(**2**):167–175, 2008. doi:10.2478/v10037-008-0023-1.

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

[12] Jarosław Kotowicz. Convergent sequences and the limit of sequences. *Formalized Mathematics*, 1(**2**):273–275, 1990.

[13] Adam Naumowicz. Conjugate sequences, bounded complex sequences and convergent complex sequences. *Formalized Mathematics*, 6(**2**):265–268, 1997.

[14] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

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

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

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

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

Received August 31, 2013

FORMALIZED MATHEMATICS
Vol. 21, No. 3, Pages 171–184, 2013
DOI: 10.2478/forma-2013-0019

VERSITA
degruyter.com/view/j/forma

Formalization of the Advanced Encryption Standard. Part I[1]

Kenichi Arai[2]
Tokyo University of Science
Chiba, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. In this article, we formalize the Advanced Encryption Standard (AES). AES, which is the most widely used symmetric cryptosystem in the world, is a block cipher that was selected by the National Institute of Standards and Technology (NIST) as an official Federal Information Processing Standard for the United States in 2001 [12]. AES is the successor to DES [13], which was formerly the most widely used symmetric cryptosystem in the world. We formalize the AES algorithm according to [12]. We then verify the correctness of the formalized algorithm that the ciphertext encoded by the AES algorithm can be decoded uniquely by the same key. Please note the following points about this formalization: the AES round process is composed of the `SubBytes`, `ShiftRows`, `MixColumns`, and `AddRoundKey` transformations (see [12]). In this formalization, the `SubBytes` and `MixColumns` transformations are given as permutations, because it is necessary to treat the finite field GF(2^8) for those transformations. The formalization of AES that considers the finite field GF(2^8) is formalized by the future article.

MSC: 68P25 94A60 03B35

Keywords: Mizar formalization; Advanced Encryption Standard (AES) algorithm; cryptology

MML identifier: `AESCIP_1`, version: `8.1.02 5.19.1189`

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

[1]This work was supported by JSPS KAKENHI 21240001 and 22300285.

[2]This research was presented during the 2012 International Conference on Foundations of Computer Science FCS'12 in Las Vegas, USA.

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

1. Preliminaries

Let us consider natural numbers k, m. Now we state the propositions:

(1) If $m \neq 0$ and $(k+1) \bmod m \neq 0$, then $(k+1) \bmod m = (k \bmod m)+1$.

(2) If $m \neq 0$ and $(k+1) \bmod m \neq 0$, then $(k+1) \operatorname{div} m = k \operatorname{div} m$.

(3) If $m \neq 0$ and $(k+1) \bmod m = 0$, then $m-1 = k \bmod m$.

(4) If $m \neq 0$ and $(k+1) \bmod m = 0$, then $(k+1) \operatorname{div} m = (k \operatorname{div} m)+1$.

(5) $(k-m) \bmod m = k \bmod m$.

(6) If $m \neq 0$, then $(k-m) \operatorname{div} m = (k \operatorname{div} m) - 1$.

Let m, n be natural numbers, X, D be non empty sets, F be a function from X into $(D^n)^m$, and x be an element of X. Let us observe that the functor $F(x)$ yields an element of $(D^n)^m$. Let m be a natural number, X, Y, D be non empty sets, and F be a function from $X \times Y$ into D^m. Let y be an element of Y. Note that the functor $F(x,y)$ yields an element of D^m. Now we state the propositions:

(7) Let us consider natural numbers m, n, a non empty set D, and elements F_1, F_2 of $(D^n)^m$. Suppose natural numbers i, j. If $i \in \operatorname{Seg} m$ and $j \in \operatorname{Seg} n$, then $F_1(i)(j) = F_2(i)(j)$. Then $F_1 = F_2$.

(8) Let us consider a non empty set D and elements x_1, x_2, x_3, x_4 of D. Then $\langle x_1, x_2, x_3, x_4\rangle$ is an element of D^4.

(9) Let us consider a non empty set D and elements x_1, x_2, x_3, x_4, x_5 of D. Then $\langle x_1, x_2, x_3, x_4, x_5\rangle$ is an element of D^5.

(10) Let us consider a non empty set D and elements x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 of D. Then $\langle x_1, x_2, x_3, x_4\rangle \frown \langle x_5, x_6, x_7, x_8\rangle$ is an element of D^8. The theorem is a consequence of (8).

(11) Let us consider a non empty set D and elements x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10} of D. Then $\langle x_1, x_2, x_3, x_4, x_5\rangle \frown \langle x_6, x_7, x_8, x_9, x_{10}\rangle$ is an element of D^{10}. The theorem is a consequence of (9).

(12) Let us consider a non empty set D and elements x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 of D^4. Then $\langle x_1 \frown x_5, x_2 \frown x_6, x_3 \frown x_7, x_4 \frown x_8\rangle$ is an element of $(D^8)^4$. The theorem is a consequence of (8).

(13) Let us consider a non empty set D, an element x of $(D^4)^4$, and an element k of $\mathbb{N}$. Suppose $k \in \operatorname{Seg} 4$. Then there exist elements x_1, x_2, x_3, x_4 of D such that

   (i) $x_1 = x(k)(1)$, and

   (ii) $x_2 = x(k)(2)$, and

   (iii) $x_3 = x(k)(3)$, and

   (iv) $x_4 = x(k)(4)$.

(14) Let us consider non empty sets X, Y, a function f from X into Y, and a function g from Y into X. Suppose

(i) for every element x of X, $g(f(x)) = x$, and

(ii) for every element y of Y, $f(g(y)) = y$.

Then

(iii) f is one-to-one, and

(iv) f is onto, and

(v) g is one-to-one, and

(vi) g is onto, and

(vii) $g = f^{-1}$, and

(viii) $f = g^{-1}$.

2. State Array

The array of AES-State yielding a function from $Boolean^{128}$ into $((Boolean^{8})^{4})^{4}$ is defined by

(Def. 1) Let us consider an element i_1 of $Boolean^{128}$ and natural numbers i, j. Suppose $i, j \in \operatorname{Seg} 4$. Then $it(i_1)(i)(j) = \operatorname{mid}(i_1, (1 + (i -' 1) \cdot 8) + (j -' 1) \cdot 32, ((1 + (i -' 1) \cdot 8) + (j -' 1) \cdot 32) + 7)$.

Now we state the propositions:

(15) Let us consider a natural number k. Suppose $1 \leqslant k \leqslant 128$. Then there exist natural numbers i, j such that

(i) $i, j \in \operatorname{Seg} 4$, and

(ii) $(1+(i-'1)\cdot 8)+(j-'1)\cdot 32 \leqslant k \leqslant ((1+(i-'1)\cdot 8)+(j-'1)\cdot 32)+7$.

(16) Let us consider natural numbers i, j, i_0, j_0. Suppose

(i) $i, j, i_0, j_0 \in \operatorname{Seg} 4$, and

(ii) it is not true that $i = i_0$ and $j = j_0$.

Then $\{k,$ where k is a natural number $: (1 + (i -' 1) \cdot 8) + (j -' 1) \cdot 32 \leqslant k \leqslant (8 + (i -' 1) \cdot 8) + (j -' 1) \cdot 32\} \cap \{k,$ where k is a natural number $: (1 + (i_0 -' 1) \cdot 8) + (j_0 -' 1) \cdot 32 \leqslant k \leqslant (8 + (i_0 -' 1) \cdot 8) + (j_0 -' 1) \cdot 32\} = \emptyset$.

(17) Let us consider natural numbers k, i, j, i_0, j_0. Suppose

(i) $1 \leqslant k \leqslant 128$, and

(ii) $i, j, i_0, j_0 \in \operatorname{Seg} 4$, and

(iii) $(1+(i-'1)\cdot 8)+(j-'1)\cdot 32 \leqslant k \leqslant ((1+(i-'1)\cdot 8)+(j-'1)\cdot 32)+7$, and

(iv) $(1+(i_0-'1)\cdot 8)+(j_0-'1)\cdot 32 \leqslant k \leqslant ((1+(i_0-'1)\cdot 8)+(j_0-'1)\cdot 32)+7$.

Then

(v) $i = i_0$, and

(vi) $j = j_0$.

The theorem is a consequence of (16).

(18) The array of AES-State is one-to-one. The theorem is a consequence of (15). PROOF: For every elements x_1, x_2 such that x_1, $x_2 \in Boolean^{128}$ and (the array of AES-State)(x_1) = (the array of AES-State)(x_2) holds $x_1 = x_2$ by [15, (3)], [2, (11)], [4, (1)]. □

(19) The array of AES-State is onto. The theorem is a consequence of (15) and (17). PROOF: For every element y such that $y \in ((Boolean^8)^4)^4$ there exists an element x such that $x \in Boolean^{128}$ and y = (the array of AES-State)(x) by [4, (1)], [7, (3)], [15, (3)]. □

Let us note that the array of AES-State is bijective.

Now we state the proposition:

(20) Let us consider an element c of $((Boolean^8)^4)^4$. Then (the array of AES-State)((the array of AES-State)$^{-1}(c)$) = c.

3. SubBytes

In this paper S denotes a permutation of $Boolean^8$.

Let us consider S. The functor SubBytes(S) yielding a function from $((Boolean^8)^4)^4$ into $((Boolean^8)^4)^4$ is defined by

(Def. 2) Let us consider an element i_1 of $((Boolean^8)^4)^4$ and natural numbers i, j. Suppose $i, j \in \mathrm{Seg}\,4$. Then there exists an element i_2 of $Boolean^8$ such that

(i) $i_2 = i_1(i)(j)$, and

(ii) $it(i_1)(i)(j) = S(i_2)$.

The functor InvSubBytes(S) yielding a function from $((Boolean^8)^4)^4$ into $((Boolean^8)^4)^4$ is defined by

(Def. 3) Let us consider an element i_1 of $((Boolean^8)^4)^4$ and natural numbers i, j. Suppose $i, j \in \mathrm{Seg}\,4$. Then there exists an element i_2 of $Boolean^8$ such that

(i) $i_2 = i_1(i)(j)$, and

(ii) $it(i_1)(i)(j) = S^{-1}(i_2)$.

Now we state the propositions:

(21) Let us consider an element i_1 of $((Boolean^8)^4)^4$.
Then $(\mathtt{InvSubBytes}(S))((\mathtt{SubBytes}(S))(i_1)) = i_1$. The theorem is a consequence of (7).

(22) Let us consider an element o of $((Boolean^8)^4)^4$.
Then $(\mathtt{SubBytes}(S))((\mathtt{InvSubBytes}(S))(o)) = o$. The theorem is a consequence of (7).

(23) (i) $\mathtt{SubBytes}(S)$ is one-to-one, and

(ii) $\mathtt{SubBytes}(S)$ is onto, and

(iii) $\mathtt{InvSubBytes}(S)$ is one-to-one, and

(iv) $\mathtt{InvSubBytes}(S)$ is onto, and

(v) $\mathtt{InvSubBytes}(S) = (\mathtt{SubBytes}(S))^{-1}$, and

(vi) $\mathtt{SubBytes}(S) = (\mathtt{InvSubBytes}(S))^{-1}$.

The theorem is a consequence of (21), (22), and (14).

4. ShiftRows

The functor ShiftRows yielding a function from $((Boolean^8)^4)^4$ into $((Boolean^8)^4)^4$ is defined by

(Def. 4) Let us consider an element i_1 of $((Boolean^8)^4)^4$ and a natural number i. Suppose $i \in \mathrm{Seg}\,4$. Then there exists an element x_i of $(Boolean^8)^4$ such that

(i) $x_i = i_1(i)$, and

(ii) $it(i_1)(i) = \text{Op-Shift}(x_i, 5 - i)$.

The functor InvShiftRows yielding a function from $((Boolean^8)^4)^4$ into $((Boolean^8)^4)^4$ is defined by

(Def. 5) Let us consider an element i_1 of $((Boolean^8)^4)^4$ and a natural number i. Suppose $i \in \mathrm{Seg}\,4$. Then there exists an element x_i of $(Boolean^8)^4$ such that

(i) $x_i = i_1(i)$, and

(ii) $it(i_1)(i) = \text{Op-Shift}(x_i, i - 1)$.

Now we state the propositions:

(24) Let us consider an element i_1 of $((Boolean^8)^4)^4$.
Then $\mathtt{InvShiftRows}(\mathtt{ShiftRows}(i_1)) = i_1$.

(25) Let us consider an element o of $((Boolean^8)^4)^4$.
Then $\mathtt{ShiftRows}(\mathtt{InvShiftRows}(o)) = o$.

(26) (i) ShiftRows is one-to-one, and

(ii) ShiftRows is onto, and

(iii) `InvShiftRows` is one-to-one, and

(iv) `InvShiftRows` is onto, and

(v) $\texttt{InvShiftRows} = \texttt{ShiftRows}^{-1}$, and

(vi) $\texttt{ShiftRows} = \texttt{InvShiftRows}^{-1}$.

5. AddRoundKey

The functor `AddRoundKey` yielding a function from $((Boolean^8)^4)^4 \times ((Boolean^8)^4)^4$ into $((Boolean^8)^4)^4$ is defined by

(Def. 6) Let us consider elements t_1, k_1 of $((Boolean^8)^4)^4$ and natural numbers i, j. Suppose $i, j \in \mathrm{Seg}\,4$. Then there exist elements t_2, k_2 of $Boolean^8$ such that

(i) $t_2 = t_1(i)(j)$, and

(ii) $k_2 = k_1(i)(j)$, and

(iii) $it(t_1, k_1)(i)(j) = \text{Op-XOR}(t_2, k_2)$.

6. Key Expansion

Let us consider S. Let x be an element of $(Boolean^8)^4$.
The functor $\texttt{SubWord}(S, x)$ yielding an element of $(Boolean^8)^4$ is defined by

(Def. 7) Let us consider an element i of $\mathrm{Seg}\,4$. Then $it(i) = S(x(i))$.

The functor $\texttt{RotWord}(x)$ yielding an element of $(Boolean^8)^4$ is defined by the term

(Def. 8) $\text{Op-LeftShift}\,x$.

Let n, m be non zero elements of $\mathbb{N}$ and s, t be elements of $(Boolean^n)^m$.
The functor $\texttt{XOR-Word}(s, t)$ yielding an element of $(Boolean^n)^m$ is defined by

(Def. 9) Let us consider an element i of $\mathrm{Seg}\,m$. Then $it(i) = \text{Op-XOR}(s(i), t(i))$.

The functor `Rcon` yielding an element of $((Boolean^8)^4)^{10}$ is defined by

(Def. 10) (i) $it(1) = \langle\langle 0,0,0,0\rangle \frown \langle 0,0,0,1\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0, 0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(ii) $it(2) = \langle\langle 0,0,0,0\rangle \frown \langle 0,0,1,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0, 0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(iii) $it(3) = \langle\langle 0,0,0,0\rangle \frown \langle 0,1,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0, 0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(iv) $it(4) = \langle\langle 0,0,0,0\rangle \frown \langle 1,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0, 0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(v) $it(5) = \langle\langle 0,0,0,1\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0, 0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(vi) $it(6) = \langle\langle 0,0,1,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0, 0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(vii) $it(7) = \langle\langle 0,1,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0, 0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(viii) $it(8) = \langle\langle 1,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0, 0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(ix) $it(9) = \langle\langle 0,0,0,1\rangle \frown \langle 1,0,1,1\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0, 0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(x) $it(10) = \langle\langle 0,0,1,1\rangle \frown \langle 0,1,1,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0, 0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$.

Let us consider S. Let m, i be natural numbers and w be an element of $(Boolean^8)^4$. Assume $m = 4$ or $m = 6$ or $m = 8$ and $i < 4 \cdot (7 + m)$ and $m \leqslant i$. The functor $\texttt{KeyExpansionT}(S, m, i, w)$ yielding an element of $(Boolean^8)^4$ is defined by

(Def. 11) (i) there exists an element T_3 of $(Boolean^8)^4$ such that $T_3 = \texttt{Rcon}(\frac{i}{m})$ and $it = \texttt{XOR-Word}(\texttt{SubWord}(S, (\texttt{RotWord}(w))), T_3)$, **if** $i \bmod m = 0$,

(ii) $it = \texttt{SubWord}(S, w)$, **if** $m = 8$ and $i \bmod 8 = 4$,

(iii) $it = w$, **otherwise**.

Let m be a natural number. Assume $m = 4$ or $m = 6$ or $m = 8$. The functor $\texttt{KeyExpansionW}(S, m)$ yielding a function from $((Boolean^8)^4)^m$ into $((Boolean^8)^4)^{4\cdot(7+m)}$ is defined by

(Def. 12) Let us consider an element K of $((Boolean^8)^4)^m$. Then

(i) for every element i of $\mathbb{N}$ such that $i < m$ holds $it(K)(i+1) = K(i+1)$, and

(ii) for every element i of $\mathbb{N}$ such that $m \leqslant i < 4 \cdot (7 + m)$ there exists an element P of $(Boolean^8)^4$ and there exists an element Q of $(Boolean^8)^4$ such that $P = it(K)((i - m) + 1)$ and $Q = it(K)(i)$ and $it(K)(i + 1) = \texttt{XOR-Word}(P, (\texttt{KeyExpansionT}(S, m, i, Q)))$.

The functor $\texttt{KeyExpansion}(S, m)$ yielding a function from $((Boolean^8)^4)^m$ into $(((Boolean^8)^4)^4)^{7+m}$ is defined by

(Def. 13) Let us consider an element K of $((Boolean^8)^4)^m$. Then there exists an element w of $((Boolean^8)^4)^{4\cdot(7+m)}$ such that

(i) $w = (\texttt{KeyExpansionW}(S, m))(K)$, and

(ii) for every natural number i such that $i < 7 + m$ holds $it(K)(i + 1) = \langle w(4 \cdot i + 1), w(4 \cdot i + 2), w(4 \cdot i + 3), w(4 \cdot i + 4)\rangle$.

7. Encryption and Decryption

In the sequel $\mathcal{M}_1$ denotes a permutation of $((Boolean^8)^4)^4$ and $\mathcal{M}_2$ denotes a permutation of $((Boolean^8)^4)^4$.

