Contents

Formaliz. Math. 17 (**2**)

FORMALIZED MATHEMATICS
Vol. **17**, No. **2**, Pages 61–65, **2009**

Some Operations on Quaternion Numbers

Bo Li
Qingdao University of Science and Technology
China

Pan Wang
Qingdao University of Science and Technology
China

Xiquan Liang
Qingdao University of Science and Technology
China

Yanping Zhuang
Qingdao University of Science and Technology
China

Summary. In this article, we give some equality and basic theorems about quaternion numbers, and some special operations.

MML identifier: `QUATERN3`, version: `7.11.02 4.120.1050`

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

In this paper z_1, z_2, z_3, z_4, z are quaternion numbers.

The following propositions are true:

(1) $\Re(z_1 \cdot z_2) = \Re(z_2 \cdot z_1)$.

(2) If z is a real number, then $z + z_3 = \Re(z) + \Re(z_3) + \Im_1(z_3) \cdot i + \Im_2(z_3) \cdot j + \Im_3(z_3) \cdot k$.

(3) If z is a real number, then $z - z_3 = \langle \Re(z) - \Re(z_3), -\Im_1(z_3), -\Im_2(z_3), -\Im_3(z_3) \rangle_{\mathbb{H}}$.

(4) If z is a real number, then $z \cdot z_3 = \langle \Re(z) \cdot \Re(z_3), \Re(z) \cdot \Im_1(z_3), \Re(z) \cdot \Im_2(z_3), \Re(z) \cdot \Im_3(z_3) \rangle_{\mathbb{H}}$.

(5) If z is a real number, then $z \cdot i = \langle 0, \Re(z), 0, 0 \rangle_{\mathbb{H}}$.

(6) If z is a real number, then $z \cdot j = \langle 0, 0, \Re(z), 0 \rangle_{\mathbb{H}}$.

(7) If z is a real number, then $z \cdot k = \langle 0, 0, 0, \Re(z) \rangle_{\mathbb{H}}$.

(8) $z - 0_{\mathbb{H}} = z$.

(9) If z is a real number, then $z \cdot z_1 = z_1 \cdot z$.

(10) If $\Im_1(z) = 0$ and $\Im_2(z) = 0$ and $\Im_3(z) = 0$, then $z = \Re(z)$.

(11) $|z|^{\mathbf{2}} = (\Re(z))^{\mathbf{2}} + (\Im_1(z))^{\mathbf{2}} + (\Im_2(z))^{\mathbf{2}} + (\Im_3(z))^{\mathbf{2}}$.

(12) $|z|^{\mathbf{2}} = |z \cdot \overline{z}|$.

(13) $|z|^{\mathbf{2}} = \Re(z \cdot \overline{z})$.

(14) $2 \cdot \Re(z) = \Re(z + \overline{z})$.

(15) If z is a real number, then $\overline{z \cdot z_1} = \overline{z} \cdot \overline{z_1}$.

(16) $\overline{z_1 \cdot z_2} = \overline{z_2} \cdot \overline{z_1}$.

(17) $|z_1 \cdot z_2|^{\mathbf{2}} = |z_1|^{\mathbf{2}} \cdot |z_2|^{\mathbf{2}}$.

(18) $i \cdot z_1 - z_1 \cdot i = \langle 0, 0, -2 \cdot \Im_3(z_1), 2 \cdot \Im_2(z_1) \rangle_{\mathbb{H}}$.

(19) $i \cdot z_1 + z_1 \cdot i = \langle -2 \cdot \Im_1(z_1), 2 \cdot \Re(z_1), 0, 0 \rangle_{\mathbb{H}}$.

(20) $j \cdot z_1 - z_1 \cdot j = \langle 0, 2 \cdot \Im_3(z_1), 0, -2 \cdot \Im_1(z_1) \rangle_{\mathbb{H}}$.

(21) $j \cdot z_1 + z_1 \cdot j = \langle -2 \cdot \Im_2(z_1), 0, 2 \cdot \Re(z_1), 0 \rangle_{\mathbb{H}}$.

(22) $k \cdot z_1 - z_1 \cdot k = \langle 0, -2 \cdot \Im_2(z_1), 2 \cdot \Im_1(z_1), 0 \rangle_{\mathbb{H}}$.

(23) $k \cdot z_1 + z_1 \cdot k = \langle -2 \cdot \Im_3(z_1), 0, 0, 2 \cdot \Re(z_1) \rangle_{\mathbb{H}}$.

(24) $\Re(\frac{1}{|z|^{\mathbf{2}}} \cdot \overline{z}) = \frac{1}{|z|^{\mathbf{2}}} \cdot \Re(z)$.

(25) $\Im_1(\frac{1}{|z|^{\mathbf{2}}} \cdot \overline{z}) = -\frac{1}{|z|^{\mathbf{2}}} \cdot \Im_1(z)$.

(26) $\Im_2(\frac{1}{|z|^{\mathbf{2}}} \cdot \overline{z}) = -\frac{1}{|z|^{\mathbf{2}}} \cdot \Im_2(z)$.

(27) $\Im_3(\frac{1}{|z|^{\mathbf{2}}} \cdot \overline{z}) = -\frac{1}{|z|^{\mathbf{2}}} \cdot \Im_3(z)$.

(28) $\frac{1}{|z|^{\mathbf{2}}} \cdot \overline{z} = \langle \frac{1}{|z|^{\mathbf{2}}} \cdot \Re(z), -\frac{1}{|z|^{\mathbf{2}}} \cdot \Im_1(z), -\frac{1}{|z|^{\mathbf{2}}} \cdot \Im_2(z), -\frac{1}{|z|^{\mathbf{2}}} \cdot \Im_3(z) \rangle_{\mathbb{H}}$.

(29) $z \cdot (\frac{1}{|z|^{\mathbf{2}}} \cdot \overline{z}) = \langle \frac{|z|^{\mathbf{2}}}{|z|^{\mathbf{2}}}, 0, 0, 0 \rangle_{\mathbb{H}}$.

(30) $\Re(z_1 \cdot z_2) = \Re(z_1) \cdot \Re(z_2) - \Im_1(z_1) \cdot \Im_1(z_2) - \Im_2(z_1) \cdot \Im_2(z_2) - \Im_3(z_1) \cdot \Im_3(z_2)$.

(31) $\Im_1(z_1 \cdot z_2) = (\Re(z_1) \cdot \Im_1(z_2) + \Im_1(z_1) \cdot \Re(z_2) + \Im_2(z_1) \cdot \Im_3(z_2)) - \Im_3(z_1) \cdot \Im_2(z_2)$.

(32) $\Im_2(z_1 \cdot z_2) = (\Re(z_1) \cdot \Im_2(z_2) + \Im_2(z_1) \cdot \Re(z_2) + \Im_3(z_1) \cdot \Im_1(z_2)) - \Im_1(z_1) \cdot \Im_3(z_2)$.

(33) $\Im_3(z_1 \cdot z_2) = (\Re(z_1) \cdot \Im_3(z_2) + \Im_3(z_1) \cdot \Re(z_2) + \Im_1(z_1) \cdot \Im_2(z_2)) - \Im_2(z_1) \cdot \Im_1(z_2)$.

(34) $|z_1 \cdot z_2 \cdot z_3|^{\mathbf{2}} = |z_1|^{\mathbf{2}} \cdot |z_2|^{\mathbf{2}} \cdot |z_3|^{\mathbf{2}}$.

(35) $\Re(z_1 \cdot z_2 \cdot z_3) = \Re(z_3 \cdot z_1 \cdot z_2)$.

(36) $|z \cdot z| = |\overline{z} \cdot \overline{z}|$.

(37) $|\overline{z} \cdot \overline{z}| = |z|^{\mathbf{2}}$.

(38) $|z_1 \cdot z_2 \cdot z_3| = |z_1| \cdot |z_2| \cdot |z_3|$.

(39) $|z_1 + z_2 + z_3| \leq |z_1| + |z_2| + |z_3|$.

(40) $|(z_1 + z_2) - z_3| \leq |z_1| + |z_2| + |z_3|$.

(41) $|z_1 - z_2 - z_3| \leq |z_1| + |z_2| + |z_3|$.

(42) $|z_1| - |z_2| \leq \frac{|z_1+z_2|+|z_1-z_2|}{2}$.

(43) $|z_1| - |z_2| \leq \frac{|z_1+z_2|+|z_2-z_1|}{2}$.

(44) $||z_1| - |z_2|| \leq |z_2 - z_1|$.

(45) $||z_1| - |z_2|| \leq |z_1| + |z_2|$.

(46) $|z_1| - |z_2| \leq |z_1 - z| + |z - z_2|$.

(47) If $|z_1| - |z_2| \neq 0$, then $(|z_1|^{\mathbf{2}} + |z_2|^{\mathbf{2}}) - 2 \cdot |z_1| \cdot |z_2| > 0$.

(48) $|z_1| + |z_2| \geq \frac{|z_1+z_2|+|z_2-z_1|}{2}$.

(49) $|z_1| + |z_2| \geq \frac{|z_1+z_2|+|z_1-z_2|}{2}$.

(50) $(z_1 \cdot z_2)^{-1} = {z_2}^{-1} \cdot {z_1}^{-1}$.

(51) $\overline{z}^{-1} = \overline{z^{-1}}$.

(52) $(1_{\mathbb{H}})^{-1} = 1_{\mathbb{H}}$.

(53) If $|z_1| = |z_2|$ and $|z_1| \neq 0$ and ${z_1}^{-1} = {z_2}^{-1}$, then $z_1 = z_2$.

(54) $(z_1 - z_2) \cdot (z_3 + z_4) = ((z_1 \cdot z_3 - z_2 \cdot z_3) + z_1 \cdot z_4) - z_2 \cdot z_4$.

(55) $(z_1 + z_2) \cdot (z_3 + z_4) = z_1 \cdot z_3 + z_2 \cdot z_3 + z_1 \cdot z_4 + z_2 \cdot z_4$.

(56) $-(z_1 + z_2) = -z_1 - z_2$.

(57) $-(z_1 - z_2) = -z_1 + z_2$.

(58) $z - (z_1 + z_2) = z - z_1 - z_2$.

(59) $z - (z_1 - z_2) = (z - z_1) + z_2$.

(60) $(z_1 + z_2) \cdot (z_3 - z_4) = (z_1 \cdot z_3 + z_2 \cdot z_3) - z_1 \cdot z_4 - z_2 \cdot z_4$.

(61) $(z_1 - z_2) \cdot (z_3 - z_4) = (z_1 \cdot z_3 - z_2 \cdot z_3 - z_1 \cdot z_4) + z_2 \cdot z_4$.

(62) $-(z_1 + z_2 + z_3) = -z_1 - z_2 - z_3$.

(63) $-(z_1 - z_2 - z_3) = -z_1 + z_2 + z_3$.

(64) $-((z_1 - z_2) + z_3) = (-z_1 + z_2) - z_3$.

(65) $-((z_1 + z_2) - z_3) = (-z_1 - z_2) + z_3$.

(66) If $z_1 + z = z_2 + z$, then $z_1 = z_2$.

(67) If $z_1 - z = z_2 - z$, then $z_1 = z_2$.

(68) $((z_1 + z_2) - z_3) \cdot z_4 = (z_1 \cdot z_4 + z_2 \cdot z_4) - z_3 \cdot z_4$.

(69) $((z_1 - z_2) + z_3) \cdot z_4 = (z_1 \cdot z_4 - z_2 \cdot z_4) + z_3 \cdot z_4$.

(70) $(z_1 - z_2 - z_3) \cdot z_4 = z_1 \cdot z_4 - z_2 \cdot z_4 - z_3 \cdot z_4$.

(71) $(z_1 + z_2 + z_3) \cdot z_4 = z_1 \cdot z_4 + z_2 \cdot z_4 + z_3 \cdot z_4$.

(72) $(z_1 - z_2) \cdot z_3 = (z_2 - z_1) \cdot -z_3$.

(73) $z_3 \cdot (z_1 - z_2) = (-z_3) \cdot (z_2 - z_1)$.

(74) $(z_1 - z_2 - z_3) + z_4 = (z_4 - z_3 - z_2) + z_1$.

(75) $(z_1 - z_2) \cdot (z_3 - z_4) = (z_2 - z_1) \cdot (z_4 - z_3)$.

(76) $z - z_1 - z_2 = z - z_2 - z_1$.

(77) $z^{-1} = \langle \frac{\Re(z)}{|z|^{\mathbf{2}}}, -\frac{\Im_1(z)}{|z|^{\mathbf{2}}}, -\frac{\Im_2(z)}{|z|^{\mathbf{2}}}, -\frac{\Im_3(z)}{|z|^{\mathbf{2}}} \rangle_{\mathbb{H}}$.