Let us consider S and $\mathcal{M}_1$. Let m be a natural number, t_1 be an element of $((Boolean^8)^4)^4$, and K be an element of $((Boolean^8)^4)^m$. The functor AES-Cipher$(S, \mathcal{M}_1, t_1, K)$ yielding an element of $((Boolean^8)^4)^4$ is defined by

(Def. 14) There exists a finite sequence s_1 of elements of $((Boolean^8)^4)^4$ such that

(i) $\operatorname{len} s_1 = (7+m) - 1$, and

(ii) there exists an element K_1 of $((Boolean^8)^4)^4$ such that $K_1 = (\mathtt{KeyExpansion}(S, m))(K)(1)$ and $s_1(1) = \mathtt{AddRoundKey}(t_1, K_1)$, and

(iii) for every natural number i such that $1 \leqslant i < (7+m) - 1$ there exists an element K_i of $((Boolean^8)^4)^4$ such that $K_i = (\mathtt{KeyExpansion}(S, m))(K)(i+1)$ and $s_1(i+1) = \mathtt{AddRoundKey}(((\mathcal{M}_1 \cdot \mathtt{ShiftRows}) \cdot \mathtt{SubBytes}(S))(s_1(i)), K_i)$, and

(iv) there exists an element K_n of $((Boolean^8)^4)^4$ such that $K_n = (\mathtt{KeyExpansion}(S, m))(K)(7+m)$ and $it = \mathtt{AddRoundKey}((\mathtt{ShiftRows} \cdot \mathtt{SubBytes}(S))(s_1((7+m)-1)), K_n)$.

The functor AES-InvCipher$(S, \mathcal{M}_1, t_1, K)$ yielding an element of $((Boolean^8)^4)^4$ is defined by

(Def. 15) There exists a finite sequence s_1 of elements of $((Boolean^8)^4)^4$ such that

(i) $\operatorname{len} s_1 = (7+m) - 1$, and

(ii) there exists an element K_1 of $((Boolean^8)^4)^4$ such that $K_1 = (\operatorname{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(1)$ and $s_1(1) = (\mathtt{InvSubBytes}(S) \cdot \mathtt{InvShiftRows})(\mathtt{AddRoundKey}(t_1, K_1))$, and

(iii) for every natural number i such that $1 \leqslant i < (7+m) - 1$ there exists an element K_i of $((Boolean^8)^4)^4$ such that $K_i = (\operatorname{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(i+1)$ and $s_1(i+1) = ((\mathtt{InvSubBytes}(S) \cdot \mathtt{InvShiftRows}) \cdot {\mathcal{M}_1}^{-1})(\mathtt{AddRoundKey}(s_1(i), K_i))$, and

(iv) there exists an element K_n of $((Boolean^8)^4)^4$ such that $K_n = (\operatorname{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(7+m)$ and $it = \mathtt{AddRoundKey}(s_1((7+m)-1), K_n)$.

Now we state the propositions:

(27) Let us consider an element i_1 of $((Boolean^8)^4)^4$. Then ${\mathcal{M}_1}^{-1}(\mathcal{M}_1(i_1)) = i_1$.

(28) Let us consider an element o of $((Boolean^8)^4)^4$. Then $\mathcal{M}_1({\mathcal{M}_1}^{-1}(o)) = o$.

Let us consider a natural number m and an element t_1 of $((Boolean^8)^4)^4$. Now we state the propositions:

(29) $(\texttt{InvSubBytes}(S) \cdot \texttt{InvShiftRows})((\texttt{ShiftRows} \cdot \texttt{SubBytes}(S))(t_1)) = t_1$.

(30) $((\texttt{InvSubBytes}(S) \cdot \texttt{InvShiftRows}) \cdot {\mathcal{M}_1}^{-1})(((\mathcal{M}_1 \cdot \texttt{ShiftRows}) \cdot \texttt{SubBytes}(S))(t_1)) = t_1$.

Now we state the propositions:

(31) Let us consider a natural number m, an element t_1 of $((Boolean^8)^4)^4$, an element K of $((Boolean^8)^4)^m$, and elements d_k, e_k of $((Boolean^8)^4)^4$. Suppose

  (i) $m = 4$ or $m = 6$ or $m = 8$, and

  (ii) $d_k = (\mathrm{Rev}((\texttt{KeyExpansion}(S, m))(K)))(1)$, and

  (iii) $e_k = (\texttt{KeyExpansion}(S, m))(K)(7 + m)$.

Then $\texttt{AddRoundKey}(\texttt{AddRoundKey}(t_1, e_k), d_k) = t_1$. The theorem is a consequence of (7).

(32) Let us consider a natural number m, an element t_1 of $((Boolean^8)^4)^4$, an element k_1 of $((Boolean^8)^4)^m$, and elements d_k, e_k of $((Boolean^8)^4)^4$. Suppose

  (i) $m = 4$ or $m = 6$ or $m = 8$, and

  (ii) $d_k = (\texttt{KeyExpansion}(S, m))(k_1)(1)$, and

  (iii) $e_k = (\mathrm{Rev}((\texttt{KeyExpansion}(S, m))(k_1)))(7 + m)$.

Then $\texttt{AddRoundKey}(\texttt{AddRoundKey}(t_1, e_k), d_k) = t_1$. The theorem is a consequence of (7).

(33) Let us consider a natural number m, elements t_1, o_1 of $((Boolean^8)^4)^4$, an element K of $((Boolean^8)^4)^m$, and elements K_1, K_n of $((Boolean^8)^4)^4$. Suppose

  (i) $m = 4$ or $m = 6$ or $m = 8$, and

  (ii) $K_1 = (\texttt{KeyExpansion}(S, m))(K)(1)$, and

  (iii) $K_n = (\mathrm{Rev}((\texttt{KeyExpansion}(S, m))(K)))(7 + m)$, and

  (iv) $o_1 = \texttt{AddRoundKey}((\texttt{ShiftRows} \cdot \texttt{SubBytes}(S))(t_1), K_n)$.

Then $(\texttt{InvSubBytes}(S) \cdot \texttt{InvShiftRows})(\texttt{AddRoundKey}(o_1, K_1)) = t_1$. The theorem is a consequence of (32) and (29).

(34) Let us consider natural numbers m, i, an element t_1 of $((Boolean^8)^4)^4$, an element K of $((Boolean^8)^4)^m$, and elements e_i, d_i of $((Boolean^8)^4)^4$. Suppose

  (i) $m = 4$ or $m = 6$ or $m = 8$, and

  (ii) $i \leqslant (7 + m) - 1$, and

  (iii) $e_i = (\texttt{KeyExpansion}(S, m))(K)((7 + m) - i)$, and

(iv) $d_i = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(i + 1)$.

Then $\mathtt{AddRoundKey}(\mathtt{AddRoundKey}(t_1, e_i), d_i) = t_1$. The theorem is a consequence of (7).

(35) Let us consider a natural number m, an element t_1 of $((Boolean^8)^4)^4$, and an element K of $((Boolean^8)^4)^m$. Suppose

(i) $m = 4$, or

(ii) $m = 6$, or

(iii) $m = 8$.

Then $\text{AES-InvCipher}(S, \mathcal{M}_1, (\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K)), K) = t_1$. The theorem is a consequence of (34) and (30). PROOF: Reconsider $N = (7 + m) - 1$ as a natural number. Consider e_s being a finite sequence of elements of $((Boolean^8)^4)^4$ such that $\operatorname{len} e_s = N$ and there exists an element K_1 of $((Boolean^8)^4)^4$ such that $K_1 = (\mathtt{KeyExpansion}(S, m))(K)(1)$ and $e_s(1) = \mathtt{AddRoundKey}(t_1, K_1)$ and for every natural number i such that $1 \leqslant i < N$ there exists an element K_i of $((Boolean^8)^4)^4$ such that $K_i = (\mathtt{KeyExpansion}(S, m))(K)(i+1)$ and $e_s(i+1) = \mathtt{AddRoundKey}(((\mathcal{M}_1 \cdot \mathtt{ShiftRows}) \cdot \mathtt{SubBytes}(S))(e_s(i)), K_i)$ and there exists an element K_n of $((Boolean^8)^4)^4$ such that $K_n = (\mathtt{KeyExpansion}(S, m))(K)(7 + m)$ and $\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K) = \mathtt{AddRoundKey}((\mathtt{ShiftRows} \cdot \mathtt{SubBytes}(S))(e_s(N)), K_n)$. Consider d_s being a finite sequence of elements of $((Boolean^8)^4)^4$ such that $\operatorname{len} d_s = N$ and there exists an element K_1 of $((Boolean^8)^4)^4$ such that $K_1 = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(1)$ and $d_s(1) = (\mathtt{InvSubBytes}(S) \cdot \mathtt{InvShiftRows})(\mathtt{AddRoundKey}(\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K), K_1))$ and for every natural number i such that $1 \leqslant i < N$ there exists an element K_i of $((Boolean^8)^4)^4$ such that $K_i = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(i+1)$ and $d_s(i+1) = ((\mathtt{InvSubBytes}(S) \cdot \mathtt{InvShiftRows}) \cdot {\mathcal{M}_1}^{-1})(\mathtt{AddRoundKey}(d_s(i), K_i))$ and there exists an element K_n of $((Boolean^8)^4)^4$ such that $K_n = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(7 + m)$ and $\text{AES-InvCipher}(S, \mathcal{M}_1, (\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K)), K) = \mathtt{AddRoundKey}(d_s(N), K_n)$. Consider e_1 being an element of $((Boolean^8)^4)^4$ such that $e_1 = (\mathtt{KeyExpansion}(S, m))(K)(1)$ and $e_s(1) = \mathtt{AddRoundKey}(t_1, e_1)$. Consider e_n being an element of $((Boolean^8)^4)^4$ such that $e_n = (\mathtt{KeyExpansion}(S, m))(K)(7 + m)$ and $\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K) = \mathtt{AddRoundKey}((\mathtt{ShiftRows} \cdot \mathtt{SubBytes}(S))(e_s(N)), e_n)$. Consider d_1 being an element of $((Boolean^8)^4)^4$ such that $d_1 = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(1)$ and $d_s(1) = (\mathtt{InvSubBytes}(S) \cdot \mathtt{InvShiftRows})(\mathtt{AddRoundKey}(\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K), d_1))$. Consider d_n being an element of $((Boolean^8)^4)^4$ such that $d_n = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(7+m)$ and $\text{AES-InvCipher}(S, \mathcal{M}_1, (\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K)), K) = \mathtt{AddRoundKey}(d_s(N), d_n)$. Define $\mathcal{R}[\text{natural number}] \equiv$ if $\$_1 < N$, then $d_s(\$_1 + 1) = e_s(N - \$_1)$. For every natural number i such that $\mathcal{R}[i]$

holds $\mathcal{R}[i+1]$ by [2, (11)], [15, (3)], [2, (14)]. For every natural number k, $\mathcal{R}[k]$ from [2, Sch. 2]. $\square$

(36) Let us consider a non empty set D, non zero elements n, m of $\mathbb{N}$, and an element r of D^n. Suppose

(i) $m \leqslant n$, and

(ii) $8 \leqslant n - m$.

Then Op-Left(Op-Right$(r, m), 8)$ is an element of D^8.

Let r be an element of $Boolean^{128}$. The functor AES-InitState128Key(r) yielding an element of $((Boolean^8)^4)^4$ is defined by

(Def. 16) (i) $it(1) = \langle$Op-Left$(r, 8)$, Op-Left(Op-Right$(r, 8), 8)$, Op-Left(Op-Right $(r, 16), 8)$, Op-Left(Op-Right$(r, 24), 8)\rangle$, and

(ii) $it(2) = \langle$Op-Left(Op-Right$(r, 32), 8)$, Op-Left(Op-Right$(r, 40), 8)$, Op-Left(Op-Right$(r, 48), 8)$, Op-Left(Op-Right$(r, 56), 8)\rangle$, and

(iii) $it(3) = \langle$Op-Left(Op-Right$(r, 64), 8)$, Op-Left(Op-Right$(r, 72), 8)$, Op-Left(Op-Right$(r, 80), 8)$, Op-Left(Op-Right$(r, 88), 8)\rangle$, and

(iv) $it(4) = \langle$Op-Left(Op-Right$(r, 96), 8)$, Op-Left(Op-Right$(r, 104), 8)$, Op-Left(Op-Right$(r, 112), 8)$, Op-Right$(r, 120)\rangle$.

Let r be an element of $Boolean^{192}$. The functor AES-InitState192Key(r) yielding an element of $((Boolean^8)^4)^6$ is defined by

(Def. 17) (i) $it(1) = \langle$Op-Left$(r, 8)$, Op-Left(Op-Right$(r, 8), 8)$, Op-Left(Op-Right $(r, 16), 8)$, Op-Left(Op-Right$(r, 24), 8)\rangle$, and

(ii) $it(2) = \langle$Op-Left(Op-Right$(r, 32), 8)$, Op-Left(Op-Right$(r, 40), 8)$, Op-Left(Op-Right$(r, 48), 8)$, Op-Left(Op-Right$(r, 56), 8)\rangle$, and

(iii) $it(3) = \langle$Op-Left(Op-Right$(r, 64), 8)$, Op-Left(Op-Right$(r, 72), 8)$, Op-Left(Op-Right$(r, 80), 8)$, Op-Left(Op-Right$(r, 88), 8)\rangle$, and

(iv) $it(4) = \langle$Op-Left(Op-Right$(r, 96), 8)$, Op-Left(Op-Right$(r, 104), 8)$, Op-Left(Op-Right$(r, 112), 8)$, Op-Left(Op-Right$(r, 120), 8)\rangle$, and

(v) $it(5) = \langle$Op-Left(Op-Right$(r, 128), 8)$, Op-Left(Op-Right$(r, 136), 8)$, Op-Left(Op-Right$(r, 144), 8)$, Op-Left(Op-Right$(r, 152), 8)\rangle$, and

(vi) $it(6) = \langle$Op-Left(Op-Right$(r, 160), 8)$, Op-Left(Op-Right$(r, 168), 8)$, Op-Left(Op-Right$(r, 176), 8)$, Op-Right$(r, 184)\rangle$.

Let r be an element of $Boolean^{256}$. The functor AES-InitState256Key(r) yielding an element of $((Boolean^8)^4)^8$ is defined by

(Def. 18) (i) $it(1) = \langle$Op-Left$(r, 8)$, Op-Left(Op-Right$(r, 8), 8)$, Op-Left (Op-Right$(r, 16), 8)$, Op-Left(Op-Right$(r, 24), 8)\rangle$, and

(ii) $it(2) = \langle$Op-Left(Op-Right$(r, 32), 8)$, Op-Left(Op-Right$(r, 40), 8)$, Op-Left(Op-Right$(r, 48), 8)$, Op-Left(Op-Right$(r, 56), 8)\rangle$, and

(iii) $it(3) = \langle$Op-Left(Op-Right$(r, 64), 8)$, Op-Left(Op-Right$(r, 72), 8)$, Op-Left(Op-Right$(r, 80), 8)$, Op-Left(Op-Right$(r, 88), 8)\rangle$, and

(iv) $it(4) = \langle$Op-Left(Op-Right$(r, 96), 8)$, Op-Left(Op-Right$(r, 104), 8)$, Op-Left(Op-Right$(r, 112), 8)$, Op-Left(Op-Right$(r, 120), 8)\rangle$, and

(v) $it(5) = \langle$Op-Left(Op-Right$(r, 128), 8)$, Op-Left(Op-Right$(r, 136), 8)$, Op-Left(Op-Right$(r, 144), 8)$, Op-Left(Op-Right$(r, 152), 8)\rangle$, and

(vi) $it(6) = \langle$Op-Left(Op-Right$(r, 160), 8)$, Op-Left(Op-Right$(r, 168), 8)$, Op-Left(Op-Right$(r, 176), 8)$, Op-Left(Op-Right$(r, 184), 8)\rangle$, and

(vii) $it(7) = \langle$Op-Left(Op-Right$(r, 192), 8)$, Op-Left(Op-Right$(r, 200), 8)$, Op-Left(Op-Right$(r, 208), 8)$, Op-Left(Op-Right$(r, 216), 8)\rangle$, and

(viii) $it(8) = \langle$Op-Left(Op-Right$(r, 224), 8)$, Op-Left(Op-Right$(r, 232), 8)$, Op-Left(Op-Right$(r, 240), 8)$, Op-Right$(r, 248)\rangle$.

Let us consider S and $\mathcal{M}_2$. Let m_1 be an element of $Boolean^{128}$ and K be an element of $Boolean^{128}$. The functor AES-128enc$(S, \mathcal{M}_2, m_1, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 19) (The array of AES-State)$^{-1}$(AES-Cipher$(S, \mathcal{M}_2$, ((the array of AES-State)(m_1)), (AES-InitState128Key(K)))).

Let c be an element of $Boolean^{128}$. The functor AES-128dec$(S, \mathcal{M}_2, c, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 20) (The array of AES-State)$^{-1}$(AES-InvCipher$(S, \mathcal{M}_2$, ((the array of AES-State)(c)), (AES-InitState128Key(K)))).

Now we state the proposition:

(37) Let us consider a permutation S of $Boolean^8$, a permutation $\mathcal{M}_2$ of $((Boolean^8)^4)^4$, and elements m_1, K of $Boolean^{128}$.
Then AES-128dec$(S, \mathcal{M}_2$, (AES-128enc$(S, \mathcal{M}_2, m_1, K)$), $K) = m_1$. The theorem is a consequence of (20) and (35).

Let us consider S and $\mathcal{M}_2$. Let m_1 be an element of $Boolean^{128}$ and K be an element of $Boolean^{192}$. The functor AES-192enc$(S, \mathcal{M}_2, m_1, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 21) (The array of AES-State)$^{-1}$(AES-Cipher$(S, \mathcal{M}_2$, ((the array of AES-State)(m_1)), (AES-InitState192Key(K)))).

Let c be an element of $Boolean^{128}$. The functor AES-192dec$(S, \mathcal{M}_2, c, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 22) (The array of AES-State)$^{-1}$(AES-InvCipher$(S, \mathcal{M}_2$, ((the array of AES-State)(c)), (AES-InitState192Key(K)))).

Now we state the proposition:

(38) Let us consider a permutation S of $Boolean^8$, a permutation $\mathcal{M}_2$ of $((Boolean^8)^4)^4$, an element m_1 of $Boolean^{128}$, and an element K of $Boolean^{192}$.

Then AES-192dec$(S, \mathcal{M}_2, (\text{AES-192enc}(S, \mathcal{M}_2, m_1, K)), K) = m_1$. The theorem is a consequence of (20) and (35).

Let us consider S and $\mathcal{M}_2$. Let m_1 be an element of $Boolean^{128}$ and K be an element of $Boolean^{256}$. The functor AES-256enc$(S, \mathcal{M}_2, m_1, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 23) (The array of AES-State)$^{-1}$(AES-Cipher$(S, \mathcal{M}_2$, ((the array of AES-State)(m_1)), (AES-InitState256Key(K)))).

Let c be an element of $Boolean^{128}$. The functor AES-256dec$(S, \mathcal{M}_2, c, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 24) (The array of AES-State)$^{-1}$(AES-InvCipher$(S, \mathcal{M}_2$, ((the array of AES-State)(c)), (AES-InitState256Key(K)))).

Now we state the proposition:

(39) Let us consider a permutation S of $Boolean^8$, a permutation $\mathcal{M}_2$ of $((Boolean^8)^4)^4$, an element m_1 of $Boolean^{128}$, and an element K of $Boolean^{256}$.
Then AES-256dec$(S, \mathcal{M}_2, (\text{AES-256enc}(S, \mathcal{M}_2, m_1, K)), K) = m_1$. The theorem is a consequence of (20) and (35).

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[5] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[12] U.S. Department of Commerce/National Institute of Standards and Technology. FIPS PUB 197, Advanced Encryption Standard (AES). *Federal Information Processing Standars Publication*, 2001.
[13] Hiroyuki Okazaki and Yasunari Shidama. Formalization of the data encryption standard. *Formalized Mathematics*, 20(**2**):125–146, 2012. doi:10.2478/v10037-012-0016-y.
[14] Andrzej Trybulec. On the decomposition of finite sequences. *Formalized Mathematics*, 5 (**3**):317–322, 1996.
[15] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[16] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[17] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

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

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

Received October 7, 2013

FORMALIZED MATHEMATICS
Vol. 21, No. 3, Pages 185–191, 2013
DOI: 10.2478/forma-2013-0020

VERSITA
degruyter.com/view/j/forma

The Linearity of Riemann Integral on Functions from ℝ into Real Banach Space[1]

Keiko Narita
Hirosaki-city
Aomori, Japan

Noboru Endou
Gifu National College of Technology
Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we described basic properties of Riemann integral on functions from ℝ into Real Banach Space. We proved mainly the linearity of integral operator about the integral of continuous functions on closed interval of the set of real numbers. These theorems were based on the article [10] and we referred to the former articles about Riemann integral. We applied definitions and theorems introduced in the article [9] and the article [11] to the proof. Using the definition of the article [10], we also proved some theorems on bounded functions.

MSC: 26A42 03B35

Keywords: formalization of Riemann integral

MML identifier: `INTEGR21`, version: `8.1.02 5.19.1189`

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

1. Some Properties of Bounded Functions

In this paper Z denotes a real normed space, a, b, c, d, e, r denote real numbers, and A, B denote non empty closed interval subsets of ℝ.

Let us consider a partial function f from ℝ to the carrier of Z. Now we state the propositions:

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

(1) If f is bounded and $A \subseteq \operatorname{dom} f$, then $f{\restriction}A$ is bounded.

(2) If $f{\restriction}A$ is bounded and $B \subseteq A$ and $B \subseteq \operatorname{dom}(f{\restriction}A)$, then $f{\restriction}B$ is bounded.

(3) If $a \leqslant c \leqslant d \leqslant b$ and $f{\restriction}[a,b]$ is bounded and $[a,b] \subseteq \operatorname{dom} f$, then $f{\restriction}[c,d]$ is bounded.

Now we state the proposition:

(4) Let us consider sets X, Y and partial functions f_1, f_2 from $\mathbb{R}$ to the carrier of Z. Suppose

(i) $f_1{\restriction}X$ is bounded, and

(ii) $f_2{\restriction}Y$ is bounded.

Then

(iii) $(f_1 + f_2){\restriction}(X \cap Y)$ is bounded, and

(iv) $(f_1 - f_2){\restriction}(X \cap Y)$ is bounded.

Let us consider a set X and a partial function f from $\mathbb{R}$ to the carrier of Z. Now we state the propositions:

(5) If $f{\restriction}X$ is bounded, then $(r \cdot f){\restriction}X$ is bounded.

(6) If $f{\restriction}X$ is bounded, then $(-f){\restriction}X$ is bounded.

Now we state the propositions:

(7) Let us consider a function f from A into the carrier of Z. Then f is bounded if and only if $\|f\|$ is bounded.

(8) Let us consider a partial function f from $\mathbb{R}$ to the carrier of Z. Suppose $A \subseteq \operatorname{dom} f$. Then $\|f{\restriction}A\| = \|f\|{\restriction}A$.

(9) Let us consider a partial function g from $\mathbb{R}$ to the carrier of Z. Suppose

(i) $A \subseteq \operatorname{dom} g$, and

(ii) $g{\restriction}A$ is bounded.

Then $\|g\|{\restriction}A$ is bounded. The theorem is a consequence of (8) and (7).

2. Some Properties of Integral of Continuous Functions

In the sequel X, Y denote real Banach spaces and E denotes a point of Y.

Let us consider a real normed space Y and a continuous partial function f from $\mathbb{R}$ to the carrier of Y. Now we state the propositions:

(10) If $a \leqslant b$ and $[a,b] \subseteq \operatorname{dom} f$, then $\|f\|{\restriction}[a,b]$ is bounded.

(11) If $a \leqslant b$ and $[a,b] \subseteq \operatorname{dom} f$, then $f{\restriction}[a,b]$ is bounded.

(12) If $a \leqslant b$ and $[a,b] \subseteq \operatorname{dom} f$, then $\|f\|$ is integrable on $[a,b]$.

Now we state the propositions:

(13) Let us consider a continuous partial function f from $\mathbb{R}$ to the carrier of Y. Suppose

(i) $a \leqslant c \leqslant d \leqslant b$, and

(ii) $[a, b] \subseteq \operatorname{dom} f$.

Then f is integrable on $[c, d]$.

(14) Let us consider a partial function f from $\mathbb{R}$ to the carrier of Y. Suppose

(i) $a \leqslant b$, and

(ii) $[a, b] \subseteq \operatorname{dom} f$.

Then $\int\limits_{b}^{a} f(x)dx = -\int\limits_{a}^{b} f(x)dx$.

(15) Let us consider a continuous partial function f from $\mathbb{R}$ to the carrier of Y. Suppose

(i) $a \leqslant b$, and

(ii) $[a, b] \subseteq \operatorname{dom} f$, and

(iii) $c \in [a, b]$.

Then

(iv) f is integrable on $[a, c]$, and

(v) f is integrable on $[c, b]$, and

(vi) $\int\limits_{a}^{b} f(x)dx = \int\limits_{a}^{c} f(x)dx + \int\limits_{c}^{b} f(x)dx$.

The theorem is a consequence of (13).

(16) Let us consider continuous partial functions f, g from $\mathbb{R}$ to the carrier of Y. Suppose

(i) $a \leqslant c \leqslant d \leqslant b$, and

(ii) $[a, b] \subseteq \operatorname{dom} f$, and

(iii) $[a, b] \subseteq \operatorname{dom} g$.

Then

(iv) $f + g$ is integrable on $[c, d]$, and

(v) $(f + g)\restriction[c, d]$ is bounded.

The theorem is a consequence of (13), (11), (3), and (4).

Let us consider a continuous partial function f from $\mathbb{R}$ to the carrier of Y. Now we state the propositions:

(17) If $a \leqslant c \leqslant d \leqslant b$ and $[a, b] \subseteq \operatorname{dom} f$, then $r \cdot f$ is integrable on $[c, d]$ and $(r \cdot f)\restriction[c, d]$ is bounded.

(18) Suppose $a \leqslant c \leqslant d \leqslant b$ and f is integrable on $[a, b]$ and $f\restriction[a, b]$ is bounded and $[a, b] \subseteq \operatorname{dom} f$. Then

(i) $-f$ is integrable on $[c,d]$, and

(ii) $(-f)\restriction[c,d]$ is bounded.

Now we state the proposition:

(19) Let us consider continuous partial functions f, g from $\mathbb{R}$ to the carrier of Y. Suppose

(i) $a \leqslant c \leqslant d \leqslant b$, and

(ii) $[a,b] \subseteq \operatorname{dom} f$, and

(iii) $[a,b] \subseteq \operatorname{dom} g$.

Then

(iv) $f-g$ is integrable on $[c,d]$, and

(v) $(f-g)\restriction[c,d]$ is bounded.

The theorem is a consequence of (11), (13), (3), and (4).

Let us consider a partial function f from $\mathbb{R}$ to the carrier of Y. Now we state the propositions:

(20) Suppose $A \subseteq \operatorname{dom} f$ and $f\restriction A$ is bounded and f is integrable on A and $\|f\|$ is integrable on A. Then $\|\int\limits_{A} f(x)dx\| \leqslant \int\limits_{A} \|f\|(x)dx$.

(21) Suppose $a \leqslant b$ and $[a,b] \subseteq \operatorname{dom} f$ and f is integrable on $[a,b]$ and $\|f\|$ is integrable on $[a,b]$ and $f\restriction[a,b]$ is bounded. Then $\|\int\limits_{a}^{b} f(x)dx\| \leqslant \int\limits_{a}^{b} \|f\|(x)dx$.

Let us consider a continuous partial function f from $\mathbb{R}$ to the carrier of Y. Now we state the propositions:

(22) Suppose $a \leqslant b$ and $[a,b] \subseteq \operatorname{dom} f$ and c, $d \in [a,b]$. Then

(i) $\|f\|$ is integrable on $[\min(c,d), \max(c,d)]$, and

(ii) $\|f\|\restriction[\min(c,d), \max(c,d)]$ is bounded, and

(iii) $\|\int\limits_{c}^{d} f(x)dx\| \leqslant \int\limits_{\min(c,d)}^{\max(c,d)} \|f\|(x)dx$.

(23) If $a \leqslant b$ and $[a,b] \subseteq \operatorname{dom} f$ and c, $d \in [a,b]$, then $\int\limits_{c}^{d} (r \cdot f)(x)dx = r \cdot \int\limits_{c}^{d} f(x)dx$.

(24) Suppose $a \leqslant b$ and $[a,b] \subseteq \operatorname{dom} f$ and c, $d \in [a,b]$. Then $\int\limits_{c}^{d} -f(x)dx = -\int\limits_{c}^{d} f(x)dx$.

(25) Suppose $a \leqslant b$ and $[a,b] \subseteq \operatorname{dom} f$ and c, $d \in [a,b]$ and for every real number x such that $x \in [\min(c,d), \max(c,d)]$ holds $\|f_x\| \leqslant e$. Then $\|\int\limits_{c}^{d} f(x)dx\| \leqslant e \cdot |d-c|$.

Now we state the propositions:

(26) Let us consider a real normed space Y, a non empty closed interval subset A of $\mathbb{R}$, a function f from A into the carrier of Y, and a point E of Y. Suppose $\operatorname{rng} f = \{E\}$. Then

(i) f is integrable, and

(ii) integral $f = \operatorname{vol}(A) \cdot E$.

PROOF: Reconsider $I = \operatorname{vol}(A) \cdot E$ as a point of Y. For every division sequence T of A and for every middle volume sequence S of f and T such that δ_T is convergent and $\lim \delta_T = 0$ holds middle sum(f,S) is convergent and lim middle sum$(f,S) = I$ by [11, (6)], [20, (70)], [11, (7)]. □

(27) Let us consider a partial function f from $\mathbb{R}$ to the carrier of Y and a point E of Y. Suppose

(i) $a \leqslant b$, and

(ii) $[a,b] \subseteq \operatorname{dom} f$, and

(iii) for every real number x such that $x \in [a,b]$ holds $f_x = E$.

Then

(iv) f is integrable on $[a,b]$, and

(v) $\int\limits_{a}^{b} f(x)dx = (b-a) \cdot E$.

The theorem is a consequence of (26). PROOF: Reconsider $A = [a,b]$ as a non empty closed interval subset of $\mathbb{R}$. Reconsider $g = f \restriction A$ as a function from A into the carrier of Y. $\{E\} \subseteq \operatorname{rng} g$ by [19, (4)], [3, (49), (3)]. $\operatorname{rng} g \subseteq \{E\}$ by [5, (3)], [3, (49)]. □

(28) Let us consider a partial function f from $\mathbb{R}$ to the carrier of Y. Suppose

(i) $a \leqslant b$, and

(ii) c, $d \in [a,b]$, and

(iii) $[a,b] \subseteq \operatorname{dom} f$, and

(iv) for every real number x such that $x \in [a,b]$ holds $f_x = E$.

Then $\int\limits_c^d f(x)dx = (d-c) \cdot E$. The theorem is a consequence of (27) and (14).

(29) Let us consider a continuous partial function f from $\mathbb{R}$ to the carrier of Y. Suppose

(i) $a \leqslant b$, and

(ii) $[a,b] \subseteq \operatorname{dom} f$, and

(iii) c, $d \in [a,b]$.

Then $\int\limits_a^d f(x)dx = \int\limits_a^c f(x)dx + \int\limits_c^d f(x)dx$. The theorem is a consequence of (14).

(30) Let us consider continuous partial functions f, g from $\mathbb{R}$ to the carrier of Y. Suppose

(i) $a \leqslant b$, and

(ii) $[a,b] \subseteq \operatorname{dom} f$, and

(iii) $[a,b] \subseteq \operatorname{dom} g$, and

(iv) c, $d \in [a,b]$.

Then $\int\limits_c^d (f-g)(x)dx = \int\limits_c^d f(x)dx - \int\limits_c^d g(x)dx$. The theorem is a consequence of (14).

References

[1] Józef Białas. Properties of the intervals of real numbers. *Formalized Mathematics*, 3(**2**): 263–269, 1992.

[2] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

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

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

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

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

[7] Noboru Endou and Artur Korniłowicz. The definition of the Riemann definite integral and some related lemmas. *Formalized Mathematics*, 8(**1**):93–102, 1999.

[8] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definition of integrability for partial functions from $\mathbb{R}$ to $\mathbb{R}$ and integrability for continuous functions. *Formalized Mathematics*, 9(**2**):281–284, 2001.

[9] Keiichi Miyajima, Takahiro Kato, and Yasunari Shidama. Riemann integral of functions from $\mathbb{R}$ into real normed space. *Formalized Mathematics*, 19(**1**):17–22, 2011. doi:10.2478/v10037-011-0003-8.

[10] Keiichi Miyajima, Artur Korniłowicz, and Yasunari Shidama. Riemann integral of functions from $\mathbb{R}$ into n-dimensional real normed space. *Formalized Mathematics*, 20(**1**):79–86, 2012. doi:10.2478/v10037-012-0011-3.

[11] Keiko Narita, Noboru Endou, and Yasunari Shidama. Riemann integral of functions from $\mathbb{R}$ into real Banach space. *Formalized Mathematics*, 21(**2**):145–152, 2013. doi:10.2478/forma-2013-0016.

[12] Adam Naumowicz. Conjugate sequences, bounded complex sequences and convergent complex sequences. *Formalized Mathematics*, 6(**2**):265–268, 1997.

[13] Hiroyuki Okazaki, Noboru Endou, and Yasunari Shidama. More on continuous functions on normed linear spaces. *Formalized Mathematics*, 19(**1**):45–49, 2011. doi:10.2478/v10037-011-0008-3.

[14] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.

[15] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.

[16] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.

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

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

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

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

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

[22] Hiroshi Yamazaki and Yasunari Shidama. Algebra of vector functions. *Formalized Mathematics*, 3(**2**):171–175, 1992.

Received October 7, 2013

FORMALIZED MATHEMATICS
Vol. 21, No. 3, Pages 193–205, 2013
DOI: 10.2478/forma-2013-0021

VERSITA
degruyter.com/view/j/forma

Object-Free Definition of Categories

Marco Riccardi
Via del Pero 102
54038 Montignoso
Italy

Summary. Category theory was formalized in Mizar with two different approaches [7], [18] that correspond to those most commonly used [16], [5]. Since there is a one-to-one correspondence between objects and identity morphisms, some authors have used an approach that does not refer to objects as elements of the theory, and are usually indicated as object-free category [1] or as arrows-only category [16]. In this article is proposed a new definition of an object-free category, introducing the two properties: left composable and right composable, and a simplification of the notation through a symbol, a binary relation between morphisms, that indicates whether the composition is defined. In the final part we define two functions that allow to switch from the two definitions, with and without objects, and it is shown that their composition produces isomorphic categories.

MSC: 18A05 03B35

Keywords: object-free category; correspondence between different approaches to category

MML identifier: `CAT_6`, version: `8.1.02 5.19.1189`

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

1. Yet Another Definition of Category

We consider category structures which extend 1-sorted structures and are systems

$$\langle \text{a carrier}, \text{a composition} \rangle$$

where the carrier is a set, the composition is a partial function from (the carrier) $\times$ the carrier to the carrier.

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

In this paper $\mathscr{C}$ denotes a category structure.

Let us consider $\mathscr{C}$. The functor Mor $\mathscr{C}$ yielding a set is defined by the term

(Def. 1) The carrier of $\mathscr{C}$.

A morphism of $\mathscr{C}$ is an element of Mor $\mathscr{C}$. In the sequel f, f_1, f_2, f_3 denote morphisms of $\mathscr{C}$.

Let us consider $\mathscr{C}$, f_1, and f_2. We say that f_1 and f_2 are composable if and only if

(Def. 2) $\langle f_1, f_2\rangle \in \mathrm{dom}$ the composition of $\mathscr{C}$.

We introduce $f_1 \triangleright f_2$ as a synonym of f_1 and f_2 are composable.

Assume $f_1 \triangleright f_2$. The functor $f_1 \circ f_2$ yielding a morphism of $\mathscr{C}$ is defined by the term

(Def. 3) (The composition of $\mathscr{C}$)(f_1, f_2).

Let us consider f. We say that f is left identity if and only if

(Def. 4) Let us consider a morphism f_1 of $\mathscr{C}$. If $f \triangleright f_1$, then $f \circ f_1 = f_1$.

We say that f is right identity if and only if

(Def. 5) Let us consider a morphism f_1 of $\mathscr{C}$. If $f_1 \triangleright f$, then $f_1 \circ f = f_1$.

We say that $\mathscr{C}$ has left identities if and only if

(Def. 6) Let us consider a morphism f_1 of $\mathscr{C}$. Suppose $f_1 \in$ the carrier of $\mathscr{C}$. Then there exists a morphism f of $\mathscr{C}$ such that

(i) $f \triangleright f_1$, and

(ii) f is left identity.

We say that $\mathscr{C}$ has right identities if and only if

(Def. 7) Let us consider a morphism f_1 of $\mathscr{C}$. Suppose $f_1 \in$ the carrier of $\mathscr{C}$. Then there exists a morphism f of $\mathscr{C}$ such that

(i) $f_1 \triangleright f$, and

(ii) f is right identity.

We say that $\mathscr{C}$ is left composable if and only if

(Def. 8) Let us consider morphisms f, f_1, f_2 of $\mathscr{C}$. Suppose $f_1 \triangleright f_2$. Then $f_1 \circ f_2 \triangleright f$ if and only if $f_2 \triangleright f$.