(78) $\frac{z_1}{z_2} = \langle \frac{\Re(z_2)\cdot\Re(z_1)+\Im_1(z_1)\cdot\Im_1(z_2)+\Im_2(z_2)\cdot\Im_2(z_1)+\Im_3(z_2)\cdot\Im_3(z_1)}{|z_2|^{\mathbf{2}}}, \frac{(\Re(z_2)\cdot\Im_1(z_1)-\Im_1(z_2)\cdot\Re(z_1)-\Im_2(z_2)\cdot\Im_3(z_1))+\Im_3(z_2)\cdot\Im_2(z_1)}{|z_2|^{\mathbf{2}}}, \frac{(\Re(z_2)\cdot\Im_2(z_1)+\Im_1(z_2)\cdot\Im_3(z_1))-\Im_2(z_2)\cdot\Re(z_1)-\Im_3(z_2)\cdot\Im_1(z_1)}{|z_2|^{\mathbf{2}}}, \frac{((\Re(z_2)\cdot\Im_3(z_1)-\Im_1(z_2)\cdot\Im_2(z_1))+\Im_2(z_2)\cdot\Im_1(z_1))-\Im_3(z_2)\cdot\Re(z_1)}{|z_2|^{\mathbf{2}}} \rangle_{\mathbb{H}}$.

(79) $(i)^{-1} = -i$.

(80) $(j)^{-1} = -j$.

(81) $(k)^{-1} = -k$.

Let z be a quaternion number. The functor $z^{\mathbf{2}}$ is defined by:

(Def. 1) $z^{\mathbf{2}} = z \cdot z$.

Let z be a quaternion number. One can verify that $z^{\mathbf{2}}$ is quaternion.

Let z be an element of $\mathbb{H}$. Then $z^{\mathbf{2}}$ is an element of $\mathbb{H}$.

One can prove the following four propositions:

(82) $z^{\mathbf{2}} = \langle (\Re(z))^{\mathbf{2}} - (\Im_1(z))^{\mathbf{2}} - (\Im_2(z))^{\mathbf{2}} - (\Im_3(z))^{\mathbf{2}}, 2 \cdot (\Re(z) \cdot \Im_1(z)), 2 \cdot (\Re(z) \cdot \Im_2(z)), 2 \cdot (\Re(z) \cdot \Im_3(z)) \rangle_{\mathbb{H}}$.

(83) $(0_{\mathbb{H}})^{\mathbf{2}} = 0$.

(84) $(1_{\mathbb{H}})^{\mathbf{2}} = 1$.

(85) $z^{\mathbf{2}} = (-z)^{\mathbf{2}}$.

Let z be a quaternion number. The functor $z^{\mathbf{3}}$ is defined as follows:

(Def. 2) $z^{\mathbf{3}} = z \cdot z \cdot z$.

Let z be a quaternion number. Observe that $z^{\mathbf{3}}$ is quaternion.

Let z be an element of $\mathbb{H}$. Then $z^{\mathbf{3}}$ is an element of $\mathbb{H}$.

Next we state several propositions:

(86) $(0_{\mathbb{H}})^{\mathbf{3}} = 0$.

(87) $(1_{\mathbb{H}})^{\mathbf{3}} = 1$.

(88) $(i)^{\mathbf{3}} = -i$.

(89) $(j)^{\mathbf{3}} = -j$.

(90) $(k)^{\mathbf{3}} = -k$.

(91) $(-1_{\mathbb{H}})^{\mathbf{2}} = 1$.

(92) $(-1_{\mathbb{H}})^{\mathbf{3}} = -1$.

(93) $z^{\mathbf{3}} = -(-z)^{\mathbf{3}}$.

References

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

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

[6] Fuguo Ge. Inner products, group, ring of quaternion numbers. *Formalized Mathematics*, 16(**2**):135–139, 2008, doi:10.2478/v10037-008-0019-x.

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

[8] Xiquan Liang and Fuguo Ge. The quaternion numbers. *Formalized Mathematics*, 14(**4**):161–169, 2006, doi:10.2478/v10037-006-0020-1.

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

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

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

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

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

Received October 14, 2008

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 67–72, 2009

Complex Function Differentiability

Chanapat Pacharapokin
Shinshu University
Nagano, Japan

Hiroshi Yamazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Yatsuka Nakamura
Shinshu University
Nagano, Japan

Summary. For a complex valued function defined on its domain in complex numbers the differentiability in a single point and on a subset of the domain is presented. The main elements of differential calculus are developed. The algebraic properties of differential complex functions are shown.

MML identifier: CFDIFF_1, version: 7.11.01 4.117.1046

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

For simplicity, we use the following convention: k, n, m denote elements of $\mathbb{N}$, X denotes a set, s_1, s_2 denote complex sequences, Y denotes a subset of $\mathbb{C}$, f, f_1, f_2 denote partial functions from $\mathbb{C}$ to $\mathbb{C}$, r denotes a real number, a, a_1, b, x, x_0, z, z_0 denote complex numbers, and N_1 denotes an increasing sequence of naturals.

Let I be a complex sequence. We say that I is convergent to 0 if and only if:

(Def. 1) I is non-zero and convergent and $\lim I = 0$.

We now state four propositions:

(1) Let r_1 be a sequence of real numbers and c_1 be a complex sequence. If $r_1 = c_1$ and r_1 is convergent, then c_1 is convergent.

(2) If $0 < r$ and for every n holds $s_1(n) = \frac{1}{n+r}$, then s_1 is convergent.

(3) If $0 < r$ and for every n holds $s_1(n) = \frac{1}{n+r}$, then $\lim s_1 = 0$.

(4) If for every n holds $s_1(n) = \frac{1}{n+1}$, then s_1 is convergent and $\lim s_1 = 0$.

ISSN 1426–2630(p), 1898-9934(e)

Let us observe that there exists a complex sequence which is convergent to 0.

Let us note that there exists a complex sequence which is constant.

Next we state four propositions:

(5) s_1 is constant iff for all n, m holds $s_1(n) = s_1(m)$.

(6) For every n holds $(s_1 \cdot N_1)(n) = s_1(N_1(n))$.

(7) If s_1 is constant and s_2 is a subsequence of s_1, then s_2 is constant.

(8) If s_1 is constant and s_2 is a subsequence of s_1, then $s_1 = s_2$.

Let s_3 be a constant complex sequence. Note that every subsequence of s_3 is constant.

In the sequel h is a convergent to 0 complex sequence and c is a constant complex sequence.

Let I be a partial function from $\mathbb{C}$ to $\mathbb{C}$. We say that I is rest-like if and only if:

(Def. 2) I is total and for every h holds $h^{-1}\,(I \cdot h)$ is convergent and $\lim(h^{-1}\,(I \cdot h)) = 0$.

Let us mention that there exists a partial function from $\mathbb{C}$ to $\mathbb{C}$ which is rest-like.

A $\mathbb{C}$-rest is a rest-like partial function from $\mathbb{C}$ to $\mathbb{C}$.

Let I be a partial function from $\mathbb{C}$ to $\mathbb{C}$. We say that I is linear if and only if:

(Def. 3) I is total and there exists a such that for every z holds $I_z = a \cdot z$.

One can check that there exists a partial function from $\mathbb{C}$ to $\mathbb{C}$ which is linear.

A $\mathbb{C}$-linear function is a linear partial function from $\mathbb{C}$ to $\mathbb{C}$.

We adopt the following convention: R, R_1, R_2 are $\mathbb{C}$-rests and L, L_1, L_2 are $\mathbb{C}$-linear functions.

Let us consider L_1, L_2. Observe that $L_1 + L_2$ is linear and $L_1 - L_2$ is linear.

The following propositions are true:

(9) For all L_1, L_2 holds $L_1 + L_2$ is a $\mathbb{C}$-linear function and $L_1 - L_2$ is a $\mathbb{C}$-linear function.

(10) For all a, L holds $a\,L$ is a $\mathbb{C}$-linear function.

(11) For all R_1, R_2 holds $R_1 + R_2$ is a $\mathbb{C}$-rest and $R_1 - R_2$ is a $\mathbb{C}$-rest and $R_1\,R_2$ is a $\mathbb{C}$-rest.

(12) $a\,R$ is a $\mathbb{C}$-rest.

(13) $L_1\,L_2$ is rest-like.

(14) $R\,L$ is a $\mathbb{C}$-rest and $L\,R$ is a $\mathbb{C}$-rest.

Let z_0 be a complex number. A subset of $\mathbb{C}$ is called a neighbourhood of z_0 if:

(Def. 4) There exists a real number g such that $0 < g$ and $\{y; y$ ranges over complex numbers: $|y - z_0| < g\} \subseteq$ it.

Next we state three propositions:

(15) For every real number g such that $0 < g$ holds $\{y; y$ ranges over complex numbers: $|y - z_0| < g\}$ is a neighbourhood of z_0.

(16) For every neighbourhood N of z_0 holds $z_0 \in N$.

(17) Let z_0 be a complex number and N_2, N_3 be neighbourhoods of z_0. Then there exists a neighbourhood N of z_0 such that $N \subseteq N_2$ and $N \subseteq N_3$.

Let us consider f and let x_0 be a complex number. We say that f is differentiable in x_0 if and only if the condition (Def. 5) is satisfied.

(Def. 5) There exists a neighbourhood N of x_0 such that $N \subseteq \operatorname{dom} f$ and there exist L, R such that for every complex number x such that $x \in N$ holds $f_x - f_{x_0} = L_{x-x_0} + R_{x-x_0}$.

Let us consider f and let z_0 be a complex number. Let us assume that f is differentiable in z_0. The functor $f'(z_0)$ yielding a complex number is defined by the condition (Def. 6).

(Def. 6) There exists a neighbourhood N of z_0 such that $N \subseteq \operatorname{dom} f$ and there exist L, R such that $f'(z_0) = L_{1_{\mathbb{C}}}$ and for every complex number z such that $z \in N$ holds $f_z - f_{z_0} = L_{z-z_0} + R_{z-z_0}$.

Let us consider f, X. We say that f is differentiable on X if and only if:

(Def. 7) $X \subseteq \operatorname{dom} f$ and for every x such that $x \in X$ holds $f{\restriction}X$ is differentiable in x.

We now state the proposition

(18) If f is differentiable on X, then X is a subset of $\mathbb{C}$.

Let X be a subset of $\mathbb{C}$. We say that X is closed if and only if:

(Def. 8) For every complex sequence s_3 such that $\operatorname{rng} s_3 \subseteq X$ and s_3 is convergent holds $\lim s_3 \in X$.

Let X be a subset of $\mathbb{C}$. We say that X is open if and only if:

(Def. 9) X^{c} is closed.

Next we state several propositions:

(19) Let X be a subset of $\mathbb{C}$. Suppose X is open. Let z_0 be a complex number. If $z_0 \in X$, then there exists a neighbourhood N of z_0 such that $N \subseteq X$.

(20) Let X be a subset of $\mathbb{C}$. Suppose X is open. Let z_0 be a complex number. Suppose $z_0 \in X$. Then there exists a real number g such that $\{y; y$ ranges over complex numbers: $|y - z_0| < g\} \subseteq X$.

(21) Let X be a subset of $\mathbb{C}$. Suppose that for every complex number z_0 such that $z_0 \in X$ there exists a neighbourhood N of z_0 such that $N \subseteq X$. Then X is open.

(22) Let X be a subset of $\mathbb{C}$. Then X is open if and only if for every complex number x such that $x \in X$ there exists a neighbourhood N of x such that $N \subseteq X$.

(23) Let X be a subset of $\mathbb{C}$, z_0 be an element of $\mathbb{C}$, and r be an element of $\mathbb{R}$. If $X = \{y; y$ ranges over complex numbers: $|y - z_0| < r\}$, then X is open.

(24) Let X be a subset of $\mathbb{C}$, z_0 be an element of $\mathbb{C}$, and r be an element of $\mathbb{R}$. If $X = \{y; y$ ranges over complex numbers: $|y - z_0| \leq r\}$, then X is closed.

Let us note that there exists a subset of $\mathbb{C}$ which is open.

In the sequel Z denotes an open subset of $\mathbb{C}$.

Next we state two propositions:

(25) f is differentiable on Z iff $Z \subseteq \operatorname{dom} f$ and for every x such that $x \in Z$ holds f is differentiable in x.

(26) If f is differentiable on Y, then Y is open.

Let us consider f, X. Let us assume that f is differentiable on X. The functor $f'_{\restriction X}$ yielding a partial function from $\mathbb{C}$ to $\mathbb{C}$ is defined by:

(Def. 10) $\operatorname{dom}(f'_{\restriction X}) = X$ and for every x such that $x \in X$ holds $(f'_{\restriction X})_x = f'(x)$.

The following propositions are true:

(27) Let given f, Z. Suppose $Z \subseteq \operatorname{dom} f$ and there exists a_1 such that $\operatorname{rng} f = \{a_1\}$. Then f is differentiable on Z and for every x such that $x \in Z$ holds $(f'_{\restriction Z})_x = 0_{\mathbb{C}}$.

(28) If s_1 is non-zero, then $s_1 \uparrow k$ is non-zero.

Let us consider h, n. Note that $h \uparrow n$ is convergent to 0.

Let us consider c, n. Note that $c \uparrow n$ is constant.

Next we state a number of propositions:

(29) $(s_1 + s_2) \uparrow k = s_1 \uparrow k + s_2 \uparrow k$.

(30) $(s_1 - s_2) \uparrow k = s_1 \uparrow k - s_2 \uparrow k$.

(31) ${s_1}^{-1} \uparrow k = (s_1 \uparrow k)^{-1}$.