We say that $\mathscr{C}$ is right composable if and only if

(Def. 9) Let us consider morphisms f, f_1, f_2 of $\mathscr{C}$. Suppose $f_1 \triangleright f_2$. Then $f \triangleright f_1 \circ f_2$ if and only if $f \triangleright f_1$.

We say that $\mathscr{C}$ is associative if and only if

(Def. 10) Let us consider morphisms f_1, f_2, f_3 of $\mathscr{C}$. Suppose

(i) $f_1 \triangleright f_2$, and

(ii) $f_2 \triangleright f_3$, and

(iii) $f_1 \circ f_2 \triangleright f_3$, and

(iv) $f_1 \triangleright f_2 \circ f_3$.

Then $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$.

We say that $\mathscr{C}$ is composable if and only if

(Def. 11) $\mathscr{C}$ is left and right composable.

We say that $\mathscr{C}$ has identities if and only if

(Def. 12) $\mathscr{C}$ has left and right identities.

Let X be a set and f be a partial function from $X \times X$ to X. Note that the functor $\frown f$ yields a partial function from $X \times X$ to X. Let us consider $\mathscr{C}$. The functor $\mathscr{C}^{\mathrm{op}}$ yielding a strict category structure is defined by the term

(Def. 13) $\langle$the carrier of $\mathscr{C}$, $\frown$the composition of $\mathscr{C}\rangle$.

Now we state the proposition:

(1) If $\mathscr{C}$ is empty, then $f_1 \not\triangleright f_2$.

In this paper g_1, g_2 denote morphisms of $\mathscr{C}^{\mathrm{op}}$.

Now we state the propositions:

(2) If $f_1 = g_1$ and $f_2 = g_2$, then $f_1 \triangleright f_2$ iff $g_2 \triangleright g_1$.

(3) If $f_1 = g_1$ and $f_2 = g_2$ and $f_1 \triangleright f_2$, then $f_1 \circ f_2 = g_2 \circ g_1$.

(4) $\mathscr{C}$ is left composable if and only if $\mathscr{C}^{\mathrm{op}}$ is right composable. The theorem is a consequence of (3). Proof: For every morphisms f, f_1, f_2 of $\mathscr{C}$ such that $f_1 \triangleright f_2$ holds $f_1 \circ f_2 \triangleright f$ iff $f_2 \triangleright f$ by [11, (42)]. □

(5) $\mathscr{C}$ is right composable if and only if $\mathscr{C}^{\mathrm{op}}$ is left composable. The theorem is a consequence of (3). Proof: For every morphisms f, f_1, f_2 of $\mathscr{C}$ such that $f_1 \triangleright f_2$ holds $f \triangleright f_1 \circ f_2$ iff $f \triangleright f_1$ by [11, (42)]. □

(6) $\mathscr{C}$ has left identities if and only if $\mathscr{C}^{\mathrm{op}}$ has right identities. The theorem is a consequence of (3). Proof: For every morphism f_1 of $\mathscr{C}$ such that $f_1 \in$ the carrier of $\mathscr{C}$ there exists a morphism f of $\mathscr{C}$ such that $f \triangleright f_1$ and f is left identity by [11, (42)]. □

(7) $\mathscr{C}$ has right identities if and only if $\mathscr{C}^{\mathrm{op}}$ has left identities. The theorem is a consequence of (3). Proof: For every morphism f_1 of $\mathscr{C}$ such that $f_1 \in$ the carrier of $\mathscr{C}$ there exists a morphism f of $\mathscr{C}$ such that $f_1 \triangleright f$ and f is right identity by [11, (42)]. □

(8) $\mathscr{C}$ is associative if and only if $\mathscr{C}^{\mathrm{op}}$ is associative. The theorem is a consequence of (3). Proof: For every morphisms f_1, f_2, f_3 of $\mathscr{C}$ such that $f_1 \triangleright f_2$ and $f_2 \triangleright f_3$ and $f_1 \circ f_2 \triangleright f_3$ and $f_1 \triangleright f_2 \circ f_3$ holds $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$ by [11, (42)]. □

Note that there exists a category structure which is composable and associative and has left identities and has not right identities and there exists a category structure which is composable and associative and has right identities and has not left identities and there exists a category structure which is non left composable, right composable, and associative and has identities and there exists a category structure which is left composable, non right composable, and associative and has identities and there exists a category structure which is non associative and composable and has identities and there exists a category structure which is empty and every category structure which is empty is also left and right composable and associative and has also left and right identities and there exists a category structure which is strict, left and right composable, and associative and has left and right identities and there exists a category structure which is strict, composable, and associative and has identities.

A category is a composable associative category structure with identities.

Let us consider $\mathscr{C}$ and f. We say that f is identity if and only if

(Def. 14) f is left and right identity.

Now we state the propositions:

(9) If $\mathscr{C}$ has identities, then f is left identity iff f is right identity. Proof: For every morphism f_1 of $\mathscr{C}$ such that $f \triangleright f_1$ holds $f \circ f_1 = f_1$. $\square$

(10) If $\mathscr{C}$ is empty, then f is identity.

(11) Let us consider morphisms g_1, g_2 of the category structure of $\mathscr{C}$. Suppose

(i) $f_1 = g_1$, and

(ii) $f_2 = g_2$, and

(iii) $f_1 \triangleright f_2$.

Then $f_1 \circ f_2 = g_1 \circ g_2$.

(12) $\mathscr{C}$ is left composable if and only if the category structure of $\mathscr{C}$ is left composable. The theorem is a consequence of (11). Proof: For every morphisms f, f_1, f_2 of $\mathscr{C}$ such that $f_1 \triangleright f_2$ holds $f_1 \circ f_2 \triangleright f$ iff $f_2 \triangleright f$. $\square$

(13) $\mathscr{C}$ is right composable if and only if the category structure of $\mathscr{C}$ is right composable. The theorem is a consequence of (11). Proof: For every morphisms f, f_1, f_2 of $\mathscr{C}$ such that $f_1 \triangleright f_2$ holds $f \triangleright f_1 \circ f_2$ iff $f \triangleright f_1$. $\square$

(14) $\mathscr{C}$ is composable if and only if the category structure of $\mathscr{C}$ is composable.

(15) $\mathscr{C}$ is associative if and only if the category structure of $\mathscr{C}$ is associative. The theorem is a consequence of (11). Proof: For every morphisms f_1, f_2, f_3 of $\mathscr{C}$ such that $f_1 \triangleright f_2$ and $f_2 \triangleright f_3$ and $f_1 \circ f_2 \triangleright f_3$ and $f_1 \triangleright f_2 \circ f_3$ holds $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$. $\square$

(16) Let us consider a morphism g of the category structure of $\mathscr{C}$. If $f = g$, then f is left identity iff g is left identity. The theorem is a consequence of (11). Proof: For every morphism f_2 of $\mathscr{C}$ such that $f \triangleright f_2$ holds $f \circ f_2 = f_2$. $\square$

(17) $\mathscr{C}$ has left identities if and only if the category structure of $\mathscr{C}$ has left identities. The theorem is a consequence of (16). Proof: For every morphism f_1 of $\mathscr{C}$ such that $f_1 \in$ the carrier of $\mathscr{C}$ there exists a morphism f of $\mathscr{C}$ such that $f \triangleright f_1$ and f is left identity. $\square$

(18) Let us consider a morphism g of the category structure of $\mathscr{C}$. If $f = g$, then f is right identity iff g is right identity. The theorem is a consequence of (11). Proof: For every morphism f_1 of $\mathscr{C}$ such that $f_1 \triangleright f$ holds $f_1 \circ f = f_1$. $\square$

(19) $\mathscr{C}$ has right identities if and only if the category structure of $\mathscr{C}$ has right identities. The theorem is a consequence of (18). Proof: For every morphism f_1 of $\mathscr{C}$ such that $f_1 \in$ the carrier of $\mathscr{C}$ there exists a morphism f of $\mathscr{C}$ such that $f_1 \triangleright f$ and f is right identity. $\square$

(20) $\mathscr{C}$ has identities if and only if the category structure of $\mathscr{C}$ has identities.

Let us consider $\mathscr{C}$. We say that $\mathscr{C}$ is discrete if and only if

(Def. 15) Every morphism of $\mathscr{C}$ is identity.

One can verify that there exists a category structure which is strict, empty, discrete, composable, and associative and has identities.

Now we state the proposition:

(21) Let us consider a discrete category structure $\mathscr{C}$ and morphisms f_1, f_2 of $\mathscr{C}$. If $f_1 \triangleright f_2$, then $f_1 = f_2$ and $f_1 \circ f_2 = f_2$.

Observe that every category structure which is discrete is also composable and associative.

Let X be a set. The discrete category of X yielding a strict discrete category is defined by

(Def. 16) The carrier of $it = X$.

Note that there exists a category which is strict and there exists a category which is strict and empty and there exists a category which is strict and non empty.

Let us consider $\mathscr{C}$. The functor $\operatorname{Ob}\mathscr{C}$ yielding a subset of $\operatorname{Mor}\mathscr{C}$ is defined by the term

(Def. 17) $\{f$, where f is a morphism of $\mathscr{C} : f$ is identity and $f \in \operatorname{Mor}\mathscr{C}\}$.

An object of $\mathscr{C}$ is an element of $\operatorname{Ob}\mathscr{C}$. Let $\mathscr{C}$ be a non empty category structure with identities. Let us observe that $\operatorname{Ob}\mathscr{C}$ is non empty.

Now we state the propositions:

(22) Let us consider a non empty category structure $\mathscr{C}$ with identities and a morphism f of $\mathscr{C}$. Then f is identity if and only if f is an object of $\mathscr{C}$.

(23) Let us consider a non empty category structure $\mathscr{C}$ with identities, morphisms f, f_1 of $\mathscr{C}$, and an object o of $\mathscr{C}$. Suppose $f = o$. Then

  (i) if $f \triangleright f_1$, then $f \circ f_1 = f_1$, and

  (ii) if $f_1 \triangleright f$, then $f_1 \circ f = f_1$, and

  (iii) $f \triangleright f$.

The theorem is a consequence of (22).

(24) Let us consider a non empty category structure $\mathscr{C}$ with identities and a morphism f of $\mathscr{C}$. If f is identity, then $f \triangleright f$. The theorem is a consequence of (22) and (23).

(25) Let us consider category structures $\mathscr{C}_1$, $\mathscr{C}_2$ with identities.
Suppose the category structure of $\mathscr{C}_1$ = the category structure of $\mathscr{C}_2$. Let us consider a morphism f_1 of $\mathscr{C}_1$ and a morphism f_2 of $\mathscr{C}_2$. If $f_1 = f_2$, then f_1 is identity iff f_2 is identity. PROOF: For every morphism f of $\mathscr{C}_1$ such that $f_1 \triangleright f$ holds $f_1 \circ f = f$. For every morphism f of $\mathscr{C}_1$ such that $f \triangleright f_1$ holds $f \circ f_1 = f$. □

Let $\mathscr{C}$ be a composable category structure with identities and f be a morphism of $\mathscr{C}$. The functor dom f yielding an object of $\mathscr{C}$ is defined by

(Def. 18) (i) there exists a morphism f_1 of $\mathscr{C}$ such that $it = f_1$ and $f \triangleright f_1$ and f_1 is identity, **if** $\mathscr{C}$ is not empty,

(ii) it = the object of $\mathscr{C}$, **otherwise**.

The functor cod f yielding an object of $\mathscr{C}$ is defined by

(Def. 19) (i) there exists a morphism f_1 of $\mathscr{C}$ such that $it = f_1$ and $f_1 \triangleright f$ and f_1 is identity, **if** $\mathscr{C}$ is not empty,

(ii) it = the object of $\mathscr{C}$, **otherwise**.

Let us consider a composable category structure $\mathscr{C}$ with identities and morphisms f, f_1 of $\mathscr{C}$. Now we state the propositions:

(26) If $f \triangleright f_1$ and f_1 is identity, then dom $f = f_1$.

(27) If $f_1 \triangleright f$ and f_1 is identity, then cod $f = f_1$.

Let $\mathscr{C}$ be category structure with identities and o be an object of $\mathscr{C}$. The functor id-o yielding a morphism of $\mathscr{C}$ is defined by the term

(Def. 20) o.

Let $\mathscr{C}$, $\mathscr{D}$ be category structures. A functor from $\mathscr{C}$ to $\mathscr{D}$ is a function from $\mathscr{C}$ into $\mathscr{D}$. In the sequel $\mathscr{C}$, $\mathscr{D}$, $\mathscr{E}$ denote category structures with identities, $\mathcal{F}$ denotes a functor from $\mathscr{C}$ to $\mathscr{D}$, $\mathcal{G}$ denotes a functor from $\mathscr{D}$ to $\mathscr{E}$, and f denotes a morphism of $\mathscr{C}$.

Let us consider $\mathscr{C}$, $\mathscr{D}$, $\mathcal{F}$, and f. The functor $\mathcal{F}(f)$ yielding a morphism of $\mathscr{D}$ is defined by the term

(Def. 21) $\begin{cases} \mathcal{F}(f), & \textbf{if } \mathscr{C} \text{ is not empty ,} \\ \text{The object of } \mathscr{D}, & \textbf{otherwise}. \end{cases}$

We say that $\mathcal{F}$ preserves identity if and only if

(Def. 22) Let us consider a morphism f of $\mathscr{C}$. If f is identity, then $\mathcal{F}(f)$ is identity.

We say that $\mathcal{F}$ is multiplicative if and only if

(Def. 23) Let us consider morphisms f_1, f_2 of $\mathscr{C}$. Suppose $f_1 \triangleright f_2$. Then

(i) $\mathcal{F}(f_1) \triangleright \mathcal{F}(f_2)$, and

(ii) $\mathcal{F}(f_1 \circ f_2) = \mathcal{F}(f_1) \circ \mathcal{F}(f_2)$.

We say that $\mathcal{F}$ is anti-multiplicative if and only if

(Def. 24) Let us consider morphisms f_1, f_2 of $\mathscr{C}$. Suppose $f_1 \triangleright f_2$. Then

(i) $\mathcal{F}(f_2) \triangleright \mathcal{F}(f_1)$, and

(ii) $\mathcal{F}(f_1 \circ f_2) = \mathcal{F}(f_2) \circ \mathcal{F}(f_1)$.

Note that there exists a functor from $\mathscr{C}$ to $\mathscr{D}$ which preserves identity.

Let $\mathscr{C}$ be an empty category structure with identities and $\mathscr{D}$ be category structure with identities. Note that there exists a functor from $\mathscr{C}$ to $\mathscr{D}$ which is multiplicative and anti-multiplicative preserves identity.

Let $\mathscr{C}$ be category structure with identities and $\mathscr{D}$ be a non empty category structure with identities. Let us observe that there exists a functor from $\mathscr{C}$ to $\mathscr{D}$ which is multiplicative and anti-multiplicative preserves identity.

Now we state the propositions:

(28) There exist categories $\mathscr{C}$, $\mathscr{D}$ and there exists a functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$ such that $\mathcal{F}$ is multiplicative and $\mathcal{F}$ does not preserve identity. The theorem is a consequence of (22). PROOF: Set $\mathscr{C}$ = the non empty category. Reconsider $X = \{0, 1\}$ as a set. Set $c_4 = \{\langle\langle 0, 0\rangle, 0\rangle, \langle\langle 1, 1\rangle, 1\rangle\} \cup \{\langle\langle 0, 1\rangle, 1\rangle, \langle\langle 1, 0\rangle, 1\rangle\}$. For every element x, $x \in c_4$ iff $x = \langle\langle 0, 0\rangle, 0\rangle$ or $x = \langle\langle 1, 1\rangle, 1\rangle$ or $x = \langle\langle 0, 1\rangle, 1\rangle$ or $x = \langle\langle 1, 0\rangle, 1\rangle$. For every elements x, y_1, y_2 such that $\langle x, y_1\rangle$, $\langle x, y_2\rangle \in c_4$ holds $y_1 = y_2$. For every element x such that $x \in c_4$ holds $x \in (X \times X) \times X$. Set $\mathscr{D} = \langle X, c_4\rangle$. For every morphisms f_1, f_2 of $\mathscr{D}$ such that $f_1 \triangleright f_2$ holds $f_1 = 0$ and $f_2 = 0$ and $f_1 \circ f_2 = 0$ or $f_1 = 1$ and $f_2 = 1$ and $f_1 \circ f_2 = 1$ or $f_1 = 0$ and $f_2 = 1$ and $f_1 \circ f_2 = 1$ or $f_1 = 1$ and $f_2 = 0$ and $f_1 \circ f_2 = 1$ by [9, (1)]. For every morphisms f_1, f_2 of $\mathscr{D}$, $f_1 \triangleright f_2$ by [9, (1)]. For every morphism f_1 of $\mathscr{D}$ such that $f_1 \in$ the carrier of $\mathscr{D}$ there exists a morphism f of $\mathscr{D}$ such that $f \triangleright f_1$ and f is left identity. For every morphism f_1 of $\mathscr{D}$ such that $f_1 \in$ the carrier of $\mathscr{D}$ there exists a morphism f of $\mathscr{D}$ such that $f_1 \triangleright f$ and f is right identity. For every morphisms f_1, f_2, f_3 of $\mathscr{D}$ such that $f_1 \triangleright f_2$ and $f_2 \triangleright f_3$ and $f_1 \circ f_2 \triangleright f_3$ and $f_1 \triangleright f_2 \circ f_3$ holds $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$. Reconsider $d_1 = 1$ as a morphism of $\mathscr{D}$. Define $\mathcal{H}(\text{element}) = d_1$. Consider $\mathcal{F}$ being a function from the carrier of $\mathscr{C}$ into the carrier of $\mathscr{D}$ such that for every element x such that $x \in$ the carrier of $\mathscr{C}$ holds $\mathcal{F}(x) = \mathcal{H}(x)$ from [10, Sch. 2]. For every morphisms f_1, f_2 of $\mathscr{C}$ such that $f_1 \triangleright f_2$ holds $\mathcal{F}(f_1) \triangleright \mathcal{F}(f_2)$ and $\mathcal{F}(f_1 \circ f_2) = \mathcal{F}(f_1) \circ \mathcal{F}(f_2)$. There exists a morphism f of $\mathscr{C}$ such that f is identity and $\mathcal{F}(f)$ is not identity. □

(29) Suppose $\mathscr{C}$ is not empty and $\mathscr{D}$ is empty. Then there exists no a functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$ such that $\mathcal{F}$ is multiplicative or $\mathcal{F}$ is anti-multiplicative. The theorem is a consequence of (23).

(30) There exist categories $\mathscr{C}$, $\mathscr{D}$ and there exists a functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$ such that $\mathcal{F}$ is not multiplicative and $\mathcal{F}$ preserves identity. The theorem is a consequence of (29).

Let us consider $\mathscr{C}$, $\mathscr{D}$, and $\mathcal{F}$. We say that $\mathcal{F}$ is covariant if and only if

(Def. 25) (i) $\mathcal{F}$ preserves identity, and

(ii) $\mathcal{F}$ is multiplicative.

We say that $\mathcal{F}$ is contravariant if and only if

(Def. 26) (i) $\mathcal{F}$ preserves identity, and

(ii) $\mathcal{F}$ is anti-multiplicative.

Let $\mathscr{C}$ be an empty category structure with identities and $\mathscr{D}$ be category structure with identities. One can check that there exists a functor from $\mathscr{C}$ to $\mathscr{D}$ which is covariant and contravariant.

Let $\mathscr{C}$ be category structure with identities and $\mathscr{D}$ be a non empty category structure with identities. Observe that there exists a functor from $\mathscr{C}$ to $\mathscr{D}$ which is covariant and contravariant.

Now we state the proposition:

(31) Suppose $\mathscr{C}$ is not empty and $\mathscr{D}$ is empty. Then there exists no a functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$ such that $\mathcal{F}$ is covariant or $\mathcal{F}$ is contravariant.

Let $\mathscr{C}$, $\mathscr{D}$ be non empty category structures with identities, $\mathcal{F}$ be a covariant functor from $\mathscr{C}$ to $\mathscr{D}$, and f be an object of $\mathscr{C}$. Observe that the functor $\mathcal{F}(f)$ yields an object of $\mathscr{D}$. Now we state the propositions:

(32) Let us consider non empty composable category structures $\mathscr{C}$, $\mathscr{D}$ with identities, a covariant functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$, and a morphism f of $\mathscr{C}$. Then

(i) $\mathcal{F}(\operatorname{dom} f) = \operatorname{dom}(\mathcal{F}(f))$, and

(ii) $\mathcal{F}(\operatorname{cod} f) = \operatorname{cod}(\mathcal{F}(f))$.

The theorem is a consequence of (22).

(33) Let us consider non empty composable category structures $\mathscr{C}$, $\mathscr{D}$ with identities, a covariant functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$, and an object o of $\mathscr{C}$. Then $\mathcal{F}(\text{id-}o) = \text{id-}(\mathcal{F}(o))$.

Let us consider $\mathscr{C}$, $\mathscr{D}$, $\mathscr{E}$, $\mathcal{F}$, and $\mathcal{G}$. Assume $\mathcal{F}$ is covariant or $\mathcal{F}$ is contravariant and $\mathcal{G}$ is covariant or $\mathcal{G}$ is contravariant. The functor $\mathcal{G} \circ \mathcal{F}$ yielding a functor from $\mathscr{C}$ to $\mathscr{E}$ is defined by the term

(Def. 27) $\mathcal{F} \cdot \mathcal{G}$.

Now we state the propositions:

(34) Suppose $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant and $\mathscr{C}$ is not empty. Then $(\mathcal{G} \circ \mathcal{F})(f) = \mathcal{G}(\mathcal{F}(f))$. The theorem is a consequence of (29).

(35) If $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant, then $\mathcal{G} \circ \mathcal{F}$ is covariant. The theorem is a consequence of (34), (22), and (10). Proof: Set $\mathcal{G}_1 = \mathcal{G} \circ \mathcal{F}$. For every morphism f of $\mathscr{C}$ such that f is identity holds $\mathcal{G}_1(f)$ is identity. For every morphisms f_1, f_2 of $\mathscr{C}$ such that $f_1 \triangleright f_2$ holds $\mathcal{G}_1(f_1) \triangleright \mathcal{G}_1(f_2)$ and $\mathcal{G}_1(f_1 \circ f_2) = \mathcal{G}_1(f_1) \circ \mathcal{G}_1(f_2)$. $\square$

Let us consider $\mathscr{C}$. Note that the functor $\mathrm{id}_{\mathscr{C}}$ yields a functor from $\mathscr{C}$ to $\mathscr{C}$. Let us observe that $\mathrm{id}_{\mathscr{C}}$ is covariant.

Let us consider $\mathscr{D}$. We say that $\mathscr{C}$ and $\mathscr{D}$ are isomorphic if and only if

(Def. 28) There exists a functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$ and there exists a functor $\mathcal{G}$ from $\mathscr{D}$ to $\mathscr{C}$ such that $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant and $\mathcal{G} \circ \mathcal{F} = \mathrm{id}_{\mathscr{C}}$ and $\mathcal{F} \circ \mathcal{G} = \mathrm{id}_{\mathscr{D}}$.

Note that the predicate is reflexive and symmetric.

We introduce $\mathscr{C} \cong \mathscr{D}$ as a synonym of $\mathscr{C}$ and $\mathscr{D}$ are isomorphic.

2. Transform a Category in the Other

Let $\mathscr{C}$ be a category structure. The functor CompMap $\mathscr{C}$ yielding a partial function from Mor $\mathscr{C} \times$ Mor $\mathscr{C}$ to Mor $\mathscr{C}$ is defined by the term

(Def. 29) The composition of $\mathscr{C}$.

Let $\mathscr{C}$ be a composable category structure with identities. The functors: SourceMap $\mathscr{C}$ and TargetMap $\mathscr{C}$ yielding functions from Mor $\mathscr{C}$ into Ob $\mathscr{C}$ are defined by conditions, respectively.

(Def. 30) (i) for every element f of Mor $\mathscr{C}$, (SourceMap $\mathscr{C}$)$(f) = \mathrm{dom}\, f$, **if** $\mathscr{C}$ is not empty,

(ii) SourceMap $\mathscr{C} = \emptyset$, **otherwise**.

(Def. 31) (i) for every element f of Mor $\mathscr{C}$, (TargetMap $\mathscr{C}$)$(f) = \mathrm{cod}\, f$, **if** $\mathscr{C}$ is not empty,

(ii) TargetMap $\mathscr{C} = \emptyset$, **otherwise**.

Let $\mathscr{C}$ be category structure with identities. The functor IdMap $\mathscr{C}$ yielding a function from Ob $\mathscr{C}$ into Mor $\mathscr{C}$ is defined by

(Def. 32) (i) for every element o of Ob $\mathscr{C}$, $it(o) = \text{id-}o$, **if** $\mathscr{C}$ is not empty,

(ii) $it = \emptyset$, **otherwise**.

Now we state the propositions:

(36) Let us consider a non empty composable category structure $\mathscr{C}$ with identities and elements f, g of Mor $\mathscr{C}$. Then $\langle g, f \rangle \in \mathrm{dom}$ CompMap $\mathscr{C}$ if and only if (SourceMap $\mathscr{C}$)$(g) =$ (TargetMap $\mathscr{C}$)(f).

(37) Let us consider a composable category structure $\mathscr{C}$ with identities and elements f, g of Mor $\mathscr{C}$. Suppose (SourceMap $\mathscr{C}$)$(g) =$ (TargetMap $\mathscr{C}$)(f). Then

(i) (SourceMap $\mathscr{C}$)((CompMap $\mathscr{C}$)(g, f)) $=$ (SourceMap $\mathscr{C}$)(f), and

(ii) (TargetMap $\mathscr{C}$)((CompMap $\mathscr{C}$)(g, f)) $=$ (TargetMap $\mathscr{C}$)(g).

The theorem is a consequence of (36).

(38) Let us consider a composable associative category structure $\mathscr{C}$ with identities and elements f, g, h of Mor $\mathscr{C}$. Suppose

(i) (SourceMap $\mathscr{C}$)(h) = (TargetMap $\mathscr{C}$)(g), and

(ii) (SourceMap $\mathscr{C}$)(g) = (TargetMap $\mathscr{C}$)(f).

Then (CompMap $\mathscr{C}$)$(h$, (CompMap $\mathscr{C}$)$(g, f))$ = (CompMap $\mathscr{C}$)((CompMap $\mathscr{C}$)$(h, g), f)$. The theorem is a consequence of (36).

(39) Let us consider a composable category structure $\mathscr{C}$ with identities and an element b of Ob $\mathscr{C}$. Then

(i) (SourceMap $\mathscr{C}$)(IdMap $\mathscr{C}(b)$) = b, and

(ii) (TargetMap $\mathscr{C}$)(IdMap $\mathscr{C}(b)$) = b, and

(iii) for every element f of Mor $\mathscr{C}$ such that (TargetMap $\mathscr{C}$)$(f) = b$ holds (CompMap $\mathscr{C}$)(IdMap $\mathscr{C}(b), f) = f$, and

(iv) for every element g of Mor $\mathscr{C}$ such that (SourceMap $\mathscr{C}$)$(g) = b$ holds (CompMap $\mathscr{C}$)$(g$, IdMap $\mathscr{C}(b)) = g$.

The theorem is a consequence of (22) and (36).

A category defined in [7], to avoid confusion, is called an object-category.

Let $\mathscr{C}$ be a non empty category. The functor Alter($\mathscr{C}$) yielding a strict object-category is defined by the term

(Def. 33) $\langle$ Ob $\mathscr{C}$, Mor $\mathscr{C}$, SourceMap $\mathscr{C}$, TargetMap $\mathscr{C}$, CompMap $\mathscr{C}\rangle$.

Let $\mathscr{A}$ be an object-category. The functor alter $\mathscr{A}$ yielding a strict category is defined by the term

(Def. 34) $\langle$the carrier' of $\mathscr{A}$, (the composition of $\mathscr{A}$)$\rangle$.

Observe that alter $\mathscr{A}$ is non empty.

Now we state the propositions:

(40) Let us consider an object-category $\mathscr{A}$, morphisms a_1, a_2 of $\mathscr{A}$, and morphisms f_1, f_2 of alter $\mathscr{A}$. Suppose

(i) $a_1 = f_1$, and

(ii) $a_2 = f_2$, and

(iii) $\langle a_1, a_2\rangle \in$ dom the composition of $\mathscr{A}$.

Then $a_1 \circ a_2 = f_1 \circ f_2$.

(41) Let us consider an object-category $\mathscr{A}$ and a morphism f of alter $\mathscr{A}$. Then f is identity if and only if there exists an object o of $\mathscr{A}$ such that $f = \mathrm{id}_o$. The theorem is a consequence of (22), (23), and (40). Proof: For every morphism f_1 of alter $\mathscr{A}$ such that $f \triangleright f_1$ holds $f \circ f_1 = f_1$ by [7, (15), (21)]. For every morphism f_1 of alter $\mathscr{A}$ such that $f_1 \triangleright f$ holds $f_1 \circ f = f_1$ by [7, (15), (22)]. $\square$

(42) Let us consider object-categories $\mathscr{A}$, $\mathscr{B}$. Then every functor from $\mathscr{A}$ to $\mathscr{B}$ is a covariant functor from alter $\mathscr{A}$ to alter $\mathscr{B}$. The theorem is a consequence of (40) and (41). Proof: Reconsider $\mathcal{H} = \mathcal{F}$ as a function from alter $\mathscr{A}$ into alter $\mathscr{B}$. For every morphisms f_1, f_2 of alter $\mathscr{A}$ such that $f_1 \triangleright f_2$ holds $\mathcal{H}(f_1) \triangleright \mathcal{H}(f_2)$ and $\mathcal{H}(f_1 \circ f_2) = \mathcal{H}(f_1) \circ \mathcal{H}(f_2)$ by [7, (15), (72), (64)]. For every morphism f of alter $\mathscr{A}$ such that f is identity holds $\mathcal{H}(f)$ is identity by [7, (62)]. □

(43) Let us consider a non empty category $\mathscr{C}$, morphisms a_1, a_2 of Alter($\mathscr{C}$), and morphisms f_1, f_2 of $\mathscr{C}$. Suppose

(i) $a_1 = f_1$, and

(ii) $a_2 = f_2$, and

(iii) $f_1 \triangleright f_2$.

Then $a_1 \circ a_2 = f_1 \circ f_2$.

(44) Let us consider a non empty category $\mathscr{C}$, a morphism f_1 of $\mathscr{C}$, and a morphism a_1 of Alter($\mathscr{C}$). Suppose $a_1 = f_1$. Then

(i) $\operatorname{dom} f_1 = \operatorname{dom} a_1$, and

(ii) $\operatorname{cod} f_1 = \operatorname{cod} a_1$.

(45) Let us consider a non empty category $\mathscr{C}$, an object o_1 of $\mathscr{C}$, and an object o_2 of Alter($\mathscr{C}$). If $o_1 = o_2$, then id-$o_1 = \mathrm{id}_{o_2}$. The theorem is a consequence of (22), (24), (44), and (43). Proof: Reconsider $a_2 = o_2$ as a morphism of Alter($\mathscr{C}$). Reconsider $a_3 = a_2$ as a morphism from o_2 to o_2. For every object b of Alter($\mathscr{C}$), if $\hom(o_2, b) \neq \emptyset$, then for every morphism a from o_2 to b, $a \circ a_3 = a$ and if $\hom(b, o_2) \neq \emptyset$, then for every morphism a from b to o_2, $a_3 \circ a = a$ by [7, (5), (15)]. □

(46) Let us consider a non empty category $\mathscr{C}$ and a morphism f of $\mathscr{C}$. Then f is identity if and only if there exists an object o of Alter($\mathscr{C}$) such that $f = \mathrm{id}_o$. The theorem is a consequence of (25) and (41).

(47) Let us consider non empty categories $\mathscr{C}$, $\mathscr{D}$. Then every covariant functor from $\mathscr{C}$ to $\mathscr{D}$ is a functor from Alter($\mathscr{C}$) to Alter($\mathscr{D}$). The theorem is a consequence of (46), (44), (32), and (45). Proof: Reconsider $\mathcal{H} = \mathcal{F}$ as a function from the carrier' of Alter($\mathscr{C}$) into the carrier' of Alter($\mathscr{D}$). For every object a of Alter($\mathscr{C}$), there exists an object b of Alter($\mathscr{D}$) such that $\mathcal{H}(\mathrm{id}_a) = \mathrm{id}_b$. For every morphism f of Alter($\mathscr{C}$), $\mathcal{H}(\mathrm{id}_{\operatorname{dom} f}) = \mathrm{id}_{\operatorname{dom}(\mathcal{H}(f))}$ and $\mathcal{H}(\mathrm{id}_{\operatorname{cod} f}) = \mathrm{id}_{\operatorname{cod}(\mathcal{H}(f))}$. For every morphisms f, g of Alter($\mathscr{C}$) such that $\operatorname{dom} g = \operatorname{cod} f$ holds $\mathcal{H}(g \circ f) = \mathcal{H}(g) \circ \mathcal{H}(f)$ by [7, (15), (16)]. □

(48) Let us consider object-categories $\mathscr{C}$, $\mathscr{D}$. Then every covariant functor from alter $\mathscr{C}$ to alter $\mathscr{D}$ is a functor from $\mathscr{C}$ to $\mathscr{D}$. The theorem is a consequence of (41), (26), and (27). Proof: Reconsider $\mathcal{H} = \mathcal{F}$ as a function from the carrier' of $\mathscr{C}$ into the carrier' of $\mathscr{D}$. For every object a of $\mathscr{C}$, there

exists an object b of $\mathscr{D}$ such that $\mathcal{H}(\mathrm{id}_a) = \mathrm{id}_b$. For every morphism f of $\mathscr{C}$, $\mathcal{H}(\mathrm{id}_{\mathrm{dom}\, f}) = \mathrm{id}_{\mathrm{dom}(\mathcal{H}(f))}$ and $\mathcal{H}(\mathrm{id}_{\mathrm{cod}\, f}) = \mathrm{id}_{\mathrm{cod}(\mathcal{H}(f))}$ by [7, (15)]. For every morphisms f, g of $\mathscr{C}$ such that $\mathrm{dom}\, g = \mathrm{cod}\, f$ holds $\mathcal{H}(g \circ f) = \mathcal{H}(g) \circ \mathcal{H}(f)$ by [7, (15), (16)]. □

Let us consider object-categories $\mathscr{C}_1$, $\mathscr{C}_2$. Now we state the propositions:

(49) If alter $\mathscr{C}_1 \cong$ alter $\mathscr{C}_2$, then $\mathscr{C}_1 \cong \mathscr{C}_2$.

(50) Suppose the carrier' of $\mathscr{C}_1 =$ the carrier' of $\mathscr{C}_2$ and the composition of $\mathscr{C}_1 =$ the composition of $\mathscr{C}_2$. Then $\mathscr{C}_1 \cong \mathscr{C}_2$.

Now we state the propositions:

(51) Let us consider an object-category $\mathscr{C}$. Then $\mathscr{C} \cong \mathrm{Alter}(\mathrm{alter}\, \mathscr{C})$.

(52) Let us consider a non empty category $\mathscr{C}$. Then $\mathscr{C} \cong \mathrm{alter}\, \mathrm{Alter}(\mathscr{C})$. The theorem is a consequence of (16) and (18). PROOF: Set $\mathscr{D} = \mathrm{alter}\, \mathrm{Alter}(\mathscr{C})$. Reconsider $\mathcal{F} = \mathrm{id}_{\mathscr{C}}$ as a functor from $\mathscr{C}$ to $\mathscr{D}$. Reconsider $\mathcal{G} = \mathrm{id}_{\mathscr{C}}$ as a functor from $\mathscr{D}$ to $\mathscr{C}$. For every morphism f of $\mathscr{C}$ such that f is identity holds $\mathcal{F}(f)$ is identity. For every morphisms f_1, f_2 of $\mathscr{C}$ such that $f_1 \triangleright f_2$ holds $\mathcal{F}(f_1) \triangleright \mathcal{F}(f_2)$ and $\mathcal{F}(f_1 \circ f_2) = \mathcal{F}(f_1) \circ \mathcal{F}(f_2)$. For every morphism f of $\mathscr{D}$ such that f is identity holds $\mathcal{G}(f)$ is identity. For every morphisms f_1, f_2 of $\mathscr{D}$ such that $f_1 \triangleright f_2$ holds $\mathcal{G}(f_1) \triangleright \mathcal{G}(f_2)$ and $\mathcal{G}(f_1 \circ f_2) = \mathcal{G}(f_1) \circ \mathcal{G}(f_2)$. □

References

[1] Jiri Adamek, Horst Herrlich, and George E. Strecker. *Abstract and Concrete Categories: The Joy of Cats*. Dover Publication, New York, 2009.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 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] Francis Borceaux. *Handbook of Categorical Algebra I. Basic Category Theory*, volume 50 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1994.