(32) $(s_1\, s_2) \uparrow k = (s_1 \uparrow k)\, (s_2 \uparrow k)$.

(33) Let x_0 be a complex number and N be a neighbourhood of x_0. Suppose f is differentiable in x_0 and $N \subseteq \operatorname{dom} f$. Let given h, c. Suppose $\operatorname{rng} c = \{x_0\}$ and $\operatorname{rng}(h + c) \subseteq N$. Then $h^{-1}\, (f \cdot (h + c) - f \cdot c)$ is convergent and $f'(x_0) = \lim(h^{-1}\, (f \cdot (h + c) - f \cdot c))$.

(34) Let given f_1, f_2, x_0. Suppose f_1 is differentiable in x_0 and f_2 is differentiable in x_0. Then $f_1 + f_2$ is differentiable in x_0 and $(f_1 + f_2)'(x_0) = {f_1}'(x_0) + {f_2}'(x_0)$.

(35) Let given f_1, f_2, x_0. Suppose f_1 is differentiable in x_0 and f_2 is differentiable in x_0. Then $f_1 - f_2$ is differentiable in x_0 and $(f_1 - f_2)'(x_0) = {f_1}'(x_0) - {f_2}'(x_0)$.

(36) For all a, f, x_0 such that f is differentiable in x_0 holds $a\,f$ is differentiable in x_0 and $(a\,f)'(x_0) = a \cdot f'(x_0)$.

(37) Let given f_1, f_2, x_0. Suppose f_1 is differentiable in x_0 and f_2 is differentiable in x_0. Then $f_1\,f_2$ is differentiable in x_0 and $(f_1\,f_2)'(x_0) = (f_2)_{x_0} \cdot {f_1}'(x_0) + (f_1)_{x_0} \cdot {f_2}'(x_0)$.

(38) For all f, Z such that $Z \subseteq \mathrm{dom}\, f$ and $f \restriction Z = \mathrm{id}_Z$ holds f is differentiable on Z and for every x such that $x \in Z$ holds $(f'_{\restriction Z})_x = 1_{\mathbb{C}}$.

(39) Let given f_1, f_2, Z. Suppose $Z \subseteq \mathrm{dom}(f_1 + f_2)$ and f_1 is differentiable on Z and f_2 is differentiable on Z. Then $f_1 + f_2$ is differentiable on Z and for every x such that $x \in Z$ holds $((f_1 + f_2)'_{\restriction Z})_x = {f_1}'(x) + {f_2}'(x)$.

(40) Let given f_1, f_2, Z. Suppose $Z \subseteq \mathrm{dom}(f_1 - f_2)$ and f_1 is differentiable on Z and f_2 is differentiable on Z. Then $f_1 - f_2$ is differentiable on Z and for every x such that $x \in Z$ holds $((f_1 - f_2)'_{\restriction Z})_x = {f_1}'(x) - {f_2}'(x)$.

(41) Let given a, f, Z. Suppose $Z \subseteq \mathrm{dom}(a\,f)$ and f is differentiable on Z. Then $a\,f$ is differentiable on Z and for every x such that $x \in Z$ holds $((a\,f)'_{\restriction Z})_x = a \cdot f'(x)$.

(42) Let given f_1, f_2, Z. Suppose $Z \subseteq \mathrm{dom}(f_1\,f_2)$ and f_1 is differentiable on Z and f_2 is differentiable on Z. Then $f_1\,f_2$ is differentiable on Z and for every x such that $x \in Z$ holds $((f_1\,f_2)'_{\restriction Z})_x = (f_2)_x \cdot {f_1}'(x) + (f_1)_x \cdot {f_2}'(x)$.

(43) If $Z \subseteq \mathrm{dom}\, f$ and f is a constant on Z, then f is differentiable on Z and for every x such that $x \in Z$ holds $(f'_{\restriction Z})_x = 0_{\mathbb{C}}$.

(44) Suppose $Z \subseteq \mathrm{dom}\, f$ and for every x such that $x \in Z$ holds $f_x = a \cdot x + b$. Then f is differentiable on Z and for every x such that $x \in Z$ holds $(f'_{\restriction Z})_x = a$.

(45) For every complex number x_0 such that f is differentiable in x_0 holds f is continuous in x_0.

(46) If f is differentiable on X, then f is continuous on X.

(47) If f is differentiable on X and $Z \subseteq X$, then f is differentiable on Z.

(48) If s_1 is convergent, then $|s_1|$ is convergent.

(49) If f is differentiable in x_0, then there exists R such that $R_{0_{\mathbb{C}}} = 0_{\mathbb{C}}$ and R is continuous in $0_{\mathbb{C}}$.

References

[1] Agnieszka Banachowicz and Anna Winnicka. Complex sequences. *Formalized Mathematics*, 4(**1**):121–124, 1993.

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

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

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

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

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

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

[10] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.

[11] Jarosław Kotowicz. Partial functions from a domain to a domain. *Formalized Mathematics*, 1(**4**):697–702, 1990.

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

[13] Takashi Mitsuishi, Katsumi Wasaki, and Yasunari Shidama. Property of complex sequence and continuity of complex function. *Formalized Mathematics*, 9(**1**):185–190, 2001.

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

[15] Yasunari Shidama and Artur Korniłowicz. Convergence and the limit of complex sequences. Series. *Formalized Mathematics*, 6(**3**):403–410, 1997.

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

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

Received November 4, 2008

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 73–77, 2009

Kolmogorov's Zero-One Law

Agnes Doll
Ludwig Maximilian University of Munich
Germany

Summary. This article presents the proof of Kolmogorov's zero-one law in probability theory. The independence of a family of σ-fields is defined and basic theorems on it are given.

MML identifier: KOLMOG01, version: 7.11.01 4.117.1046

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

For simplicity, we adopt the following convention: Ω, I are non empty sets, $\mathcal{F}$ is a σ-field of subsets of Ω, P is a probability on $\mathcal{F}$, D, E, F are families of subsets of Ω, A, B, s are non empty subsets of $\mathcal{F}$, b is an element of B, a is an element of $\mathcal{F}$, p, q, u, v are events of $\mathcal{F}$, n is an element of $\mathbb{N}$, and i is a set.

Next we state three propositions:

(1) For every function f and for every set X such that $X \subseteq \operatorname{dom} f$ holds if $X \neq \emptyset$, then $\operatorname{rng}(f \restriction X) \neq \emptyset$.

(2) For every real number r such that $r \cdot r = r$ holds $r = 0$ or $r = 1$.

(3) For every family X of subsets of Ω such that $X = \emptyset$ holds $\sigma(X) = \{\emptyset, \Omega\}$.

Let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, let B be a subset of $\mathcal{F}$, and let P be a probability on $\mathcal{F}$. The functor $\operatorname{Indep}(B, P)$ yielding a subset of $\mathcal{F}$ is defined as follows:

(Def. 1) For every element a of $\mathcal{F}$ holds $a \in \operatorname{Indep}(B, P)$ iff for every element b of B holds $P(a \cap b) = P(a) \cdot P(b)$.

Next we state several propositions:

(4) Let f be a sequence of subsets of $\mathcal{F}$. Suppose for all n, b holds $P(f(n) \cap b) = P(f(n)) \cdot P(b)$ and f is disjoint valued. Then $P(b \cap \bigcup f) = P(b) \cdot P(\bigcup f)$.

ISSN 1426–2630(p), 1898-9934(e)

(5) Indep(B, P) is a Dynkin system of Ω.

(6) For every family A of subsets of Ω such that A is intersection stable and $A \subseteq$ Indep(B, P) holds $\sigma(A) \subseteq$ Indep(B, P).

(7) Let A, B be non empty subsets of $\mathcal{F}$. Then $A \subseteq$ Indep(B, P) if and only if for all p, q such that $p \in A$ and $q \in B$ holds p and q are independent w.r.t. P.

(8) For all non empty subsets A, B of $\mathcal{F}$ such that $A \subseteq$ Indep(B, P) holds $B \subseteq$ Indep(A, P).

(9) Let A be a family of subsets of Ω. Suppose A is a non empty subset of $\mathcal{F}$ and intersection stable. Let B be a non empty subset of $\mathcal{F}$. Suppose B is intersection stable. If $A \subseteq$ Indep(B, P), then for all D, s such that $D = B$ and $\sigma(D) = s$ holds $\sigma(A) \subseteq$ Indep(s, P).

(10) Let given E, F. Suppose that

(i) E is a non empty subset of $\mathcal{F}$ and intersection stable, and

(ii) F is a non empty subset of $\mathcal{F}$ and intersection stable.

Suppose that for all p, q such that $p \in E$ and $q \in F$ holds p and q are independent w.r.t. P. Let given u, v. If $u \in \sigma(E)$ and $v \in \sigma(F)$, then u and v are independent w.r.t. P.

Let I be a set, let Ω be a non empty set, and let $\mathcal{F}$ be a σ-field of subsets of Ω. A function from I into $2^{\mathcal{F}}$ is said to be a many sorted σ-field over I and $\mathcal{F}$ if:

(Def. 2) For every i such that $i \in I$ holds it(i) is a σ-field of subsets of Ω.

Let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, let P be a probability on $\mathcal{F}$, let I be a set, and let A be a function from I into $\mathcal{F}$. We say that A is independent w.r.t. P if and only if:

(Def. 3) For every one-to-one finite sequence e of elements of I such that $e \neq \emptyset$ holds $\prod(P \cdot A \cdot e) = P(\bigcap \mathrm{rng}(A \cdot e))$.

Let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, let I be a set, let J be a subset of I, and let F be a many sorted σ-field over I and $\mathcal{F}$. A function from J into $\mathcal{F}$ is said to be a σ-section over J and F if:

(Def. 4) For every i such that $i \in J$ holds it$(i) \in F(i)$.

Let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, let P be a probability on $\mathcal{F}$, let I be a set, and let F be a many sorted σ-field over I and $\mathcal{F}$. We say that F is independent w.r.t. P if and only if:

(Def. 5) For every finite subset E of I holds every σ-section over E and F is independent w.r.t. P.

Let I be a set, let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, let F be a many sorted σ-field over I and $\mathcal{F}$, and let J be a subset of I. Then $F \restriction J$ is a function from J into $2^{\mathcal{F}}$.

Let I be a set, let J be a subset of I, let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, and let F be a function from J into $2^{\mathcal{F}}$. Then $\bigcup F$ is a family of subsets of Ω.

Let I be a set, let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, let F be a many sorted σ-field over I and $\mathcal{F}$, and let J be a subset of I. The functor $\mathrm{sigUn}(F, J)$ yields a σ-field of subsets of Ω and is defined as follows:

(Def. 6) $\mathrm{sigUn}(F, J) = \sigma(\bigcup(F \restriction J))$.

Let I be a set, let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, and let F be a many sorted σ-field over I and $\mathcal{F}$. The functor $\mathrm{futSigmaFields}(F, I)$ yielding a family of subsets of 2^{Ω} is defined as follows:

(Def. 7) For every family S of subsets of Ω holds $S \in \mathrm{futSigmaFields}(F, I)$ iff there exists a finite subset E of I such that $S = \mathrm{sigUn}(F, I \setminus E)$.

Let I be a set, let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, and let F be a many sorted σ-field over I and $\mathcal{F}$. Note that $\mathrm{futSigmaFields}(F, I)$ is non empty.

Let I be a set, let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, and let F be a many sorted σ-field over I and $\mathcal{F}$. The functor $\mathrm{tailSigmaField}(F, I)$ yielding a family of subsets of Ω is defined as follows:

(Def. 8) $\mathrm{tailSigmaField}(F, I) = \bigcap \mathrm{futSigmaFields}(F, I)$.

Let I be a set, let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, and let F be a many sorted σ-field over I and $\mathcal{F}$. Note that $\mathrm{tailSigmaField}(F, I)$ is non empty.

Let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, let I be a non empty set, let J be a non empty subset of I, and let F be a many sorted σ-field over I and $\mathcal{F}$. The functor $\mathrm{MeetSections}(J, F)$ yields a family of subsets of Ω and is defined by the condition (Def. 9).

(Def. 9) Let x be a subset of Ω. Then $x \in \mathrm{MeetSections}(J, F)$ if and only if there exists a non empty finite subset E of I and there exists a σ-section f over E and F such that $E \subseteq J$ and $x = \bigcap \mathrm{rng}\, f$.

One can prove the following propositions:

(11) For every many sorted σ-field F over I and $\mathcal{F}$ and for every non empty subset J of I holds $\sigma(\mathrm{MeetSections}(J, F)) = \mathrm{sigUn}(F, J)$.

(12) Let F be a many sorted σ-field over I and $\mathcal{F}$ and J, K be non empty subsets of I. Suppose F is independent w.r.t. P and J misses K. Let a, c be subsets of Ω. If $a \in \mathrm{MeetSections}(J, F)$ and $c \in \mathrm{MeetSections}(K, F)$, then $P(a \cap c) = P(a) \cdot P(c)$.

(13) Let F be a many sorted σ-field over I and $\mathcal{F}$ and J be a non empty subset of I. Then $\mathrm{MeetSections}(J, F)$ is a non empty subset of $\mathcal{F}$.

Let us consider I, Ω, $\mathcal{F}$, let F be a many sorted σ-field over I and $\mathcal{F}$, and let J be a non empty subset of I. Observe that $\mathrm{MeetSections}(J, F)$ is intersection stable.

The following proposition is true

(14) Let F be a many sorted σ-field over I and $\mathcal{F}$ and J, K be non empty subsets of I. Suppose F is independent w.r.t. P and J misses K. Let given u, v. If $u \in \mathrm{sigUn}(F, J)$ and $v \in \mathrm{sigUn}(F, K)$, then $P(u \cap v) = P(u) \cdot P(v)$.

Let I be a set, let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, and let F be a many sorted σ-field over I and $\mathcal{F}$. The functor $\mathrm{finSigmaFields}(F, I)$ yielding a family of subsets of Ω is defined as follows:

(Def. 10) For every subset S of Ω holds $S \in \mathrm{finSigmaFields}(F, I)$ iff there exists a finite subset E of I such that $S \in \mathrm{sigUn}(F, E)$.

One can prove the following propositions:

(15) For every many sorted σ-field F over I and $\mathcal{F}$ holds $\mathrm{tailSigmaField}(F, I)$ is a σ-field of subsets of Ω.

(16) Let F be a many sorted σ-field over I and $\mathcal{F}$. If F is independent w.r.t. P and $a \in \mathrm{tailSigmaField}(F, I)$, then $P(a) = 0$ or $P(a) = 1$.

Acknowledgments

The author wishes to express her sincere appreciation to Prof. F. Merkl for his kind support and encouragement during the course of this work.

References

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

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

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

[4] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.

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

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

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

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

[9] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

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

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

[12] Franz Merkl. Dynkin's lemma in measure theory. *Formalized Mathematics*, 9(**3**):591–595, 2001.

[13] Andrzej Nędzusiak. Probability. *Formalized Mathematics*, 1(**4**):745–749, 1990.

[14] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.

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

[16] Alexander Yu. Shibakov and Andrzej Trybulec. The Cantor set. *Formalized Mathematics*, 5(**2**):233–236, 1996.

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

[18] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.

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

[20] 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.

Received November 4, 2008

FORMALIZED MATHEMATICS
Vol. **17**, No. **2**, Pages 79–87, **2009**

Second-Order Partial Differentiation of Real Binary Functions

Bing Xie
Qingdao University of Science
and Technology
China

Xiquan Liang
Qingdao University of Science
and Technology
China

Xiuzhuan Shen
Qingdao University of Science
and Technology
China

Summary. In this article we define second-order partial differentiation of real binary functions and discuss the relation of second-order partial derivatives and partial derivatives defined in [17].

MML identifier: `PDIFF_3`, version: `7.11.01 4.117.1046`

The papers [15], [3], [4], [16], [5], [10], [1], [8], [11], [9], [2], [14], [6], [13], [12], [7], and [17] provide the terminology and notation for this paper.

1. Second-Order Partial Derivatives

For simplicity, we adopt the following rules: x, x_0, y, y_0, r denote real numbers, z, z_0 denote elements of $\mathcal{R}^2$, f, f_1, f_2 denote partial functions from $\mathcal{R}^2$ to $\mathbb{R}$, R denotes a rest, and L denotes a linear function.

One can check that every rest is total.

Let f be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and let z be an element of $\mathcal{R}^2$. The functor pdiff1(f, z) yielding a function from $\mathcal{R}^2$ into $\mathbb{R}$ is defined by:

(Def. 1) For every z such that $z \in \mathcal{R}^2$ holds $(\mathrm{pdiff1}(f, z))(z) = \mathrm{partdiff1}(f, z)$.

The functor pdiff2(f, z) yields a function from $\mathcal{R}^2$ into $\mathbb{R}$ and is defined as follows:

ISSN 1426–2630(p), 1898-9934(e)

(Def. 2) For every z such that $z \in \mathcal{R}^2$ holds $(\mathrm{pdiff2}(f, z))(z) = \mathrm{partdiff2}(f, z)$.

Let f be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and let z be an element of $\mathcal{R}^2$. We say that f is partial differentiable on 1st-1st coordinate in z if and only if the condition (Def. 3) is satisfied.

(Def. 3) There exist real numbers x_0, y_0 such that

(i) $z = \langle x_0, y_0 \rangle$, and

(ii) there exists a neighbourhood N of x_0 such that $N \subseteq \mathrm{dom}\,\mathrm{SVF1}(\mathrm{pdiff1}(f, z), z)$ and there exist L, R such that for every x such that $x \in N$ holds $(\mathrm{SVF1}(\mathrm{pdiff1}(f, z), z))(x) - (\mathrm{SVF1}(\mathrm{pdiff1}(f, z), z))(x_0) = L(x - x_0) + R(x - x_0)$.

We say that f is partial differentiable on 1st-2nd coordinate in z if and only if the condition (Def. 4) is satisfied.

(Def. 4) There exist real numbers x_0, y_0 such that

(i) $z = \langle x_0, y_0 \rangle$, and

(ii) there exists a neighbourhood N of y_0 such that $N \subseteq \mathrm{dom}\,\mathrm{SVF2}(\mathrm{pdiff1}(f, z), z)$ and there exist L, R such that for every y such that $y \in N$ holds $(\mathrm{SVF2}(\mathrm{pdiff1}(f, z), z))(y) - (\mathrm{SVF2}(\mathrm{pdiff1}(f, z), z))(y_0) = L(y - y_0) + R(y - y_0)$.

We say that f is partial differentiable on 2nd-1st coordinate in z if and only if the condition (Def. 5) is satisfied.

(Def. 5) There exist real numbers x_0, y_0 such that

(i) $z = \langle x_0, y_0 \rangle$, and

(ii) there exists a neighbourhood N of x_0 such that $N \subseteq \mathrm{dom}\,\mathrm{SVF1}(\mathrm{pdiff2}(f, z), z)$ and there exist L, R such that for every x such that $x \in N$ holds $(\mathrm{SVF1}(\mathrm{pdiff2}(f, z), z))(x) - (\mathrm{SVF1}(\mathrm{pdiff2}(f, z), z))(x_0) = L(x - x_0) + R(x - x_0)$.

We say that f is partial differentiable on 2nd-2nd coordinate in z if and only if the condition (Def. 6) is satisfied.

(Def. 6) There exist real numbers x_0, y_0 such that

(i) $z = \langle x_0, y_0 \rangle$, and

(ii) there exists a neighbourhood N of y_0 such that $N \subseteq \mathrm{dom}\,\mathrm{SVF2}(\mathrm{pdiff2}(f, z), z)$ and there exist L, R such that for every y such that $y \in N$ holds $(\mathrm{SVF2}(\mathrm{pdiff2}(f, z), z))(y) - (\mathrm{SVF2}(\mathrm{pdiff2}(f, z), z))(y_0) = L(y - y_0) + R(y - y_0)$.

Let f be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and let z be an element of $\mathcal{R}^2$. Let us assume that f is partial differentiable on 1st-1st coordinate in z. The functor $\mathrm{hpartdiff11}(f, z)$ yielding a real number is defined by the condition (Def. 7).

(Def. 7) There exist real numbers x_0, y_0 such that

(i) $z = \langle x_0, y_0 \rangle$, and

(ii) there exists a neighbourhood N of x_0 such that $N \subseteq \operatorname{dom} \mathrm{SVF1}(\mathrm{pdiff1}(f,z),z)$ and there exist L, R such that $\mathrm{hpartdiff11}(f,z) = L(1)$ and for every x such that $x \in N$ holds $(\mathrm{SVF1}(\mathrm{pdiff1}(f,z),z))(x) - (\mathrm{SVF1}(\mathrm{pdiff1}(f,z),z))(x_0) = L(x - x_0) + R(x - x_0)$.

Let f be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and let z be an element of $\mathcal{R}^2$. Let us assume that f is partial differentiable on 1st-2nd coordinate in z. The functor $\mathrm{hpartdiff12}(f,z)$ yielding a real number is defined by the condition (Def. 8).

(Def. 8) There exist real numbers x_0, y_0 such that

(i) $z = \langle x_0, y_0 \rangle$, and

(ii) there exists a neighbourhood N of y_0 such that $N \subseteq \operatorname{dom} \mathrm{SVF2}(\mathrm{pdiff1}(f,z),z)$ and there exist L, R such that $\mathrm{hpartdiff12}(f,z) = L(1)$ and for every y such that $y \in N$ holds $(\mathrm{SVF2}(\mathrm{pdiff1}(f,z),z))(y) - (\mathrm{SVF2}(\mathrm{pdiff1}(f,z),z))(y_0) = L(y - y_0) + R(y - y_0)$.

Let f be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and let z be an element of $\mathcal{R}^2$. Let us assume that f is partial differentiable on 2nd-1st coordinate in z. The functor $\mathrm{hpartdiff21}(f,z)$ yields a real number and is defined by the condition (Def. 9).

(Def. 9) There exist real numbers x_0, y_0 such that

(i) $z = \langle x_0, y_0 \rangle$, and

(ii) there exists a neighbourhood N of x_0 such that $N \subseteq \operatorname{dom} \mathrm{SVF1}(\mathrm{pdiff2}(f,z),z)$ and there exist L, R such that $\mathrm{hpartdiff21}(f,z) = L(1)$ and for every x such that $x \in N$ holds $(\mathrm{SVF1}(\mathrm{pdiff2}(f,z),z))(x) - (\mathrm{SVF1}(\mathrm{pdiff2}(f,z),z))(x_0) = L(x - x_0) + R(x - x_0)$.

Let f be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and let z be an element of $\mathcal{R}^2$. Let us assume that f is partial differentiable on 2nd-2nd coordinate in z. The functor $\mathrm{hpartdiff22}(f,z)$ yielding a real number is defined by the condition (Def. 10).

(Def. 10) There exist real numbers x_0, y_0 such that

(i) $z = \langle x_0, y_0 \rangle$, and

(ii) there exists a neighbourhood N of y_0 such that $N \subseteq \operatorname{dom} \mathrm{SVF2}(\mathrm{pdiff2}(f,z),z)$ and there exist L, R such that $\mathrm{hpartdiff22}(f,z) = L(1)$ and for every y such that $y \in N$ holds $(\mathrm{SVF2}(\mathrm{pdiff2}(f,z),z))(y) - (\mathrm{SVF2}(\mathrm{pdiff2}(f,z),z))(y_0) = L(y - y_0) + R(y - y_0)$.

The following propositions are true:

(1) If $z = \langle x_0, y_0 \rangle$ and f is partial differentiable on 1st-1st coordinate in z, then $\mathrm{SVF1}(\mathrm{pdiff1}(f,z),z)$ is differentiable in x_0.

(2) If $z = \langle x_0, y_0 \rangle$ and f is partial differentiable on 1st-2nd coordinate in z, then $\mathrm{SVF2}(\mathrm{pdiff1}(f,z),z)$ is differentiable in y_0.

(3) If $z = \langle x_0, y_0 \rangle$ and f is partial differentiable on 2nd-1st coordinate in z, then $\mathrm{SVF1}(\mathrm{pdiff2}(f,z),z)$ is differentiable in x_0.

(4) If $z = \langle x_0, y_0 \rangle$ and f is partial differentiable on 2nd-2nd coordinate in z, then SVF2(pdiff2(f, z), z) is differentiable in y_0.

(5) If $z = \langle x_0, y_0 \rangle$ and f is partial differentiable on 1st-1st coordinate in z, then hpartdiff11(f, z) = (SVF1(pdiff1(f, z), z))$'(x_0)$.

(6) If $z = \langle x_0, y_0 \rangle$ and f is partial differentiable on 1st-2nd coordinate in z, then hpartdiff12(f, z) = (SVF2(pdiff1(f, z), z))$'(y_0)$.

(7) If $z = \langle x_0, y_0 \rangle$ and f is partial differentiable on 2nd-1st coordinate in z, then hpartdiff21(f, z) = (SVF1(pdiff2(f, z), z))$'(x_0)$.

(8) If $z = \langle x_0, y_0 \rangle$ and f is partial differentiable on 2nd-2nd coordinate in z, then hpartdiff22(f, z) = (SVF2(pdiff2(f, z), z))$'(y_0)$.

Let f be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and let Z be a set. We say that f is partial differentiable on 1st-1st coordinate on Z if and only if:

(Def. 11) $Z \subseteq \operatorname{dom} f$ and for every element z of $\mathcal{R}^2$ such that $z \in Z$ holds $f{\restriction}Z$ is partial differentiable on 1st-1st coordinate in z.

We say that f is partial differentiable on 1st-2nd coordinate on Z if and only if:

(Def. 12) $Z \subseteq \operatorname{dom} f$ and for every element z of $\mathcal{R}^2$ such that $z \in Z$ holds $f{\restriction}Z$ is partial differentiable on 1st-2nd coordinate in z.

We say that f is partial differentiable on 2nd-1st coordinate on Z if and only if:

(Def. 13) $Z \subseteq \operatorname{dom} f$ and for every element z of $\mathcal{R}^2$ such that $z \in Z$ holds $f{\restriction}Z$ is partial differentiable on 2nd-1st coordinate in z.