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

[7] Czesław Byliński. Introduction to categories and functors. *Formalized Mathematics*, 1 (**2**):409–420, 1990.

[8] Czesław Byliński. Subcategories and products of categories. *Formalized Mathematics*, 1 (**4**):725–732, 1990.

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

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

[11] 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.

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

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

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

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

[16] Saunders Mac Lane. *Categories for the Working Mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer Verlag, New York, Heidelberg, Berlin, 1971.

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

[18] Andrzej Trybulec. Categories without uniqueness of **cod** and **dom**. *Formalized Mathematics*, 5(**2**):259–267, 1996.

[19] Andrzej Trybulec. Isomorphisms of categories. *Formalized Mathematics*, 2(**5**):629–634, 1991.

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

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

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

Received October 7, 2013

FORMALIZED MATHEMATICS
Vol. 21, No. 3, Pages 207–211, 2013
DOI: 10.2478/forma-2013-0022

VERSITA
degruyter.com/view/j/forma

Isomorphisms of Direct Products of Cyclic Groups of Prime Power Order

Hiroshi Yamazaki
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Kazuhisa Nakasho
Shinshu University
Nagano, Japan

Yasunari Shidama[1]
Shinshu University
Nagano, Japan

Summary. In this paper we formalized some theorems concerning the cyclic groups of prime power order. We formalize that every commutative cyclic group of prime power order is isomorphic to a direct product of family of cyclic groups [1], [18].

MSC: 13D99 06A75 03B35

Keywords: formalization of the commutative cyclic group; prime power set

MML identifier: GROUP_18, version: 8.1.02 5.19.1189

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

1. Basic Properties of Cyclic Groups of Prime Power Order

Let G be a finite group. The functor $\mathrm{Ordset}(G)$ yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 1) the set of all $\mathrm{ord}(a)$ where a is an element of G.

One can check that $\mathrm{Ordset}(G)$ is finite and non empty.

Now we state the propositions:

(1) Let us consider a finite group G. Then there exists an element g of G such that $\mathrm{ord}(g) = \sup \mathrm{Ordset}(G)$.

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

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

(2) Let us consider a strict group G and a strict normal subgroup N of G. If G is commutative, then ${}^{G}/_{N}$ is commutative.

(3) Let us consider a finite group G and elements a, b of G. Then $b \in \mathrm{gr}(\{a\})$ if and only if there exists an element p of $\mathbb{N}$ such that $b = a^p$.

(4) Let us consider a finite group G, an element a of G, and elements n, p, s of $\mathbb{N}$. Suppose

(i) $\overline{\overline{\mathrm{gr}(\{a\})}} = n$, and

(ii) $n = p \cdot s$.

Then $\mathrm{ord}(a^p) = s$.

Let us consider an element k of $\mathbb{N}$, a finite group G, and an element a of G. Now we state the propositions:

(5) $\mathrm{gr}(\{a\}) = \mathrm{gr}(\{a^k\})$ if and only if $\gcd(k, \mathrm{ord}(a)) = 1$.

(6) If $\gcd(k, \mathrm{ord}(a)) = 1$, then $\mathrm{ord}(a) = \mathrm{ord}(a^k)$.

(7) $\mathrm{ord}(a) \mid k \cdot \mathrm{ord}(a^k)$.

Now we state the proposition:

(8) Let us consider a group G and elements a, b of G. Suppose $b \in \mathrm{gr}(\{a\})$. Then $\mathrm{gr}(\{b\})$ is a strict subgroup of $\mathrm{gr}(\{a\})$.

Let G be a strict commutative group and x be an element of $\mathrm{SubGr}\, G$. The functor $\mathrm{NormSp}_{\mathbb{R}}(x)$ yielding a normal strict subgroup of G is defined by the term

(Def. 2) x.

Now we state the propositions:

(9) Let us consider groups G, H, a subgroup K of H, and a homomorphism f from G to H. Then there exists a strict subgroup J of G such that the carrier of $J = f^{-1}$(the carrier of K). PROOF: Reconsider $I_3 = f^{-1}$(the carrier of K) as a non empty subset of the carrier of G. For every elements g_1, g_2 of G such that g_1, $g_2 \in I_3$ holds $g_1 \cdot g_2 \in I_3$ by [8, (38)], [25, (50)]. For every element g of G such that $g \in I_3$ holds $g^{-1} \in I_3$ by [8, (38)], [25, (51)], [28, (32)]. Consider J being a strict subgroup of G such that the carrier of $J = f^{-1}$(the carrier of K). □

(10) Let us consider a natural number p, a finite group G, and elements x, d of G. Suppose

(i) $\mathrm{ord}(d) = p$, and

(ii) p is prime, and

(iii) $x \in \mathrm{gr}(\{d\})$.

Then

(iv) $x = \mathbf{1}_G$, or

(v) $\mathrm{gr}(\{x\}) = \mathrm{gr}(\{d\})$.

The theorem is a consequence of (8). Proof: If $\mathrm{gr}(\{x\}) = \{\mathbf{1}\}_{\mathrm{gr}(\{d\})}$, then $x = \mathbf{1}_G$ by [19, (2)], [25, (44)]. $\square$

(11) Let us consider a group G and normal subgroups H, K of G. Suppose (the carrier of H) $\cap$ (the carrier of K) $= \{\mathbf{1}_G\}$. Then (the canonical homomorphism onto cosets of H)$\restriction$(the carrier of K) is one-to-one. Proof: Set $f =$ the canonical homomorphism onto cosets of H. Set $g = f\restriction$the carrier of K. For every elements x_1, x_2 such that x_1, $x_2 \in \mathrm{dom}\, g$ and $g(x_1) = g(x_2)$ holds $x_1 = x_2$ by [30, (57)], [7, (49)], [25, (46), (103), (51)]. $\square$

Let us consider finite commutative groups G, F, an element a of G, and a homomorphism f from G to F. Now we state the propositions:

(12) The carrier of $\mathrm{gr}(\{f(a)\}) = f^{\circ}$the carrier of $\mathrm{gr}(\{a\})$.

(13) $\mathrm{ord}(f(a)) \leqslant \mathrm{ord}(a)$.

(14) If f is one-to-one, then $\mathrm{ord}(f(a)) = \mathrm{ord}(a)$.

Now we state the propositions:

(15) Let us consider groups G, F, a subgroup H of G, and a homomorphism f from G to F. Then $f\restriction$the carrier of H is a homomorphism from H to F. Proof: Reconsider $g = f\restriction$the carrier of H as a function from the carrier of H into the carrier of F. For every elements a, b of H, $g(a \cdot b) = g(a) \cdot g(b)$ by [25, (40)], [7, (49)], [25, (43)]. $\square$

(16) Let us consider finite commutative groups G, F, an element a of G, and a homomorphism f from G to F. Suppose $f\restriction$the carrier of $\mathrm{gr}(\{a\})$ is one-to-one. Then $\mathrm{ord}(f(a)) = \mathrm{ord}(a)$. The theorem is a consequence of (15) and (14).

(17) Let us consider a finite commutative group G, a prime number p, a natural number m, and an element a of G. Suppose

(i) $\overline{\overline{G}} = p^m$, and

(ii) $a \neq \mathbf{1}_G$.

Then there exists a natural number n such that $\mathrm{ord}(a) = p^{n+1}$.

(18) Let us consider a prime number p and natural numbers j, m, k. If $m = p^k$ and $p \nmid j$, then $\gcd(j, m) = 1$.

2. Isomorphism of Cyclic Groups of Prime Power Order

Let us consider a strict finite commutative group G, a prime number p, and a natural number m. Now we state the propositions:

(19) Suppose $\overline{\overline{G}} = p^m$. Then there exists a normal strict subgroup K of G and there exist natural numbers n, k and there exists an element g of G such that $\mathrm{ord}(g) = \sup \mathrm{Ordset}(G)$ and K is finite and commutative and

(the carrier of K) $\cap$ (the carrier of $\operatorname{gr}(\{g\})) = \{\mathbf{1}_G\}$ and for every element x of G, there exist elements b_1, a_1 of G such that $b_1 \in K$ and $a_1 \in \operatorname{gr}(\{g\})$ and $x = b_1 \cdot a_1$ and $\operatorname{ord}(g) = p^n$ and $k = m - n$ and $n \leqslant m$ and $\overline{\overline{K}} = p^k$ and there exists a homomorphism F from $\prod\langle K, \operatorname{gr}(\{g\})\rangle$ to G such that F is bijective and for every elements a, b of G such that $a \in K$ and $b \in \operatorname{gr}(\{g\})$ holds $F(\langle a, b\rangle) = a \cdot b$.

(20) Suppose $\overline{\overline{G}} = p^m$. Then there exists a non zero natural number k and there exists a k-element finite sequence a of elements of G and there exists a k-element finite sequence I_2 of elements of $\mathbb{N}$ and there exists an associative group-like commutative multiplicative magma family F of $\operatorname{Seg} k$ and there exists a homomorphism H_1 from $\prod F$ to G such that for every natural number i such that $i \in \operatorname{Seg} k$ there exists an element a_2 of G such that $a_2 = a(i)$ and $F(i) = \operatorname{gr}(\{a_2\})$ and $\operatorname{ord}(a_2) = p^{I_2(i)}$ and for every natural number i such that $1 \leqslant i \leqslant k-1$ holds $I_2(i) \leqslant I_2(i+1)$ and for every elements p, q of $\operatorname{Seg} k$ such that $p \neq q$ holds (the carrier of $F(p)$) $\cap$ (the carrier of $F(q)) = \{\mathbf{1}_G\}$ and H_1 is bijective and for every (the carrier of G)-valued total $\operatorname{Seg} k$-defined function x such that for every element p of $\operatorname{Seg} k$, $x(p) \in F(p)$ holds $x \in \prod F$ and $H_1(x) = \prod x$.

(21) Suppose $\overline{\overline{G}} = p^m$. Then there exists a non zero natural number k and there exists a k-element finite sequence a of elements of G and there exists a k-element finite sequence I_2 of elements of $\mathbb{N}$ and there exists an associative group-like commutative multiplicative magma family F of $\operatorname{Seg} k$ such that for every natural number i such that $i \in \operatorname{Seg} k$ there exists an element a_2 of G such that $a_2 = a(i)$ and $F(i) = \operatorname{gr}(\{a_2\})$ and $\operatorname{ord}(a_2) = p^{I_2(i)}$ and for every natural number i such that $1 \leqslant i \leqslant k-1$ holds $I_2(i) \leqslant I_2(i+1)$ and for every elements p, q of $\operatorname{Seg} k$ such that $p \neq q$ holds (the carrier of $F(p)$) $\cap$ (the carrier of $F(q)) = \{\mathbf{1}_G\}$ and for every element y of G, there exists a (the carrier of G)-valued total $\operatorname{Seg} k$-defined function x such that for every element p of $\operatorname{Seg} k$, $x(p) \in F(p)$ and $y = \prod x$ and for every (the carrier of G)-valued total $\operatorname{Seg} k$-defined functions x_1, x_2 such that for every element p of $\operatorname{Seg} k$, $x_1(p) \in F(p)$ and for every element p of $\operatorname{Seg} k$, $x_2(p) \in F(p)$ and $\prod x_1 = \prod x_2$ holds $x_1 = x_2$.

References

[1] Kenichi Arai, Hiroyuki Okazaki, and Yasunari Shidama. Isomorphisms of direct products of finite cyclic groups. *Formalized Mathematics*, 20(**4**):343–347, 2012. doi:10.2478/v10037-012-0038-5.

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

[3] Grzegorz Bancerek. Monoids. *Formalized Mathematics*, 3(**2**):213–225, 1992.

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

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

[6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite

sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

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

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

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

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

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

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

[13] Artur Korniłowicz. The product of the families of the groups. *Formalized Mathematics*, 7(**1**):127–134, 1998.

[14] Jarosław Kotowicz. Convergent real sequences. Upper and lower bound of sets of real numbers. *Formalized Mathematics*, 1(**3**):477–481, 1990.

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

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

[17] Beata Madras. Product of family of universal algebras. *Formalized Mathematics*, 4(**1**): 103–108, 1993.

[18] Hiroyuki Okazaki, Hiroshi Yamazaki, and Yasunari Shidama. Isomorphisms of direct products of finite commutative groups. *Formalized Mathematics*, 21(**1**):65–74, 2013. doi:10.2478/forma-2013-0007.

[19] Dariusz Surowik. Isomorphisms of cyclic groups. Some properties of cyclic groups. *Formalized Mathematics*, 3(**1**):29–32, 1992.

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

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

[22] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.

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

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

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

[26] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.

[27] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.

[28] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.

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

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

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

Received October 7, 2013

FORMALIZED MATHEMATICS
Vol. 21, No. 3, Pages 213–221, 2013
DOI: 10.2478/forma-2013-0023

VERSITA
degruyter.com/view/j/forma

Prime Filters and Ideals in Distributive Lattices

Adam Grabowski
Institute of Informatics
University of Białystok
Akademicka 2, 15-267 Białystok
Poland

Summary. The article continues the formalization of the lattice theory (as structures with two binary operations, not in terms of ordering relations). In the Mizar Mathematical Library, there are some attempts to formalize prime ideals and filters; one series of articles written as decoding [9] proven some results; we tried however to follow [21], [12], and [13]. All three were devoted to the Stone representation theorem [18] for Boolean or Heyting lattices. The main aim of the present article was to bridge this gap between general distributive lattices and Boolean algebras, having in mind that the more general approach will eventually replace the common proof of aforementioned articles.[1]

Because in Boolean algebras the notions of ultrafilters, prime filters and maximal filters coincide, we decided to construct some concrete examples of ultrafilters in nontrivial Boolean lattice. We proved also the Prime Ideal Theorem not as BPI (Boolean Prime Ideal), but in the more general setting.

In the final section we present Nachbin theorems [15],[1] expressed both in terms of maximal and prime filters and as the unordered spectra of a lattice [11], [10]. This shows that if the notion of maximal and prime filters coincide in the lattice, it is Boolean.

MSC: 06D05 03B35

Keywords: prime filters; prime ideals; distributive lattices

MML identifier: `LATTICEA`, version: `8.1.02 5.19.1189`

The notation and terminology used in this paper have been introduced in the following articles: [2], [3], [5], [6], [4], [24], [12], [7], [17], [22], [23], [16], [20], and [8].

[1]As one of the anonymous reviewers pointed out, it would be interesting to show counterexamples showing that the assumptions of the distributivity and boundedness are necessary, and this will be our plan for future work as basic examples of non-distributive lattices are available as of now only as relational structures.

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

1. Preliminaries

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

(Def. 1) Let us consider sets p_1, p_2. Suppose

(i) $p_1, p_2 \in X$, and

(ii) $p_1 \neq p_2$.

Then p_1 and p_2 are $\subseteq$-incomparable.

Let us note that there exists a Boolean lattice which is non trivial.

Now we state the propositions:

(1) Let us consider a non trivial bounded lattice L. Then $\top_L \neq \bot_L$.

(2) Let us consider a lattice L and an ideal I of L. Then I is prime if and only if I^{c} is a filter of L or $I^{\mathrm{c}} = \emptyset$. Proof: If I is prime, then I^{c} is a filter of L or $I^{\mathrm{c}} = \emptyset$ by [20, (29)]. For every elements x, y of L, $x \sqcap y \in I$ iff $x \in I$ or $y \in I$ by [2, (9), (8)]. $\square$

(3) Let us consider a lattice L and a filter F of L. Then F is prime if and only if F^{c} is an ideal of L or $F^{\mathrm{c}} = \emptyset$. Proof: Set $F = I^{\mathrm{c}}$. If I is prime, then F is an ideal of L or $F = \emptyset$ by [20, (29)]. For every elements x, y of L, $x \sqcup y \in I$ iff $x \in I$ or $y \in I$ by [3, (21), (86)]. $\square$

Let L be a lattice. The functor $\mathrm{PFilters}\, L$ yielding a family of subsets of L is defined by the term

(Def. 2) $\{F$, where F is a filter of $L : F$ is prime$\}$.

Observe that $(L]$ is prime.

Now we state the proposition:

(4) Let us consider a distributive lattice L.
Then $\mathrm{PrimeFilters}(L) \subset \mathrm{PFilters}\, L$. Proof: $\mathrm{PrimeFilters}(L) \subseteq \mathrm{PFilters}\, L$. $[L) \notin \mathrm{PrimeFilters}(L)$. $\square$

2. Examples of Filters in Nontrivial Boolean Lattices

Now we state the propositions:

(5) The carrier of the lattice of subsets of $\{\emptyset\} = \{\emptyset, \{\emptyset\}\}$.

(6) Let us consider a lattice L and a subset A of L. Suppose $L =$ the lattice of subsets of $\{\emptyset\}$. Then

(i) $A = \emptyset$, or

(ii) $A = \{\emptyset\}$, or

(iii) $A = \{\emptyset, \{\emptyset\}\}$, or

(iv) $A = \{\{\emptyset\}\}$.

Let us consider a lattice L and a filter A of L. Now we state the propositions:

(7) Suppose $L =$ the lattice of subsets of $\{\emptyset\}$. Then

(i) $A = \emptyset$, or

(ii) $A = \{\emptyset, \{\emptyset\}\}$, or

(iii) $A = \{\{\emptyset\}\}$.

(8) If $L =$ the lattice of subsets of $\{\emptyset\}$, then $A = \{\top_L\}$ or $A = [L)$.

Now we state the propositions:

(9) Let us consider a non trivial Boolean lattice L and a filter A of L. Suppose

(i) $L =$ the lattice of subsets of $\{\emptyset\}$, and

(ii) $A = \{\top_L\}$.

Then A is prime. The theorem is a consequence of (5) and (7). Proof: For every filter H of L such that $A \subseteq H$ and $H \neq$ the carrier of L holds $A = H$ by [4, (4)]. $\square$

(10) Let us consider a lattice L and a filter A of L. Suppose

(i) $L =$ the lattice of subsets of $\{\emptyset\}$, and

(ii) A is an ultrafilter.

Then $A = \{\top_L\}$. The theorem is a consequence of (7). Proof: $\emptyset \notin A$ by [4, (3)], [21, (29)]. $\square$

3. On Prime and Maximal Filters and Ideals

Now we state the proposition:

(11) Let us consider a lattice L and an element a of L. Then $\{F,$ where F is a filter of $L : F$ is prime and $a \in F\} \subseteq \mathrm{PFilters}\, L$.

Let L be a lattice and F be a filter of L. We say that F is maximal if and only if

(Def. 3) (i) F is proper, and

(ii) for every filter G of L such that G is proper and $F \subseteq G$ holds $F = G$.