We say that f is partial differentiable on 2nd-2nd coordinate on Z if and only if:

(Def. 14) $Z \subseteq \operatorname{dom} f$ and for every element z of $\mathcal{R}^2$ such that $z \in Z$ holds $f{\restriction}Z$ is partial differentiable on 2nd-2nd coordinate in z.

Let f be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and let Z be a set. Let us assume that f is partial differentiable on 1st-1st coordinate on Z. The functor $f_{\restriction Z}^{\mathrm{1st}-\mathrm{1st}}$ yielding a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ is defined as follows:

(Def. 15) $\operatorname{dom}(f_{\restriction Z}^{\mathrm{1st}-\mathrm{1st}}) = Z$ and for every element z of $\mathcal{R}^2$ such that $z \in Z$ holds $f_{\restriction Z}^{\mathrm{1st}-\mathrm{1st}}(z) = \text{hpartdiff11}(f, z)$.

Let f be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and let Z be a set. Let us assume that f is partial differentiable on 1st-2nd coordinate on Z. The functor $f_{\restriction Z}^{\mathrm{1st}-\mathrm{2nd}}$ yielding a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ is defined by:

(Def. 16) $\operatorname{dom}(f_{\restriction Z}^{\mathrm{1st}-\mathrm{2nd}}) = Z$ and for every element z of $\mathcal{R}^2$ such that $z \in Z$ holds $f_{\restriction Z}^{\mathrm{1st}-\mathrm{2nd}}(z) = \text{hpartdiff12}(f, z)$.

Let f be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and let Z be a set. Let us assume that f is partial differentiable on 2nd-1st coordinate on Z. The functor $f_{\restriction Z}^{\mathrm{2nd}-\mathrm{1st}}$ yields a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and is defined by:

(Def. 17) $\mathrm{dom}(f{\restriction}_Z^{\mathrm{2nd-1st}}) = Z$ and for every element z of $\mathcal{R}^2$ such that $z \in Z$ holds $f{\restriction}_Z^{\mathrm{2nd-1st}}(z) = \mathrm{hpartdiff21}(f, z)$.

Let f be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and let Z be a set. Let us assume that f is partial differentiable on 2nd-2nd coordinate on Z. The functor $f{\restriction}_Z^{\mathrm{2nd-2nd}}$ yields a partial function from $\mathcal{R}^2$ to $\mathbb{R}$ and is defined by:

(Def. 18) $\mathrm{dom}(f{\restriction}_Z^{\mathrm{2nd-2nd}}) = Z$ and for every element z of $\mathcal{R}^2$ such that $z \in Z$ holds $f{\restriction}_Z^{\mathrm{2nd-2nd}}(z) = \mathrm{hpartdiff22}(f, z)$.

2. Main Properties of Second-Order Partial Derivatives

Next we state a number of propositions:

(9) f is partial differentiable on 1st-1st coordinate in z if and only if $\mathrm{pdiff1}(f, z)$ is partial differentiable on 1st coordinate in z.

(10) f is partial differentiable on 1st-2nd coordinate in z if and only if $\mathrm{pdiff1}(f, z)$ is partial differentiable on 2nd coordinate in z.

(11) f is partial differentiable on 2nd-1st coordinate in z if and only if $\mathrm{pdiff2}(f, z)$ is partial differentiable on 1st coordinate in z.

(12) f is partial differentiable on 2nd-2nd coordinate in z if and only if $\mathrm{pdiff2}(f, z)$ is partial differentiable on 2nd coordinate in z.

(13) f is partial differentiable on 1st-1st coordinate in z if and only if $\mathrm{pdiff1}(f, z)$ is partially differentiable in z w.r.t. coordinate 1.

(14) f is partial differentiable on 1st-2nd coordinate in z if and only if $\mathrm{pdiff1}(f, z)$ is partially differentiable in z w.r.t. coordinate 2.

(15) f is partial differentiable on 2nd-1st coordinate in z if and only if $\mathrm{pdiff2}(f, z)$ is partially differentiable in z w.r.t. coordinate 1.

(16) f is partial differentiable on 2nd-2nd coordinate in z if and only if $\mathrm{pdiff2}(f, z)$ is partially differentiable in z w.r.t. coordinate 2.

(17) If f is partial differentiable on 1st-1st coordinate in z, then $\mathrm{hpartdiff11}(f, z) = \mathrm{partdiff1}(\mathrm{pdiff1}(f, z), z)$.

(18) If f is partial differentiable on 1st-2nd coordinate in z, then $\mathrm{hpartdiff12}(f, z) = \mathrm{partdiff2}(\mathrm{pdiff1}(f, z), z)$.

(19) If f is partial differentiable on 2nd-1st coordinate in z, then $\mathrm{hpartdiff21}(f, z) = \mathrm{partdiff1}(\mathrm{pdiff2}(f, z), z)$.

(20) If f is partial differentiable on 2nd-2nd coordinate in z, then $\mathrm{hpartdiff22}(f, z) = \mathrm{partdiff2}(\mathrm{pdiff2}(f, z), z)$.

(21) Let z_0 be an element of $\mathcal{R}^2$ and N be a neighbourhood of $(\mathrm{proj}(1, 2))(z_0)$. Suppose f is partial differentiable on 1st-1st coordinate in z_0 and $N \subseteq \mathrm{dom}\,\mathrm{SVF1}(\mathrm{pdiff1}(f, z_0), z_0)$. Let h be a convergent to 0 sequence of real numbers and c be a constant sequence of real numbers. Suppose $\mathrm{rng}\, c =$

$\{(\mathrm{proj}(1,2))(z_0)\}$ and $\mathrm{rng}(h+c) \subseteq N$. Then $h^{-1}\,(\mathrm{SVF1}(\mathrm{pdiff1}(f,z_0),z_0)\cdot(h+c) - \mathrm{SVF1}(\mathrm{pdiff1}(f,z_0),z_0)\cdot c)$ is convergent and $\mathrm{hpartdiff11}(f,z_0) = \lim(h^{-1}\,(\mathrm{SVF1}(\mathrm{pdiff1}(f,z_0),z_0)\cdot(h+c) - \mathrm{SVF1}(\mathrm{pdiff1}(f,z_0),z_0)\cdot c))$.

(22) Let z_0 be an element of $\mathcal{R}^2$ and N be a neighbourhood of $(\mathrm{proj}(2,2))(z_0)$. Suppose f is partial differentiable on 1st-2nd coordinate in z_0 and $N \subseteq \mathrm{dom}\,\mathrm{SVF2}(\mathrm{pdiff1}(f,z_0),z_0)$. Let h be a convergent to 0 sequence of real numbers and c be a constant sequence of real numbers. Suppose $\mathrm{rng}\,c = \{(\mathrm{proj}(2,2))(z_0)\}$ and $\mathrm{rng}(h+c) \subseteq N$. Then $h^{-1}\,(\mathrm{SVF2}(\mathrm{pdiff1}(f,z_0),z_0)\cdot(h+c) - \mathrm{SVF2}(\mathrm{pdiff1}(f,z_0),z_0)\cdot c)$ is convergent and $\mathrm{hpartdiff12}(f,z_0) = \lim(h^{-1}\,(\mathrm{SVF2}(\mathrm{pdiff1}(f,z_0),z_0)\cdot(h+c) - \mathrm{SVF2}(\mathrm{pdiff1}(f,z_0),z_0)\cdot c))$.

(23) Let z_0 be an element of $\mathcal{R}^2$ and N be a neighbourhood of $(\mathrm{proj}(1,2))(z_0)$. Suppose f is partial differentiable on 2nd-1st coordinate in z_0 and $N \subseteq \mathrm{dom}\,\mathrm{SVF1}(\mathrm{pdiff2}(f,z_0),z_0)$. Let h be a convergent to 0 sequence of real numbers and c be a constant sequence of real numbers. Suppose $\mathrm{rng}\,c = \{(\mathrm{proj}(1,2))(z_0)\}$ and $\mathrm{rng}(h+c) \subseteq N$. Then $h^{-1}\,(\mathrm{SVF1}(\mathrm{pdiff2}(f,z_0),z_0)\cdot(h+c) - \mathrm{SVF1}(\mathrm{pdiff2}(f,z_0),z_0)\cdot c)$ is convergent and $\mathrm{hpartdiff21}(f,z_0) = \lim(h^{-1}\,(\mathrm{SVF1}(\mathrm{pdiff2}(f,z_0),z_0)\cdot(h+c) - \mathrm{SVF1}(\mathrm{pdiff2}(f,z_0),z_0)\cdot c))$.

(24) Let z_0 be an element of $\mathcal{R}^2$ and N be a neighbourhood of $(\mathrm{proj}(2,2))(z_0)$. Suppose f is partial differentiable on 2nd-2nd coordinate in z_0 and $N \subseteq \mathrm{dom}\,\mathrm{SVF2}(\mathrm{pdiff2}(f,z_0),z_0)$. Let h be a convergent to 0 sequence of real numbers and c be a constant sequence of real numbers. Suppose $\mathrm{rng}\,c = \{(\mathrm{proj}(2,2))(z_0)\}$ and $\mathrm{rng}(h+c) \subseteq N$. Then $h^{-1}\,(\mathrm{SVF2}(\mathrm{pdiff2}(f,z_0),z_0)\cdot(h+c) - \mathrm{SVF2}(\mathrm{pdiff2}(f,z_0),z_0)\cdot c)$ is convergent and $\mathrm{hpartdiff22}(f,z_0) = \lim(h^{-1}\,(\mathrm{SVF2}(\mathrm{pdiff2}(f,z_0),z_0)\cdot(h+c) - \mathrm{SVF2}(\mathrm{pdiff2}(f,z_0),z_0)\cdot c))$.

(25) Suppose that

(i) f_1 is partial differentiable on 1st-1st coordinate in z_0, and

(ii) f_2 is partial differentiable on 1st-1st coordinate in z_0.

Then $\mathrm{pdiff1}(f_1,z_0)+\mathrm{pdiff1}(f_2,z_0)$ is partial differentiable on 1st coordinate in z_0 and $\mathrm{partdiff1}(\mathrm{pdiff1}(f_1,z_0)+\mathrm{pdiff1}(f_2,z_0),z_0) = \mathrm{hpartdiff11}(f_1,z_0)+\mathrm{hpartdiff11}(f_2,z_0)$.

(26) Suppose that

(i) f_1 is partial differentiable on 1st-2nd coordinate in z_0, and

(ii) f_2 is partial differentiable on 1st-2nd coordinate in z_0.

Then $\mathrm{pdiff1}(f_1,z_0) + \mathrm{pdiff1}(f_2,z_0)$ is partial differentiable on 2nd coordinate in z_0 and $\mathrm{partdiff2}(\mathrm{pdiff1}(f_1,z_0) + \mathrm{pdiff1}(f_2,z_0),z_0) = \mathrm{hpartdiff12}(f_1,z_0) + \mathrm{hpartdiff12}(f_2,z_0)$.

(27) Suppose that

(i) f_1 is partial differentiable on 2nd-1st coordinate in z_0, and

(ii) f_2 is partial differentiable on 2nd-1st coordinate in z_0.

Then $\mathrm{pdiff2}(f_1,z_0)+\mathrm{pdiff2}(f_2,z_0)$ is partial differentiable on 1st coordinate in z_0 and $\mathrm{partdiff1}(\mathrm{pdiff2}(f_1,z_0)+\mathrm{pdiff2}(f_2,z_0),z_0) = \mathrm{hpartdiff21}(f_1,z_0)+$

hpartdiff21(f_2, z_0).

(28) Suppose that

(i) f_1 is partial differentiable on 2nd-2nd coordinate in z_0, and

(ii) f_2 is partial differentiable on 2nd-2nd coordinate in z_0.

Then pdiff2(f_1, z_0) + pdiff2(f_2, z_0) is partial differentiable on 2nd coordinate in z_0 and partdiff2(pdiff2(f_1, z_0) + pdiff2$(f_2, z_0), z_0)$ = hpartdiff22(f_1, z_0) + hpartdiff22(f_2, z_0).

(29) Suppose that

(i) f_1 is partial differentiable on 1st-1st coordinate in z_0, and

(ii) f_2 is partial differentiable on 1st-1st coordinate in z_0.

Then pdiff1(f_1, z_0)−pdiff1(f_2, z_0) is partial differentiable on 1st coordinate in z_0 and partdiff1(pdiff1(f_1, z_0)−pdiff1$(f_2, z_0), z_0)$ = hpartdiff11(f_1, z_0)− hpartdiff11(f_2, z_0).

(30) Suppose that

(i) f_1 is partial differentiable on 1st-2nd coordinate in z_0, and

(ii) f_2 is partial differentiable on 1st-2nd coordinate in z_0.

Then pdiff1(f_1, z_0) − pdiff1(f_2, z_0) is partial differentiable on 2nd coordinate in z_0 and partdiff2(pdiff1(f_1, z_0) − pdiff1$(f_2, z_0), z_0)$ = hpartdiff12(f_1, z_0) − hpartdiff12(f_2, z_0).

(31) Suppose that

(i) f_1 is partial differentiable on 2nd-1st coordinate in z_0, and

(ii) f_2 is partial differentiable on 2nd-1st coordinate in z_0.

Then pdiff2(f_1, z_0)−pdiff2(f_2, z_0) is partial differentiable on 1st coordinate in z_0 and partdiff1(pdiff2(f_1, z_0)−pdiff2$(f_2, z_0), z_0)$ = hpartdiff21(f_1, z_0)− hpartdiff21(f_2, z_0).

(32) Suppose that

(i) f_1 is partial differentiable on 2nd-2nd coordinate in z_0, and

(ii) f_2 is partial differentiable on 2nd-2nd coordinate in z_0.

Then pdiff2(f_1, z_0) − pdiff2(f_2, z_0) is partial differentiable on 2nd coordinate in z_0 and partdiff2(pdiff2(f_1, z_0) − pdiff2$(f_2, z_0), z_0)$ = hpartdiff22(f_1, z_0) − hpartdiff22(f_2, z_0).

(33) Suppose f is partial differentiable on 1st-1st coordinate in z_0. Then r pdiff1(f, z_0) is partial differentiable on 1st coordinate in z_0 and partdiff1(r pdiff1$(f, z_0), z_0)$ = $r \cdot$ hpartdiff11(f, z_0).

(34) Suppose f is partial differentiable on 1st-2nd coordinate in z_0. Then r pdiff1(f, z_0) is partial differentiable on 2nd coordinate in z_0 and partdiff2(r pdiff1$(f, z_0), z_0)$ = $r \cdot$ hpartdiff12(f, z_0).

(35) Suppose f is partial differentiable on 2nd-1st coordinate in z_0. Then r pdiff2(f, z_0) is partial differentiable on 1st coordinate in z_0 and partdiff1(r pdiff2$(f, z_0), z_0)$ = $r \cdot$ hpartdiff21(f, z_0).

(36) Suppose f is partial differentiable on 2nd-2nd coordinate in z_0. Then r pdiff2(f, z_0) is partial differentiable on 2nd coordinate in z_0 and partdiff2$(r$ pdiff2$(f, z_0), z_0) = r \cdot$ hpartdiff22(f, z_0).

(37) Suppose that

(i) f_1 is partial differentiable on 1st-1st coordinate in z_0, and

(ii) f_2 is partial differentiable on 1st-1st coordinate in z_0.

Then pdiff1(f_1, z_0) pdiff1(f_2, z_0) is partial differentiable on 1st coordinate in z_0.

(38) Suppose that

(i) f_1 is partial differentiable on 1st-2nd coordinate in z_0, and

(ii) f_2 is partial differentiable on 1st-2nd coordinate in z_0.

Then pdiff1(f_1, z_0) pdiff1(f_2, z_0) is partial differentiable on 2nd coordinate in z_0.

(39) Suppose that

(i) f_1 is partial differentiable on 2nd-1st coordinate in z_0, and

(ii) f_2 is partial differentiable on 2nd-1st coordinate in z_0.

Then pdiff2(f_1, z_0) pdiff2(f_2, z_0) is partial differentiable on 1st coordinate in z_0.

(40) Suppose that

(i) f_1 is partial differentiable on 2nd-2nd coordinate in z_0, and

(ii) f_2 is partial differentiable on 2nd-2nd coordinate in z_0.

Then pdiff2(f_1, z_0) pdiff2(f_2, z_0) is partial differentiable on 2nd coordinate in z_0.

(41) Let z_0 be an element of $\mathcal{R}^2$. Suppose f is partial differentiable on 1st-1st coordinate in z_0. Then SVF1(pdiff1$(f, z_0), z_0)$ is continuous in (proj$(1, 2))(z_0)$.

(42) Let z_0 be an element of $\mathcal{R}^2$. Suppose f is partial differentiable on 1st-2nd coordinate in z_0. Then SVF2(pdiff1$(f, z_0), z_0)$ is continuous in (proj$(2, 2))(z_0)$.

(43) Let z_0 be an element of $\mathcal{R}^2$. Suppose f is partial differentiable on 2nd-1st coordinate in z_0. Then SVF1(pdiff2$(f, z_0), z_0)$ is continuous in (proj$(1, 2))(z_0)$.

(44) Let z_0 be an element of $\mathcal{R}^2$. Suppose f is partial differentiable on 2nd-2nd coordinate in z_0. Then SVF2(pdiff2$(f, z_0), z_0)$ is continuous in (proj$(2, 2))(z_0)$.

(45) If f is partial differentiable on 1st-1st coordinate in z_0, then there exists R such that $R(0) = 0$ and R is continuous in 0.

(46) If f is partial differentiable on 1st-2nd coordinate in z_0, then there exists R such that $R(0) = 0$ and R is continuous in 0.

(47) If f is partial differentiable on 2nd-1st coordinate in z_0, then there exists R such that $R(0) = 0$ and R is continuous in 0.

(48) If f is partial differentiable on 2nd-2nd coordinate in z_0, then there exists R such that $R(0) = 0$ and R is continuous in 0.

References

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

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

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

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

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

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

[7] Noboru Endou, Yasunari Shidama, and Keiichi Miyajima. Partial differentiation on normed linear spaces $\mathcal{R}^n$. *Formalized Mathematics*, 15(**2**):65–72, 2007, doi:10.2478/v10037-007-0008-5.

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

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

[10] Jarosław Kotowicz. Properties of real functions. *Formalized Mathematics*, 1(**4**):781–786, 1990.

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

[12] Konrad Raczkowski and Paweł Sadowski. Real function continuity. *Formalized Mathematics*, 1(**4**):787–791, 1990.

[13] Konrad Raczkowski and Paweł Sadowski. Real function differentiability. *Formalized Mathematics*, 1(**4**):797–801, 1990.

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

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

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

[17] Bing Xie, Xiquan Liang, and Hongwei Li. Partial differentiation of real binary functions. *Formalized Mathematics*, 16(**4**):333–338, 2008, doi:10.2478/v10037-008-0041-z.

Received December 16, 2008

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 89–97, 2009

The Measurability of Complex-Valued Functional Sequences

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 formalized the measurability of complex-valued functional sequences. First, we proved the measurability of the limits of real-valued functional sequences. Next, we defined complex-valued functional sequences dividing real part into imaginary part. Then using the former theorems, we proved the measurability of each part. Lastly, we proved the measurability of the limits of complex-valued functional sequences. We also showed several properties of complex-valued measurable functions. In addition, we proved properties of complex-valued simple functions.

MML identifier: MESFUN7C, version: 7.11.01 4.117.1046

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

1. Real-Valued Functional Sequences

For simplicity, we adopt the following convention: X denotes a non empty set, Y denotes a set, S denotes a σ-field of subsets of X, M denotes a σ-measure on S, f, g denote partial functions from X to $\mathbb{C}$, r denotes a real number, k denotes a real number, and E denotes an element of S.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{R}$. The functor $\overline{\mathbb{R}}(f)$ yielding a sequence of partial functions from X into $\overline{\mathbb{R}}$ is defined as follows:

ISSN 1426–2630(p), 1898-9934(e)

(Def. 1) $\overline{\mathbb{R}}(f) = f$.

Next we state the proposition

(1) Let X be a non empty set, f be a sequence of partial functions from X into $\mathbb{R}$, and x be an element of X. Then $f\#x = \overline{\mathbb{R}}(f)\#x$.

Let X be a non empty set and let f be a function from X into $\mathbb{R}$. Note that $\overline{\mathbb{R}}(f)$ is total.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{R}$. The functor $\inf f$ yields a partial function from X to $\overline{\mathbb{R}}$ and is defined by:

(Def. 2) $\inf f = \inf \overline{\mathbb{R}}(f)$.

Next we state the proposition

(2) Let X be a non empty set, f be a sequence of partial functions from X into $\mathbb{R}$, and x be an element of X. If $x \in \operatorname{dom} \inf f$, then $(\inf f)(x) = \inf \operatorname{rng} \overline{\mathbb{R}}(f\#x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{R}$. The functor $\sup f$ yielding a partial function from X to $\overline{\mathbb{R}}$ is defined as follows:

(Def. 3) $\sup f = \sup \overline{\mathbb{R}}(f)$.

We now state the proposition

(3) Let X be a non empty set, f be a sequence of partial functions from X into $\mathbb{R}$, and x be an element of X. If $x \in \operatorname{dom} \sup f$, then $(\sup f)(x) = \sup \operatorname{rng} \overline{\mathbb{R}}(f\#x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{R}$. The inferior real sequence of f yields a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom and is defined as follows:

(Def. 4) The inferior real sequence of f = the inferior real sequence of $\overline{\mathbb{R}}(f)$.

One can prove the following proposition

(4) Let X be a non empty set, f be a sequence of partial functions from X into $\mathbb{R}$, and n be a natural number. Then

(i) dom (the inferior real sequence of f)$(n) = \operatorname{dom} f(0)$, and

(ii) for every element x of X such that $x \in$ dom (the inferior real sequence of f)(n) holds (the inferior real sequence of f)$(n)(x)$ = (the inferior real sequence of $\overline{\mathbb{R}}(f\#x))(n)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{R}$. The superior real sequence of f yielding a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom is defined as follows:

(Def. 5) The superior real sequence of f = the superior real sequence of $\overline{\mathbb{R}}(f)$.

One can prove the following two propositions:

(5) Let X be a non empty set, f be a sequence of partial functions from X into $\mathbb{R}$, and n be a natural number. Then

(i) dom (the superior real sequence of $f)(n) = \operatorname{dom} f(0)$, and

(ii) for every element x of X such that $x \in$ dom (the superior real sequence of $f)(n)$ holds (the superior real sequence of $f)(n)(x) =$ (the superior real sequence of $\overline{\mathbb{R}}(f\#x))(n)$.

(6) Let f be a sequence of partial functions from X into $\mathbb{R}$ and x be an element of X. Suppose $x \in \operatorname{dom} f(0)$. Then (the inferior real sequence of $f)\#x =$ the inferior real sequence of $\overline{\mathbb{R}}(f\#x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{R}$ with the same dom. Note that $\overline{\mathbb{R}}(f)$ has the same dom.

One can prove the following propositions:

(7) Let X be a non empty set, f be a sequence of partial functions from X into $\mathbb{R}$ with the same dom, S be a σ-field of subsets of X, E be an element of S, and n be a natural number. If $f(n)$ is measurable on E, then $(\overline{\mathbb{R}}(f))(n)$ is measurable on E.

(8) Let X be a non empty set, f be a sequence of partial functions from X into $\mathbb{R}$, and n be an element of $\mathbb{N}$. Then $\overline{\mathbb{R}}(f) \uparrow n = \overline{\mathbb{R}}(f \uparrow n)$.

(9) Let f be a sequence of partial functions from X into $\mathbb{R}$ with the same dom and n be an element of $\mathbb{N}$. Then (the inferior real sequence of $f)(n) = \inf(f \uparrow n)$.

(10) Let f be a sequence of partial functions from X into $\mathbb{R}$ with the same dom and n be an element of $\mathbb{N}$. Then (the superior real sequence of $f)(n) = \sup(f \uparrow n)$.

(11) Let f be a sequence of partial functions from X into $\mathbb{R}$ and x be an element of X. Suppose $x \in \operatorname{dom} f(0)$. Then (the superior real sequence of $f)\#x =$ the superior real sequence of $\overline{\mathbb{R}}(f\#x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{R}$. The functor $\liminf f$ yielding a partial function from X to $\overline{\mathbb{R}}$ is defined as follows:

(Def. 6) $\liminf f = \liminf \overline{\mathbb{R}}(f)$.

We now state the proposition

(12) Let X be a non empty set, f be a sequence of partial functions from X into $\mathbb{R}$, and x be an element of X. If $x \in \operatorname{dom} \liminf f$, then $(\liminf f)(x) = \liminf \overline{\mathbb{R}}(f\#x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{R}$. The functor $\limsup f$ yielding a partial function from X to $\overline{\mathbb{R}}$ is defined by:

(Def. 7) $\limsup f = \limsup \overline{\mathbb{R}}(f)$.

Next we state the proposition

(13) Let X be a non empty set, f be a sequence of partial functions from X into $\mathbb{R}$, and x be an element of X. If $x \in \operatorname{dom} \limsup f$, then $(\limsup f)(x) = \limsup \overline{\mathbb{R}}(f\#x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{R}$. The functor $\lim f$ yielding a partial function from X to $\overline{\mathbb{R}}$ is defined by:

(Def. 8) $\lim f = \lim \overline{\mathbb{R}}(f)$.

One can prove the following propositions:

(14) Let X be a non empty set, f be a sequence of partial functions from X into $\mathbb{R}$, and x be an element of X. If $x \in \operatorname{dom} \lim f$, then $(\lim f)(x) = \lim \overline{\mathbb{R}}(f\#x)$.

(15) Let f be a sequence of partial functions from X into $\mathbb{R}$ and x be an element of X. If $x \in \operatorname{dom} \lim f$ and $f\#x$ is convergent, then $(\lim f)(x) = (\limsup f)(x)$ and $(\lim f)(x) = (\liminf f)(x)$.