One can check that every filter of L which is maximal is also proper.

Observe that every filter of L which is maximal is also an ultrafilter and every filter of L which is an ultrafilter is also maximal.

Let I be an ideal of L. We say that I is maximal if and only if

(Def. 4) (i) I is proper, and

(ii) for every ideal J of L such that J is proper and $I \subseteq J$ holds $I = J$.

Now we state the proposition:

(12) Let us consider a lattice L and an ideal I of L. Then I is max-ideal if and only if I is maximal. Proof: For every ideal J of L such that $I \subseteq J$ and $J \neq$ the carrier of L holds $I = J$. $\square$

Let L be a lattice. Observe that every ideal of L which is maximal is also max-ideal and every ideal of L which is max-ideal is also maximal.

Let us observe that every ideal of L which is maximal is also proper.

Now we state the propositions:

(13) Let us consider a lattice L and a filter F of L. Suppose F is not prime. Then there exist elements a, b of L such that

(i) $a \sqcup b \in F$, and

(ii) $a \notin F$, and

(iii) $b \notin F$.

(14) Let us consider a lattice L and an ideal F of L. Suppose F is not prime. Then there exist elements a, b of L such that

(i) $a \sqcap b \in F$, and

(ii) $a \notin F$, and

(iii) $b \notin F$.

(15) Let us consider a lattice L, a filter F of L, an element a of L, and a set G. Suppose

(i) $G = \{x,$ where x is an element of $L:$ there exists an element u of L such that $u \in F$ and $a \sqcap u \sqsubseteq x\}$, and

(ii) $a \in G$.

Then G is a filter of L. Proof: $G \subseteq$ the carrier of L. Reconsider $G_1 = G$ as a subset of L. G_1 is meet-closed by [2, (5), (8)]. G_1 is final by [24, (7)]. $\square$

(16) Let us consider a lattice L, an ideal F of L, an element a of L, and a set G. Suppose

(i) $G = \{x,$ where x is an element of $L:$ there exists an element u of L such that $u \in F$ and $x \sqsubseteq a \sqcup u\}$, and

(ii) $a \in G$.

Then G is an ideal of L. Proof: $G \subseteq$ the carrier of L. G is join-closed by [2, (4)], [3, (86)]. G is initial by [24, (7)]. $\square$

(17) Let us consider a distributive lattice L and a filter F of L. If F is maximal, then F is prime. The theorem is a consequence of (13) and (15). Proof: Consider a, b being elements of L such that $a \sqcup b \in F$ and $a \notin F$ and $b \notin F$. Set $G = \{x,$ where x is an element of $L:$ there exists an element u of L such that $u \in F$ and $a \sqcap u \sqsubseteq x\}$. $b \notin G$ by [2, (10), (8)], [24, (11)]. $F \subseteq G$ by [24, (6)]. $\square$

Let L be a distributive lattice. One can verify that every filter of L which is maximal is also prime.

Now we state the proposition:

(18) Let us consider a distributive lattice L and an ideal F of L. If F is maximal, then F is prime. The theorem is a consequence of (14) and (16). Proof: Consider a, b being elements of L such that $a \sqcap b \in F$ and $a \notin F$ and $b \notin F$. Set $G = \{x,$ where x is an element of $L :$ there exists an element u of L such that $u \in F$ and $x \sqsubseteq a \sqcup u\}$. $G \subseteq$ the carrier of L. $b \notin G$ by [3, (22), (21)], [24, (4)]. $F \subseteq G$ by [24, (5)]. □

Let L be a distributive lattice. Observe that every ideal of L which is maximal is also prime.

4. Prime Ideal Theorem for Distributive Lattices

Now we state the propositions:

(19) Prime ideal theorem for distributive lattices:
Let us consider a distributive lattice L, an ideal I of L, and a filter F of L. Suppose I misses F. Then there exists an ideal P of L such that

(i) P is prime, and

(ii) $I \subseteq P$, and

(iii) P misses F.

The theorem is a consequence of (14). Proof: Set $X = \{i,$ where i is an ideal of $L : I \subseteq i$ and i misses $F\}$. For every set Z such that $Z \neq \emptyset$ and $Z \subseteq X$ and Z is $\subseteq$-linear holds $\bigcup Z \in X$ by [19, (1)], [8, (74)], [3, (21)]. Consider Y being a set such that $Y \in X$ and for every set Z such that $Z \in X$ and $Z \neq Y$ holds $Y \not\subseteq Z$. Consider i being an ideal of L such that $Y = i$ and $I \subseteq i$ and i misses F. i is prime by [3, (50), (28)], [2, (1), (9), (8)]. □

(20) Let us consider a distributive lattice L, an ideal I of L, and an element a of L. Suppose $a \notin I$. Then there exists an ideal P of L such that

(i) P is prime, and

(ii) $I \subseteq P$, and

(iii) $a \notin P$.

The theorem is a consequence of (19). Proof: Set $F = [a)$. I misses F by [2, (15)], [3, (21)]. Consider P being an ideal of L such that P is prime and $I \subseteq P$ and P misses F. □

Let us consider a distributive lattice L and elements a, b of L. Now we state the propositions:

(21) If $a \neq b$, then there exists an ideal P of L such that P is prime and $a \in P$ and $b \notin P$ or $a \notin P$ and $b \in P$.

(22) If $a \not\sqsubseteq b$, then there exists an ideal P of L such that P is prime and $a \notin P$ and $b \in P$.

Now we state the proposition:

(23) Let us consider a distributive lattice L and an ideal I of L. Then $I = \bigcap\{P,$ where P is an ideal of $L : P$ is prime and $I \subseteq P\}$. The theorem is a consequence of (20). PROOF: Ω_L is prime. □

5. The Stone Representation

Let L be a lattice. The prime filters of L yielding a function is defined by

(Def. 5) (i) dom it = the carrier of L, and

(ii) for every element a of L, $it(a) = \{F,$ where F is a filter of L : F is prime and $a \in F\}$.

Now we state the propositions:

(24) Let us consider a lattice L, an element a of L, and a set x. Then $x \in$ (the prime filters of L)(a) if and only if there exists a filter F of L such that $F = x$ and F is prime and $a \in F$. PROOF: If $x \in$ (the prime filters of L)(a), then there exists a filter F of L such that $F = x$ and F is prime and $a \in F$. □

(25) Let us consider a lattice L, an element a of L, and a filter F of L. Then $F \in$ (the prime filters of L)(a) if and only if F is prime and $a \in F$. The theorem is a consequence of (24).

Let us consider a distributive lattice L and elements a, b of L. Now we state the propositions:

(26) (The prime filters of L)($a \sqcap b$) = (the prime filters of L)(a) $\cap$ (the prime filters of L)(b).

(27) (The prime filters of L)($a \sqcup b$) = (the prime filters of L)(a) $\cup$ (the prime filters of L)(b).

Let L be a distributive lattice. Let us note that the prime filters of L yields a function from the carrier of L into $2^{\mathrm{PFilters}\, L}$. The functor StoneR($L$) yielding a set is defined by the term

(Def. 6) rng the prime filters of L.

Note that StoneR(L) is non empty.

Now we state the proposition:

(28) Let us consider a distributive lattice L and a set x. Then $x \in$ StoneR(L) if and only if there exists an element a of L such that (the prime filters of L)(a) $= x$. PROOF: If $x \in$ StoneR(L), then there exists an element a of L such that (the prime filters of L)(a) $= x$. □

Let L be an upper-bounded distributive lattice. The functor StoneSpace(L) yielding a strict topological space is defined by

(Def. 7) (i) the carrier of it = PFilters L, and

(ii) the topology of $it =$
$\{\bigcup A,$ where A is a family of subsets of PFilters $L : A \subseteq$ StoneR$(L)\}$.

Let L be a non trivial upper-bounded distributive lattice. One can check that StoneSpace(L) is non empty.

6. Pseudo Complements in Lattices

Let L be a lattice and a be an element of L. The functors: the set of pseudo-complements of a and the set of dual pseudo-complements of a yielding subsets of L are defined by terms, respectively.

(Def. 8) $\{x,$ where x is an element of $L : a \sqcap x = \bot_L\}$.

(Def. 9) $\{x,$ where x is an element of $L : a \sqcup x = \top_L\}$.

Let L be a distributive bounded lattice.

Note that the set of pseudo-complements of a is initial non empty and join-closed and the set of dual pseudo-complements of a is final non empty and meet-closed.

Let us consider a lattice L and elements a, b of L. Now we state the propositions:

(29) $b \in$ the set of pseudo-complements of a if and only if $b \sqcap a = \bot_L$.

(30) $b \in$ the set of dual pseudo-complements of a if and only if $b \sqcup a = \top_L$.

Let us consider a bounded lattice L and an element a of L. Now we state the propositions:

(31) $\bot_L \in$ the set of pseudo-complements of a.

(32) $\top_L \in$ the set of dual pseudo-complements of a.

7. Nachbin's Theorem for Bounded Distributive Lattices

Let L be a lattice. The spectrum of L yielding a family of subsets of L is defined by the term

(Def. 10) $\{I,$ where I is an ideal of $L : I$ is prime and proper$\}$.

Now we state the proposition:

(33) Nachbin's theorem for bounded distributive lattices:
Let us consider a distributive bounded lattice L. Then L is Boolean if and only if for every ideal I of L such that I is proper and prime holds I is maximal. The theorem is a consequence of (19). Proof: If L is Boolean, then for every ideal I of L such that I is proper and prime holds I is maximal by [3, (57)]. Consider a being an element of L such that there exists no an element b of L such that b is a complement of a. Set $I_0 =$ the set of pseudo-complements of a. Set $I_1 = \{x,$ where x is an element of $L :$ there exists an element y of L such that $y \in I_0$ and $x \sqsubseteq a \sqcup y\}$.

$I_1 \subseteq$ the carrier of L. For every elements p, q of L such that $p \sqsubseteq q$ and $q \in I_1$ holds $p \in I_1$ by [24, (7)]. For every elements p, q of L such that p, $q \in I_1$ holds $p \sqcup q \in I_1$ by [2, (4)]. $I_0 \subseteq I_1$ by [24, (5)]. $\top_L \notin I_1$. Set $F_2 = [\top_L)$. Consider J_0 being an ideal of L such that J_0 is prime and $I_1 \subseteq J_0$ and J_0 misses F_2. Set $T =$ the carrier of L. Reconsider $D = T \setminus J_0$ as a non empty subset of L. For every elements p, q of L such that $p \sqsubseteq q$ and $p \in D$ holds $q \in D$ by [3, (21)]. For every elements p, q of L such that p, $q \in D$ holds $p \sqcap q \in D$. Reconsider $F = [[a) \cup D)$ as a filter of L. F misses I_0 by [13, (3)], [24, (6)], [14, (9)]. Consider J_1 being an ideal of L such that J_1 is prime and $I_0 \subseteq J_1$ and J_1 misses F. $J_1 \subseteq J_0$. $\square$

Let L be a non trivial distributive bounded lattice. Let us note that the spectrum of L is non empty.

Now we state the proposition:

(34) Nachbin theorem for spectra of distributive lattices: Let us consider a distributive bounded lattice L. Then L is Boolean if and only if the spectrum of L is unordered. The theorem is a consequence of (19) and (20). Proof: If L is Boolean, then the spectrum of L is unordered by [3, (57), (58)], [24, (20)]. Consider a being an element of L such that there exists no an element b of L such that b is a complement of a. Set $D =$ the set of dual pseudo-complements of a. Set $D_1 = [D \cup [a))$. $D_1 \subseteq \{x,$ where x is an element of $L:$ there exists an element d of L such that $d \in D$ and $a \sqcap d \sqsubseteq x\}$ by [2, (15), (5)], [24, (7)]. $\{x,$ where x is an element of $L:$ there exists an element d of L such that $d \in D$ and $a \sqcap d \sqsubseteq x\} \subseteq D_1$. $\bot_L \notin D_1$ by [24, (8)]. Reconsider $I_0 = \{\bot_L\}$ as an ideal of L. Consider P being an ideal of L such that P is prime and $I_0 \subseteq P$ and P misses D_1. Set $P_1 = (P \cup (a]]$. $\top_L \notin P_1$ by [3, (49)], [2, (1)], [3, (28)]. Consider Q being an ideal of L such that Q is prime and $P_1 \subseteq Q$ and $\top_L \notin Q$. $\square$

Let L be a Boolean lattice. Note that the spectrum of L is unordered.

References

[1] Raymond Balbes and Philip Dwinger. *Distributive Lattices*. University of Missouri Press, 1975.

[2] Grzegorz Bancerek. Filters – part I. *Formalized Mathematics*, 1(**5**):813–819, 1990.

[3] Grzegorz Bancerek. Ideals. *Formalized Mathematics*, 5(**2**):149–156, 1996.

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

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

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

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

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

[9] G. Gierz, K.H. Hofmann, K. Keimel, J.D. Lawson, M. Mislove, and D.S. Scott. *A Compendium of Continuous Lattices*. Springer-Verlag, Berlin, Heidelberg, New York, 1980.

[10] George Grätzer. *General Lattice Theory.* Academic Press, New York, 1978.
[11] George Grätzer. *Lattice Theory: Foundation.* Birkhäuser, 2011.
[12] Jolanta Kamieńska. Representation theorem for Heyting lattices. *Formalized Mathematics*, 4(**1**):41–45, 1993.
[13] Jolanta Kamieńska and Jarosław Stanisław Walijewski. Homomorphisms of lattices, finite join and finite meet. *Formalized Mathematics*, 4(**1**):35–40, 1993.
[14] Agnieszka Julia Marasik. Boolean properties of lattices. *Formalized Mathematics*, 5(**1**): 31–35, 1996.
[15] Leopoldo Nachbin. Une propriété characteristique des algebres booleiennes. *Portugaliae Mathematica*, 6:115–118, 1947.
[16] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[17] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[18] Marshall H. Stone. The theory of representations of Boolean algebras. *Transactions of the American Mathematical Society*, 40:37–111, 1936.
[19] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[20] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[21] Jarosław Stanisław Walijewski. Representation theorem for Boolean algebras. *Formalized Mathematics*, 4(**1**):45–50, 1993.
[22] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[23] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[24] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

Received October 7, 2013

FORMALIZED MATHEMATICS
Vol. 21, No. 3, Pages 223–233, 2013
DOI: 10.2478/forma-2013-0024

VERSITA
degruyter.com/view/j/forma

Introduction to Formal Preference Spaces

Eliza Niewiadomska
Institute of Mathematics
University of Białystok
Akademicka 2, 15-267 Białystok
Poland

Adam Grabowski
Institute of Informatics
University of Białystok
Akademicka 2, 15-267 Białystok
Poland

Summary. In the article the formal characterization of preference spaces [1] is given. As the preference relation is one of the very basic notions of mathematical economics [9], it prepares some ground for a more thorough formalization of consumer theory (although some work has already been done – see [17]). There was an attempt to formalize similar results in Mizar, but this work seems still unfinished [18].

There are many approaches to preferences in literature. We modelled them in a rather illustrative way (similar structures were considered in [8]): either the consumer (strictly) prefers an alternative, or they are of equal interest; he/she could also have no opinion of the choice. Then our structures are based on three relations on the (arbitrary, not necessarily finite) set of alternatives. The completeness property can however also be modelled, although we rather follow [2] which is more general [12]. Additionally we assume all three relations are disjoint and their set-theoretic union gives a whole universe of alternatives.

We constructed some positive and negative examples of preference structures; the main aim of the article however is to give the characterization of consumer preference structures in terms of a binary relation, called characteristic relation [10], and to show the way the corresponding structure can be obtained only using this relation. Finally, we show the connection between tournament and total spaces and usual properties of the ordering relations.

MSC: 91B08 03B35

Keywords: preferences; preference spaces; social choice

MML identifier: `PREFER_1`, version: `8.1.02 5.19.1189`

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

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

1. Preliminaries

Let X, Y, Z be sets. We say that X, Y, and Z are mutually disjoint if and only if

(Def. 1) (i) X misses Y, and

(ii) Y misses Z, and

(iii) X misses Z.

Now we state the proposition:

(1) Let us consider a set A. Then $\emptyset$, A, and $\emptyset$ are mutually disjoint.

Let us observe that every set which is 2-element is also non empty.

Now we state the propositions:

(2) Let us consider sets a, b. Suppose $a \neq b$. Then $\{\langle a, a\rangle, \langle b, b\rangle\} \neq \{\langle a, a\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle b, b\rangle\}$.

(3) Let us consider a 2-element set A and elements a, b of A. If $a \neq b$, then $A = \{a, b\}$.

(4) Let us consider a 2-element set A. Then there exist elements a, b of A such that

(i) $a \neq b$, and

(ii) $A = \{a, b\}$.

(5) Let us consider a non trivial set A. Then there exist elements a, b of A such that $a \neq b$.

(6) Let us consider sets x_1, x_2, x_3, x_4. Then $(\{x_1\} \cup \{x_2\}) \cup \{x_3, x_4\} = \{x_3, x_1, x_2, x_4\}$.

(7) Let us consider sets a, b. Suppose $a \neq b$. Then $\{\langle a, a\rangle, \langle b, b\rangle\}$ misses $\{\langle a, b\rangle, \langle b, a\rangle\}$.

(8) Let us consider a 2-element set A and elements a, b of A. Suppose $a \neq b$. Then $\mathrm{id}_A = \{\langle a, a\rangle, \langle b, b\rangle\}$. The theorem is a consequence of (3).

(9) Let us consider elements a, b and a binary relation R. Suppose $R = \{\langle a, b\rangle\}$. Then $R^{\smile} = \{\langle b, a\rangle\}$.

(10) Let us consider sets a, b. Then $a \neq b$ if and only if $\{\langle a, b\rangle\}$ misses $\{\langle a, a\rangle, \langle b, b\rangle\}$. Proof: If $a \neq b$, then $\{\langle a, b\rangle\}$ misses $\{\langle a, a\rangle, \langle b, b\rangle\}$. $\square$

(11) Let us consider a non empty set X, a binary relation R on X, and elements x, y of X. Suppose $\langle x, y\rangle \notin R^{\mathrm{c}}$. Then $\langle x, y\rangle \in R$.

(12) Let us consider a non empty set X and a binary relation R on X. Then $R \cap (R^{\smile})^{\mathrm{c}}$, $R \cap R^{\smile}$, and $R^{\mathrm{c}} \cap (R^{\smile})^{\mathrm{c}}$ are mutually disjoint.

(13) Let us consider binary relations P, R. If P misses R, then $P^{\smile}$ misses $R^{\smile}$.