(16) Let f be a sequence of partial functions from X into $\mathbb{R}$ with the same dom, F be a sequence of subsets of S, and r be a real number. Suppose that for every natural number n holds $F(n) = \operatorname{dom} f(0) \cap \text{GT-dom}(f(n), r)$. Then $\bigcup \operatorname{rng} F = \operatorname{dom} f(0) \cap \text{GT-dom}(\sup f, r)$.

(17) Let f be a sequence of partial functions from X into $\mathbb{R}$ with the same dom, F be a sequence of subsets of S, and r be a real number. Suppose that for every natural number n holds $F(n) = \operatorname{dom} f(0) \cap \text{GTE-dom}(f(n), r)$. Then $\bigcap \operatorname{rng} F = \operatorname{dom} f(0) \cap \text{GTE-dom}(\inf f, r)$.

(18) Let f be a sequence of partial functions from X into $\mathbb{R}$ with the same dom and E be an element of S. Suppose $\operatorname{dom} f(0) = E$ and for every natural number n holds $f(n)$ is measurable on E. Then $\limsup f$ is measurable on E.

(19) Let f be a sequence of partial functions from X into $\mathbb{R}$ with the same dom and E be an element of S. Suppose $\operatorname{dom} f(0) = E$ and for every natural number n holds $f(n)$ is measurable on E. Then $\liminf f$ is measurable on E.

(20) Let f be a sequence of partial functions from X into $\mathbb{R}$ and x be an element of X. Suppose $x \in \operatorname{dom} f(0)$ and $f\#x$ is convergent. Then (the superior real sequence of f)$\#x$ is lower bounded.

(21) Let f be a sequence of partial functions from X into $\mathbb{R}$ with the same dom and E be an element of S. Suppose that

(i) $\operatorname{dom} f(0) = E$,

(ii) for every natural number n holds $f(n)$ is measurable on E, and

(iii) for every element x of X such that $x \in E$ holds $f\#x$ is convergent.

Then $\lim f$ is measurable on E.

(22) Let f be a sequence of partial functions from X into $\mathbb{R}$ with the same

dom, g be a partial function from X to $\overline{\mathbb{R}}$, and E be an element of S. Suppose that

(i) $\operatorname{dom} f(0) = E$,

(ii) for every natural number n holds $f(n)$ is measurable on E,

(iii) $\operatorname{dom} g = E$, and

(iv) for every element x of X such that $x \in E$ holds $f\#x$ is convergent and $g(x) = \lim(f\#x)$.

Then g is measurable on E.

2. The Measurability of Complex-Valued Functional Sequences

Let X be a non empty set, let H be a sequence of partial functions from X into $\mathbb{C}$, and let x be an element of X. The functor $H\#x$ yielding a complex sequence is defined by:

(Def. 9) For every natural number n holds $(H\#x)(n) = H(n)(x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{C}$. The functor $\lim f$ yields a partial function from X to $\mathbb{C}$ and is defined as follows:

(Def. 10) $\operatorname{dom} \lim f = \operatorname{dom} f(0)$ and for every element x of X such that $x \in \operatorname{dom} \lim f$ holds $(\lim f)(x) = \lim(f\#x)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{C}$. The functor $\Re(f)$ yielding a sequence of partial functions from X into $\mathbb{R}$ is defined by the condition (Def. 11).

(Def. 11) Let n be a natural number. Then $\operatorname{dom} \Re(f)(n) = \operatorname{dom} f(n)$ and for every element x of X such that $x \in \operatorname{dom} \Re(f)(n)$ holds $\Re(f)(n)(x) = \Re(f\#x)(n)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{C}$ with the same dom. Then $\Re(f)$ is a sequence of partial functions from X into $\mathbb{R}$ with the same dom.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{C}$. The functor $\Im(f)$ yielding a sequence of partial functions from X into $\mathbb{R}$ is defined by the condition (Def. 12).

(Def. 12) Let n be a natural number. Then $\operatorname{dom} \Im(f)(n) = \operatorname{dom} f(n)$ and for every element x of X such that $x \in \operatorname{dom} \Im(f)(n)$ holds $\Im(f)(n)(x) = \Im(f\#x)(n)$.

Let X be a non empty set and let f be a sequence of partial functions from X into $\mathbb{C}$ with the same dom. Then $\Im(f)$ is a sequence of partial functions from X into $\mathbb{R}$ with the same dom.

We now state several propositions:

(23) Let f be a sequence of partial functions from X into $\mathbb{C}$ with the same dom and x be an element of X. If $x \in \operatorname{dom} f(0)$, then $\Re(f)\#x = \Re(f\#x)$ and $\Im(f)\#x = \Im(f\#x)$.

(24) Let f be a sequence of partial functions from X into $\mathbb{C}$ and n be a natural number. Then $\Re(f)(n) = \Re(f(n))$ and $\Im(f)(n) = \Im(f(n))$.

(25) Let f be a sequence of partial functions from X into $\mathbb{C}$ with the same dom. Suppose that for every element x of X such that $x \in \operatorname{dom} f(0)$ holds $f\#x$ is convergent. Then $\lim \Re(f) = \Re(\lim f)$ and $\lim \Im(f) = \Im(\lim f)$.

(26) Let f be a sequence of partial functions from X into $\mathbb{C}$ with the same dom and E be an element of S. Suppose that

(i) $\operatorname{dom} f(0) = E$,

(ii) for every natural number n holds $f(n)$ is measurable on E, and

(iii) for every element x of X such that $x \in E$ holds $f\#x$ is convergent.

Then $\lim f$ is measurable on E.

(27) Let f be a sequence of partial functions from X into $\mathbb{C}$ with the same dom, g be a partial function from X to $\mathbb{C}$, and E be an element of S. Suppose that

(i) $\operatorname{dom} f(0) = E$,

(ii) for every natural number n holds $f(n)$ is measurable on E,

(iii) $\operatorname{dom} g = E$, and

(iv) for every element x of X such that $x \in E$ holds $f\#x$ is convergent and $g(x) = \lim(f\#x)$.

Then g is measurable on E.

3. Selected Properties of Complex-Valued Measurable Functions

One can prove the following propositions:

(28) $(r\,f){\restriction}Y = r\,(f{\restriction}Y)$.

(29) If $0 \leq k$ and $E \subseteq \operatorname{dom} f$ and f is measurable on E, then $|f|^k$ is measurable on E.

(30) For all partial functions f, g from X to $\mathbb{R}$ holds $\overline{\mathbb{R}}(f)\,\overline{\mathbb{R}}(g) = \overline{\mathbb{R}}(f\,g)$.

(31) Let f, g be partial functions from X to $\mathbb{R}$. Suppose $\operatorname{dom} f \cap \operatorname{dom} g = E$ and f is measurable on E and g is measurable on E. Then $f\,g$ is measurable on E.

(32) $\Re(f\,g) = \Re(f)\,\Re(g) - \Im(f)\,\Im(g)$ and $\Im(f\,g) = \Im(f)\,\Re(g) + \Re(f)\,\Im(g)$.

(33) If $\operatorname{dom} f \cap \operatorname{dom} g = E$ and f is measurable on E and g is measurable on E, then $f\,g$ is measurable on E.

(34) Let f, g be partial functions from X to $\mathbb{R}$. Suppose that

(i) there exists an element E of S such that $E = \operatorname{dom} f$ and $E = \operatorname{dom} g$ and f is measurable on E and g is measurable on E,

(ii) f is non-negative,

(iii) g is non-negative, and

(iv) for every element x of X such that $x \in \operatorname{dom} g$ holds $g(x) \leq f(x)$.

Then $\int g \, \mathrm{d}M \leq \int f \, \mathrm{d}M$.

(35) Let X be a non empty set, S be a σ-field of subsets of X, M be a σ-measure on S, and f be a partial function from X to $\mathbb{C}$. Suppose f is integrable on M. Then there exists an element A of S such that $A = \operatorname{dom} f$ and f is measurable on A and $|f|$ is integrable on M.

(36) Suppose f is integrable on M. Then there exists a function F from $\mathbb{N}$ into S such that

(i) for every natural number n holds $F(n) = \operatorname{dom} f \cap \text{GTE-dom}(|f|, \overline{\mathbb{R}}(\frac{1}{n+1}))$,

(ii) $\operatorname{dom} f \setminus \text{EQ-dom}(|f|, 0) = \bigcup \operatorname{rng} F$, and

(iii) for every natural number n holds $F(n) \in S$ and $M(F(n)) < +\infty$.

In the sequel x, A denote sets.

We now state several propositions:

(37) $|f| \restriction A = |f \restriction A|$.

(38) $\operatorname{dom}(|f| + |g|) = \operatorname{dom} f \cap \operatorname{dom} g$ and $\operatorname{dom} |f + g| \subseteq \operatorname{dom} |f|$.

(39) $|f| \restriction \operatorname{dom} |f + g| + |g| \restriction \operatorname{dom} |f + g| = (|f| + |g|) \restriction \operatorname{dom} |f + g|$.

(40) If $x \in \operatorname{dom} |f + g|$, then $|f + g|(x) \leq (|f| + |g|)(x)$.

(41) Let f, g be partial functions from X to $\mathbb{R}$. If for every set x such that $x \in \operatorname{dom} f$ holds $f(x) \leq g(x)$, then $g - f$ is non-negative.

(42) Suppose f is integrable on M and g is integrable on M. Then there exists an element E of S such that $E = \operatorname{dom}(f + g)$ and $\int |f + g| \restriction E \, \mathrm{d}M \leq \int |f| \restriction E \, \mathrm{d}M + \int |g| \restriction E \, \mathrm{d}M$.

4. Properties of Complex-Valued Simple Functions

Let X be a non empty set, let S be a σ-field of subsets of X, and let f be a partial function from X to $\mathbb{C}$. We say that f is simple function in S if and only if the condition (Def. 13) is satisfied.

(Def. 13) There exists a finite sequence F of separated subsets of S such that

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

(ii) for every natural number n and for all elements x, y of X such that $n \in \operatorname{dom} F$ and $x, y \in F(n)$ holds $f(x) = f(y)$.

Let X be a non empty set, let S be a σ-field of subsets of X, let f be a partial function from X to $\mathbb{R}$, let F be a finite sequence of separated subsets of S, and let a be a finite sequence of elements of $\mathbb{R}$. We say that F and a are representation of f if and only if the conditions (Def. 14) are satisfied.

(Def. 14)(i) $\operatorname{dom} f = \bigcup \operatorname{rng} F$,

(ii) $\operatorname{dom} F = \operatorname{dom} a$, and

(iii) for every natural number n such that $n \in \operatorname{dom} F$ and for every set x such that $x \in F(n)$ holds $f(x) = a(n)$.

Let us consider X, S, f, let F be a finite sequence of separated subsets of S, and let a be a finite sequence of elements of $\mathbb{C}$. We say that F and a are representation of f if and only if the conditions (Def. 15) are satisfied.

(Def. 15)(i) $\operatorname{dom} f = \bigcup \operatorname{rng} F$,

(ii) $\operatorname{dom} F = \operatorname{dom} a$, and

(iii) for every natural number n such that $n \in \operatorname{dom} F$ and for every set x such that $x \in F(n)$ holds $f(x) = a(n)$.

The following three propositions are true:

(43) f is simple function in S if and only if $\Re(f)$ is simple function in S and $\Im(f)$ is simple function in S.

(44) Suppose f is simple function in S. Then there exists a finite sequence F of separated subsets of S and there exists a finite sequence a of elements of $\mathbb{C}$ such that

(i) $\operatorname{dom} f = \bigcup \operatorname{rng} F$,

(ii) $\operatorname{dom} F = \operatorname{dom} a$, and

(iii) for every natural number n such that $n \in \operatorname{dom} F$ and for every set x such that $x \in F(n)$ holds $f(x) = a(n)$.

(45) f is simple function in S if and only if there exists a finite sequence F of separated subsets of S and there exists a finite sequence a of elements of $\mathbb{C}$ such that F and a are representation of f.

In the sequel c is a finite sequence of elements of $\mathbb{C}$.

Next we state four propositions:

(46) For every natural number n such that $n \in \operatorname{dom} \Re(c)$ holds $\Re(c)(n) = \Re(c(n))$.

(47) For every natural number n such that $n \in \operatorname{dom} \Im(c)$ holds $\Im(c)(n) = \Im(c(n))$.

(48) Let F be a finite sequence of separated subsets of S and a be a finite sequence of elements of $\mathbb{C}$. Then F and a are representation of f if and only if F and $\Re(a)$ are representation of $\Re(f)$ and F and $\Im(a)$ are representation of $\Im(f)$.

(49) f is simple function in S if and only if there exists a finite sequence F of separated subsets of S and there exists a finite sequence c of elements of $\mathbb{C}$ such that $\operatorname{dom} f = \bigcup \operatorname{rng} F$ and $\operatorname{dom} F = \operatorname{dom} c$ and for every natural number n such that $n \in \operatorname{dom} F$ and for every set x such that $x \in F(n)$ holds $\Re(f)(x) = \Re(c)(n)$ and for every natural number n such that $n \in \operatorname{dom} F$ and for every set x such that $x \in F(n)$ holds $\Im(f)(x) = \Im(c)(n)$.

References

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

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

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

[4] Józef Białas. Infimum and supremum of the set of real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):163–171, 1991.

[5] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.