Let us consider a non empty set X and a binary relation R on X. Now we state the propositions:

(14) $R = (((R^{\smile})^{c})^{\smile})^{c}$.

(15) $R^{\smile} = ((R^{c})^{\smile})^{c}$.

(16) $((R^{\smile})^{c})^{\smile} = R^{c}$.

2. Properties of Binary Relations

Let X be a set. Observe that there exists an order in X which is connected and linear order.

Now we state the propositions:

(17) Let us consider a non empty set X and a total reflexive binary relation R on X. Then $R^{\smile}$ is total.

(18) Let us consider a non empty set X and a total binary relation R on X. Then $\operatorname{field} R = X$.

Let us consider a binary relation R. Now we state the propositions:

(19) R is irreflexive if and only if for every element x such that $x \in \operatorname{field} R$ holds $\langle x, x\rangle \notin R$.

(20) R is symmetric if and only if for every elements x, y such that $\langle x, y\rangle \in R$ holds $\langle y, x\rangle \in R$.

Now we state the propositions:

(21) Let us consider a set X and a binary relation R on X. Then $R \cap R^{\smile}$ is symmetric.

(22) Let us consider a binary relation R. Then R is asymmetric if and only if for every elements x, y such that $\langle x, y\rangle \in R$ holds $\langle y, x\rangle \notin R$. Proof: If R is asymmetric, then for every elements x, y such that $\langle x, y\rangle \in R$ holds $\langle y, x\rangle \notin R$ by [19, (15)]. If for every elements x, y such that $\langle x, y\rangle \in R$ holds $\langle y, x\rangle \notin R$, then R is asymmetric. □

(23) Let us consider elements a, b. If $a \neq b$, then $\{\langle a, b\rangle\}$ is asymmetric. The theorem is a consequence of (22). Proof: Set $R = \{\langle a, b\rangle\}$. For every elements x, y such that $\langle x, y\rangle \in R$ holds $\langle y, x\rangle \notin R$. □

(24) Let us consider a non empty set X and a binary relation R on X. Then $R \cap (R^{\smile})^{c}$ is asymmetric. The theorem is a consequence of (22).

Let us consider a non empty set X and a total reflexive binary relation R on X. Now we state the propositions:

(25) $R \cap R^{\smile}$ is reflexive.

(26) $R \cap R^{\smile}$ is total.

Now we state the propositions:

(27) Let us consider elements a, b. Suppose $a \neq b$. Then $\{\langle a, b\rangle, \langle b, a\rangle\}$ is irreflexive and symmetric. The theorem is a consequence of (20). Proof: Reconsider $R = \{\langle a, b\rangle, \langle b, a\rangle\}$ as a binary relation. For every elements x,

y such that $\langle x, y\rangle \in R$ holds $\langle y, x\rangle \in R$. For every element x such that $x \in \operatorname{field} R$ holds $\langle x, x\rangle \notin R$. $\square$

(28) Let us consider a non empty set X, a total binary relation R on X, and a binary relation S on X. Then $R \cup S$ is total.

(29) Let us consider a non empty set X and a total reflexive binary relation R on X. Then $R^{c} \cap (R^{\smile})^{c}$ is irreflexive and symmetric. The theorem is a consequence of (11) and (20). PROOF: For every elements x, y such that $\langle x, y\rangle \in R^{c} \cap (R^{\smile})^{c}$ holds $\langle y, x\rangle \in R^{c} \cap (R^{\smile})^{c}$ by [6, (87)]. $\square$

(30) Let us consider a set X and a binary relation R on X. If R is symmetric, then R^{c} is symmetric. The theorem is a consequence of (11) and (20). PROOF: For every elements x, y such that $\langle x, y\rangle \in R^{c}$ holds $\langle y, x\rangle \in R^{c}$ by [19, (15)], [16, (23)]. $\square$

(31) Let us consider an element X and a binary relation R. Then R is antisymmetric if and only if for every elements x, y such that $\langle x, y\rangle, \langle y, x\rangle \in R$ holds $x = y$. PROOF: If R is antisymmetric, then for every elements x, y such that $\langle x, y\rangle$, $\langle y, x\rangle \in R$ holds $x = y$ by [19, (15)]. $\square$

(32) Let us consider a set A and an asymmetric binary relation R on A. Then $R \cup \mathrm{id}_A$ is antisymmetric. The theorem is a consequence of (22) and (31). PROOF: For every elements x, y such that $\langle x, y\rangle$, $\langle y, x\rangle \in R \cup \mathrm{id}_A$ holds $x = y$. $\square$

(33) Let us consider an element X and a binary relation R. Then R is connected if and only if for every elements x, y such that $x \neq y$ and $x, y \in \operatorname{field} R$ holds $\langle x, y\rangle \in R$ or $\langle y, x\rangle \in R$.

(34) Let us consider a binary relation R. Then R is connected if and only if $\operatorname{field} R \times \operatorname{field} R = (R \cup R^{\smile}) \cup \mathrm{id}_{\operatorname{field} R}$.

(35) Let us consider a set A and an asymmetric binary relation R on A. Then R misses $R^{\smile}$. The theorem is a consequence of (22). PROOF: For every elements x, y, $\langle x, y\rangle \notin R \cap R^{\smile}$. $\square$

(36) Let us consider binary relations R, P. If R misses P and P is symmetric, then $R^{\smile}$ misses P. The theorem is a consequence of (13).

Let us consider a set X and an asymmetric binary relation R on X. Now we state the propositions:

(37) R misses id_X.

(38) $R \cdot R$ misses id_X.

Let X be a set and R be a binary relation on X. The functor $\operatorname{SymCl} R$ yielding a binary relation on X is defined by the term

(Def. 2) $R \cup R^{\smile}$.

Let R be a total binary relation on X. Note that $\operatorname{SymCl} R$ is total.

Let R be a binary relation on X. One can verify that $\operatorname{SymCl} R$ is symmetric.

3. Preference Structures

We consider pure preference structures which extend 1-sorted structures and are systems

$$\langle \text{a carrier}, \text{a preference relation} \rangle$$

where the carrier is a set, the preference relation is a binary relation on the carrier.

We consider preference-indifference structures which extend pure preference structures and alternative relational structures and are systems

$$\langle \text{a carrier}, \text{a preference relation}, \text{an alternative relation} \rangle$$

where the carrier is a set, the preference relation and the alternative relation are binary relations on the carrier.

We consider preference structures which extend preference-indifference structures, relational structures, and pure preference structures and are systems

$$\langle \text{a carrier}, \text{a preference relation}, \text{an alternative relation}, \text{an internal relation} \rangle$$

where the carrier is a set, the preference relation and the alternative relation and the internal relation are binary relations on the carrier.

Let us note that there exists a preference-indifference structure which is non empty and strict and there exists a preference-indifference structure which is empty and strict and there exists a pure preference structure which is non empty and strict and there exists a pure preference structure which is empty and strict and there exists a preference-indifference structure which is non empty and strict and there exists a preference structure which is non empty and strict.

Let X be a preference structure. We say that X is preference-like if and only if

(Def. 3) (i) the preference relation of X is asymmetric, and

(ii) the alternative relation of X is a tolerance of the carrier of X, and

(iii) the internal relation of X is irreflexive and symmetric, and

(iv) the preference relation of X, the alternative relation of X, and the internal relation of X are mutually disjoint, and

(v) (((the preference relation of X) $\cup$ (the preference relation of X)$^{\smile}$) $\cup$ the alternative relation of X) $\cup$ the internal relation of $X = \nabla_{\alpha}$,

where α is the carrier of X.

Let X be a set. The functor PrefSpace X yielding a strict preference structure is defined by the term

(Def. 4) $\langle X, \emptyset_{X,X}, \nabla_X, \emptyset_{X,X} \rangle$.

Let A be a non empty set. Observe that PrefSpace A is non empty and preference-like and there exists a preference structure which is non empty, strict, and preference-like.

A preference space is a preference-like preference structure. Note that every preference structure which is empty is also preference-like and PrefSpace $\emptyset$ is empty and preference-like and there exists a preference space which is empty.

Let A be a trivial non empty set. Let us observe that PrefSpace A is trivial.

Let us observe that PrefSpace A is non empty and preference-like.

4. Constructing Examples

Let A be a set. The functor IdPrefSpace A yielding a strict preference structure is defined by

(Def. 5) (i) the carrier of $it = A$, and

(ii) the preference relation of $it = \emptyset$, and

(iii) the alternative relation of $it = \mathrm{id}_A$, and

(iv) the internal relation of $it = \emptyset$.

Let A be a non trivial set. Let us observe that IdPrefSpace A is non preference-like.

Let A be a 2-element set and a, b be elements of A.

The functor PrefSpace(A, a, b) yielding a strict preference structure is defined by

(Def. 6) (i) the carrier of $it = A$, and

(ii) the preference relation of $it = \{\langle a,\, b\rangle\}$, and

(iii) the alternative relation of $it = \{\langle a,\, a\rangle, \langle b,\, b\rangle\}$, and

(iv) the internal relation of $it = \emptyset$.

Now we state the proposition:

(39) Let us consider a 2-element set A and elements a, b of A. If $a \neq b$, then PrefSpace(A, a, b) is preference-like. The theorem is a consequence of (8), (10), (9), (3), (6), and (23).

Let A be a non empty set and a, b be elements of A.

The functor IntPrefSpace(A, a, b) yielding a strict preference structure is defined by

(Def. 7) (i) the carrier of $it = A$, and

(ii) the preference relation of $it = \emptyset$, and

(iii) the alternative relation of $it = \{\langle a,\, a\rangle, \langle b,\, b\rangle\}$, and

(iv) the internal relation of $it = \{\langle a,\, b\rangle, \langle b,\, a\rangle\}$.

Now we state the proposition:

(40) Let us consider a 2-element set A and elements a, b of A. Suppose $a \neq b$. Then IntPrefSpace(A, a, b) is non empty and preference-like. The theorem is a consequence of (8), (7), (3), and (27).

5. Characteristic Relation of a Preference Space

Let P be a preference-indifference structure. The functor CharRel P yielding a binary relation on the carrier of P is defined by the term

(Def. 8) (The preference relation of P) $\cup$ (the alternative relation of P).

We say that P is PI-preference-like if and only if

(Def. 9) (i) the preference relation of P is asymmetric, and

(ii) the alternative relation of P is a tolerance of the carrier of P, and

(iii) (the preference relation of P) $\cap$ (the alternative relation of P) $= \emptyset$, and

(iv) ((the preference relation of P) $\cup$ (the preference relation of P)$^{\smile}$) $\cup$ the alternative relation of $P = \nabla_{\alpha}$,

where α is the carrier of P.

Observe that there exists a non empty strict preference-indifference structure which is PI-preference-like and there exists an empty strict preference-indifference structure which is PI-preference-like.

Let us consider a non empty preference-indifference structure P. Now we state the propositions:

(41) Suppose P is PI-preference-like. Then the preference relation of $P =$ CharRel $P \cap ((\mathrm{CharRel}\,P)^{\smile})^{\mathrm{c}}$.

(42) Suppose P is PI-preference-like. Then the alternative relation of $P =$ CharRel $P \cap (\mathrm{CharRel}\,P)^{\smile}$.

Let us consider a non empty preference structure P. Now we state the propositions:

(43) Suppose P is preference-like.
Then the preference relation of $P = \mathrm{CharRel}\,P \cap ((\mathrm{CharRel}\,P)^{\smile})^{\mathrm{c}}$.

(44) Suppose P is preference-like.
Then the alternative relation of $P = \mathrm{CharRel}\,P \cap (\mathrm{CharRel}\,P)^{\smile}$.

(45) Suppose P is preference-like.
Then the internal relation of $P = (\mathrm{CharRel}\,P)^{\mathrm{c}} \cap ((\mathrm{CharRel}\,P)^{\smile})^{\mathrm{c}}$.

6. Generating Preference Space from Arbitrary (Characteristic) Relation

Let X be a set and R be a binary relation on X. The functor $\mathrm{Aux}(R)$ yielding a binary relation on X is defined by the term

(Def. 10) $\mathrm{SymCl}((R \cap (R^{\smile})^{\mathrm{c}} \cup (R \cap (R^{\smile})^{\mathrm{c}})^{\smile}) \cup R \cap R^{\smile})^{\mathrm{c}}$.

Now we state the proposition:

(46) Let us consider a non empty set X and a binary relation R on X. Then $((R \cap (R^{\smile})^{\mathrm{c}} \cup (R \cap (R^{\smile})^{\mathrm{c}})^{\smile}) \cup R \cap R^{\smile}) \cup \mathrm{Aux}(R) = \nabla_X$.

Let us consider a non empty set X and a total reflexive binary relation R on X. Now we state the propositions:

(47) $\mathrm{Aux}(R) = (R^{\smile})^{\mathrm{c}} \cap R^{\mathrm{c}} \cup (R^{\mathrm{c}})^{\smile} \cap (R^{\mathrm{c}} \cup R^{\smile})$.

(48) $R \cap (R^{\smile})^{\mathrm{c}}$ misses $\mathrm{Aux}(R)$.

(49) $\mathrm{Aux}(R)$ is irreflexive and symmetric.

Let X be a non empty set and R be a total reflexive binary relation on X. One can check that $\mathrm{Aux}(R)$ is irreflexive and symmetric.

Let us consider a non empty set X and a total reflexive binary relation R on X. Now we state the propositions:

(50) $R \cap R^{\smile}$ misses $\mathrm{Aux}(R)$.

(51) $R \cap (R^{\smile})^{\mathrm{c}}$, $R \cap R^{\smile}$, and $\mathrm{Aux}(R)$ are mutually disjoint.

Let X be a set and P be a binary relation on X. The functor $\mathrm{CharPrefSpace}\,P$ yielding a strict preference structure is defined by

(Def. 11) (i) the carrier of $it = X$, and

(ii) the preference relation of $it = P \cap (P^{\smile})^{\mathrm{c}}$, and

(iii) the alternative relation of $it = P \cap P^{\smile}$, and

(iv) the internal relation of $it = \mathrm{Aux}(P)$.

Now we state the proposition:

(52) Let us consider a non empty set A and a total reflexive binary relation R on A. Then $\mathrm{CharPrefSpace}\,R$ is preference-like. The theorem is a consequence of (24), (46), (51), (26), and (21).

Let X be a non empty set and P be a binary relation on X. Let us observe that $\mathrm{CharPrefSpace}\,P$ is non empty.

Let P be a total reflexive binary relation on X.
Let us note that $\mathrm{CharPrefSpace}\,P$ is preference-like.

7. Flat Preference Spaces

Let P be a preference structure. We say that P is flat if and only if

(Def. 12) (i) the alternative relation of $P = \mathrm{id}_\alpha$, and

(ii) there exists an element a of P such that the preference relation of $P = \{a\} \times ((\text{the carrier of } P) \setminus \{a\})$ and the internal relation of $P = ((\text{the carrier of } P) \setminus \{a\}) \times ((\text{the carrier of } P) \setminus \{a\})$,

where α is the carrier of P.

Now we state the proposition:

(53) Let us consider a trivial set A. Then $\mathrm{IdPrefSpace}\, A = \mathrm{PrefSpace}\, A$.

Let A be a trivial non empty set. One can check that $\mathrm{IdPrefSpace}\, A$ is non empty and preference-like.

One can check that $\mathrm{IdPrefSpace}\, A$ is flat.

8. Tournament Preference Spaces

Let P be a preference structure. We say that P is tournament-like if and only if

(Def. 13) (i) the alternative relation of $P = \mathrm{id}_\alpha$, and

(ii) the internal relation of $P = \emptyset$,

where α is the carrier of P.

One can check that every preference structure which is empty is also tournament-like and every preference structure which is tournament-like is also void and there exists an empty preference space which is tournament-like and there exists a non empty preference space which is tournament-like.

Now we state the proposition:

(54) Let us consider a non empty preference space P. Then P is tournament-like if and only if $\mathrm{CharRel}\, P$ is connected, antisymmetric, and total. The theorem is a consequence of (33), (32), (35), (34), and (45). Proof: If P is tournament-like, then $\mathrm{CharRel}\, P$ is connected, antisymmetric, and total by [6, (87)]. If $\mathrm{CharRel}\, P$ is connected, total, and antisymmetric, then P is tournament-like by [21, (22)], [19, (23)], [21, (13)]. □

9. Total Preference Spaces

Let P be a preference structure. We say that P is total if and only if

(Def. 14) (i) the preference relation of P is transitive, and

(ii) the alternative relation of $P = \mathrm{id}_\alpha$, and

(iii) the internal relation of $P = \emptyset$,

where α is the carrier of P.

Let us observe that every preference structure which is total is also void and every preference structure which is total is also tournament-like and PrefSpace $\emptyset$ is total.

Let A be a set. One can verify that IdPrefSpace A is total.

Let A be a trivial non empty set. Let us note that PrefSpace A is total and there exists an empty preference space which is total and there exists a non empty preference space which is total.

Now we state the proposition:

(55) Let us consider a non empty preference space P. Then P is total if and only if CharRel P is a connected order in the carrier of P. The theorem is a consequence of (35), (37), (38), and (36). Proof: If P is total, then CharRel P is a connected order in the carrier of P by [15, (12)], [21, (13)], [19, (18), (23)]. If CharRel P is a connected order in the carrier of P, then P is total by [15, (12)], [21, (13), (1), (22)]. $\square$

References

[1] Kenneth J. Arrow. *Social Choice and Individual Values.* Yale University Press, 1963.
[2] Robert J. Aumann. Utility theory without the completeness axiom. *Econometrica*, 30(3): 445–462, 1962.
[3] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[5] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[6] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[7] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[8] Klaus E. Grue and Artur Korniłowicz. Basic operations on preordered coherent spaces. *Formalized Mathematics*, 15(**4**):213–230, 2007. doi:10.2478/v10037-007-0025-4.
[9] Sören Halldén. *On the Logic of Better.* Lund: Library of Theoria, 1957.
[10] Emil Panek. *Podstawy ekonomii matematycznej.* Uniwersytet Ekonomiczny w Poznaniu, 2005. In Polish.
[11] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.
[12] George F. Schumm. Transitivity, preference, and indifference. *Philosophical Studies*, 52: 435–437, 1987.
[13] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.
[14] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.
[15] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[16] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[17] Freek Wiedijk. Arrow's impossibility theorem. *Formalized Mathematics*, 15(**4**):171–174, 2007. doi:10.2478/v10037-007-0020-9.
[18] Krzysztof Wojszko and Artur Kuzyka. Formalization of commodity space and preference relation in Mizar. *Mechanized Mathematics and Its Applications*, 4:67–74, 2005.
[19] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[20] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[21] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Received October 7, 2013