[6] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.

[7] Józef Białas. Some properties of the intervals. *Formalized Mathematics*, 5(**1**):21–26, 1996.

[8] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 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. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

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

[13] Wenpai Chang, Hiroshi Yamazaki, and Yatsuka Nakamura. The inner product and conjugate of finite sequences of complex numbers. *Formalized Mathematics*, 13(**3**):367–373, 2005.

[14] Noboru Endou and Yasunari Shidama. Integral of measurable function. *Formalized Mathematics*, 14(**2**):53–70, 2006, doi:10.2478/v10037-006-0008-x.

[15] Noboru Endou, Yasunari Shidama, and Keiko Narita. Egoroff's theorem. *Formalized Mathematics*, 16(**1**):57–63, 2008, doi:10.2478/v10037-008-0009-z.

[16] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definitions and basic properties of measurable functions. *Formalized Mathematics*, 9(**3**):495–500, 2001.

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

[18] Jarosław Kotowicz and Yuji Sakai. Properties of partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 3(**2**):279–288, 1992.

[19] Keiko Narita, Noboru Endou, and Yasunari Shidama. Integral of complex-valued measurable function. *Formalized Mathematics*, 16(**4**):319–324, 2008, doi:10.2478/v10037-008-0039-6.

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

[21] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.

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

[23] Beata Perkowska. Functional sequence from a domain to a domain. *Formalized Mathematics*, 3(**1**):17–21, 1992.

[24] Yasunari Shidama and Noboru Endou. Integral of real-valued measurable function. *Formalized Mathematics*, 14(**4**):143–152, 2006, doi:10.2478/v10037-006-0018-8.

[25] Yasunari Shidama and Artur Korniłowicz. Convergence and the limit of complex sequences. Series. *Formalized Mathematics*, 6(**3**):403–410, 1997.

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

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

[28] Hiroshi Yamazaki, Noboru Endou, Yasunari Shidama, and Hiroyuki Okazaki. Inferior limit, superior limit and convergence of sequences of extended real numbers. *Formalized Mathematics*, 15(**4**):231–236, 2007, doi:10.2478/v10037-007-0026-3.

Received December 16, 2008

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 99–115, 2009

Collective Operations on Number-Membered Sets

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

Summary. The article starts with definitions of sets of opposite and inverse numbers of a given number membered set. Next, collective addition, subtraction, multiplication and division of two sets are defined. Complex numbers cases and extended real numbers ones are introduced separately and unified for reals. Shortcuts for singletons cases are also defined.

MML identifier: MEMBER_1, version: 7.11.01 4.117.1046

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

For simplicity, we adopt the following convention: w, w_1, w_2 are elements of $\overline{\mathbb{R}}$, c, c_1, c_2 are elements of $\mathbb{C}$, A, B, C, D are complex-membered sets, F, G, H, I are extended real-membered sets, a, b are complex numbers, f, g are extended real numbers, r is a real number, and e is a set.

Let us consider w. Then $-w$ is an element of $\overline{\mathbb{R}}$. Then w^{-1} is an element of $\overline{\mathbb{R}}$. Let us consider w_1. Then $w \cdot w_1$ is an element of $\overline{\mathbb{R}}$.

Let a, b, c, d be complex numbers. One can check that $\{a, b, c, d\}$ is complex-membered.

Let a, b, c, d be extended real numbers. Observe that $\{a, b, c, d\}$ is extended real-membered.

Let F be an extended real-membered set. The functor $\ominus F$ yielding an extended real-membered set is defined by:

(Def. 1) $\ominus F = \{-w : w \in F\}$.

ISSN 1426–2630(p), 1898-9934(e)

Let us note that the functor $\ominus F$ is involutive.

The following propositions are true:

(1) $f \in F$ iff $-f \in \ominus F$.

(2) $-f \in F$ iff $f \in \ominus F$.

Let F be an empty set. One can check that $\ominus F$ is empty.

Let F be an extended real-membered non empty set. Note that $\ominus F$ is non empty.

The following propositions are true:

(3) $F \subseteq G$ iff $\ominus F \subseteq \ominus G$.

(4) If $\ominus F = \ominus G$, then $F = G$.

(5) $\ominus(F \cup G) = \ominus F \cup \ominus G$.

(6) $\ominus(F \cap G) = \ominus F \cap \ominus G$.

(7) $\ominus(F \setminus G) = \ominus F \setminus \ominus G$.

(8) $\ominus(F \dot{-} G) = \ominus F \dot{-} \ominus G$.

(9) $\ominus\{f\} = \{-f\}$.

(10) $\ominus\{f, g\} = \{-f, -g\}$.

Let A be a complex-membered set. The functor $\ominus A$ yields a complex-membered set and is defined as follows:

(Def. 2) $\ominus A = \{-c : c \in A\}$.

Let us note that the functor $\ominus A$ is involutive.

Next we state two propositions:

(11) $a \in A$ iff $-a \in \ominus A$.

(12) $-a \in A$ iff $a \in \ominus A$.

Let A be an empty set. One can check that $\ominus A$ is empty.

Let A be a complex-membered non empty set. One can verify that $\ominus A$ is non empty.

Let A be a real-membered set. One can check that $\ominus A$ is real-membered.

Let A be a rational-membered set. Note that $\ominus A$ is rational-membered.

Let A be an integer-membered set. Observe that $\ominus A$ is integer-membered.

Let A be a real-membered set and let F be an extended real-membered set. One can verify that $\ominus A$ and $\ominus F$ can be identified when $A = F$.

We now state several propositions:

(13) $A \subseteq B$ iff $\ominus A \subseteq \ominus B$.

(14) If $\ominus A = \ominus B$, then $A = B$.

(15) $\ominus(A \cup B) = \ominus A \cup \ominus B$.

(16) $\ominus(A \cap B) = \ominus A \cap \ominus B$.

(17) $\ominus(A \setminus B) = \ominus A \setminus \ominus B$.

(18) $\ominus(A \dot{-} B) = \ominus A \dot{-} \ominus B$.

(19) $\ominus\{a\} = \{-a\}$.

(20) $\ominus\{a, b\} = \{-a, -b\}$.

Let F be an extended real-membered set. The functor F^{-1} yields an extended real-membered set and is defined by:

(Def. 3) $F^{-1} = \{w^{-1} : w \in F\}$.

Next we state the proposition

(21) If $f \in F$, then $f^{-1} \in F^{-1}$.

Let F be an empty set. Note that F^{-1} is empty.

Let F be an extended real-membered non empty set. One can check that F^{-1} is non empty.

The following propositions are true:

(22) If $F \subseteq G$, then $F^{-1} \subseteq G^{-1}$.

(23) $(F \cup G)^{-1} = F^{-1} \cup G^{-1}$.

(24) $(F \cap G)^{-1} \subseteq F^{-1} \cap G^{-1}$.

(25) $\ominus(F^{-1}) = (\ominus F)^{-1}$.

(26) $\{f\}^{-1} = \{f^{-1}\}$.

(27) $\{f, g\}^{-1} = \{f^{-1}, g^{-1}\}$.

Let A be a complex-membered set. The functor A^{-1} yields a complex-membered set and is defined as follows:

(Def. 4) $A^{-1} = \{c^{-1} : c \in A\}$.

Let us notice that the functor A^{-1} is involutive.

One can prove the following propositions:

(28) $a \in A$ iff $a^{-1} \in A^{-1}$.

(29) $a^{-1} \in A$ iff $a \in A^{-1}$.

Let A be an empty set. Observe that A^{-1} is empty.

Let A be a complex-membered non empty set. Observe that A^{-1} is non empty.

Let A be a real-membered set. Note that A^{-1} is real-membered.

Let A be a rational-membered set. One can verify that A^{-1} is rational-membered.

Let A be a real-membered set and let F be an extended real-membered set. One can verify that A^{-1} and F^{-1} can be identified when $A = F$.

Next we state several propositions:

(30) $A \subseteq B$ iff $A^{-1} \subseteq B^{-1}$.

(31) If $A^{-1} = B^{-1}$, then $A = B$.

(32) $(A \cup B)^{-1} = A^{-1} \cup B^{-1}$.

(33) $(A \cap B)^{-1} = A^{-1} \cap B^{-1}$.

(34) $(A \setminus B)^{-1} = A^{-1} \setminus B^{-1}$.

(35) $(A \dot{-} B)^{-1} = A^{-1} \dot{-} B^{-1}$.

(36) $\ominus(A^{-1}) = (\ominus A)^{-1}$.

(37) $\{a\}^{-1} = \{a^{-1}\}$.

(38) $\{a, b\}^{-1} = \{a^{-1}, b^{-1}\}$.

Let F, G be extended real-membered sets. The functor $F \oplus G$ is defined as follows:

(Def. 5) $F \oplus G = \{w_1 + w_2 : w_1 \in F \ \wedge\ w_2 \in G\}$.

Let us note that the functor $F \oplus G$ is commutative.

Next we state the proposition

(39) If $f \in F$ and $g \in G$, then $f + g \in F \oplus G$.

Let F be an empty set and let G be an extended real-membered set. Observe that $F \oplus G$ is empty and $G \oplus F$ is empty.

Let F, G be extended real-membered non empty sets. One can check that $F \oplus G$ is non empty.

Let F, G be extended real-membered sets. Observe that $F \oplus G$ is extended real-membered.

Next we state several propositions:

(40) If $F \subseteq G$ and $H \subseteq I$, then $F \oplus H \subseteq G \oplus I$.

(41) $F \oplus (G \cup H) = (F \oplus G) \cup (F \oplus H)$.

(42) $F \oplus G \cap H \subseteq (F \oplus G) \cap (F \oplus H)$.

(43) $\{f\} \oplus \{g\} = \{f + g\}$.

(44) $\{f\} \oplus \{g, h\} = \{f + g, f + h\}$.

(45) $\{f, g\} \oplus \{h, i\} = \{f + h, f + i, g + h, g + i\}$.

Let A, B be complex-membered sets. The functor $A \oplus B$ is defined by:

(Def. 6) $A \oplus B = \{c_1 + c_2 : c_1 \in A \ \wedge\ c_2 \in B\}$.

Let us note that the functor $A \oplus B$ is commutative.

Next we state the proposition

(46) If $a \in A$ and $b \in B$, then $a + b \in A \oplus B$.

Let A be an empty set and let B be a complex-membered set. One can check that $A \oplus B$ is empty and $B \oplus A$ is empty.

Let A, B be complex-membered non empty sets. Note that $A \oplus B$ is non empty.

Let A, B be complex-membered sets. One can check that $A \oplus B$ is complex-membered.

Let A, B be real-membered sets. Observe that $A \oplus B$ is real-membered.

Let A, B be rational-membered sets. Observe that $A \oplus B$ is rational-membered.

Let A, B be integer-membered sets. One can verify that $A \oplus B$ is integer-membered.

Let A, B be natural-membered sets. Observe that $A \oplus B$ is natural-membered.

Let A, B be real-membered sets and let F, G be extended real-membered sets. Observe that $A \oplus B$ and $F \oplus G$ can be identified when $A = F$ and $B = G$.

We now state several propositions:

(47) If $A \subseteq B$ and $C \subseteq D$, then $A \oplus C \subseteq B \oplus D$.

(48) $A \oplus (B \cup C) = (A \oplus B) \cup (A \oplus C)$.

(49) $A \oplus B \cap C \subseteq (A \oplus B) \cap (A \oplus C)$.

(50) $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.

(51) $\{a\} \oplus \{b\} = \{a + b\}$.

(52) $\{a\} \oplus \{s, t\} = \{a + s, a + t\}$.

(53) $\{a, b\} \oplus \{s, t\} = \{a + s, a + t, b + s, b + t\}$.

Let F, G be extended real-membered sets. The functor $F \ominus G$ is defined by:

(Def. 7) $F \ominus G = F \oplus \ominus G$.

Next we state two propositions:

(54) $F \ominus G = \{w_1 - w_2 : w_1 \in F \ \wedge \ w_2 \in G\}$.

(55) If $f \in F$ and $g \in G$, then $f - g \in F \ominus G$.

Let F be an empty set and let G be an extended real-membered set. Note that $F \ominus G$ is empty and $G \ominus F$ is empty.

Let F, G be extended real-membered non empty sets. Observe that $F \ominus G$ is non empty.

Let F, G be extended real-membered sets. Note that $F \ominus G$ is extended real-membered.

One can prove the following propositions:

(56) If $F \subseteq G$ and $H \subseteq I$, then $F \ominus H \subseteq G \ominus I$.

(57) $F \ominus (G \cup H) = (F \ominus G) \cup (F \ominus H)$.

(58) $F \ominus G \cap H \subseteq (F \ominus G) \cap (F \ominus H)$.

(59) $\ominus(F \oplus G) = \ominus F \ominus G$.

(60) $\ominus(F \ominus G) = \ominus F \oplus G$.

(61) $\{f\} \ominus \{g\} = \{f - g\}$.

(62) $\{f\} \ominus \{h, i\} = \{f - h, f - i\}$.

(63) $\{f, g\} \ominus \{h\} = \{f - h, g - h\}$.

(64) $\{f, g\} \ominus \{h, i\} = \{f - h, f - i, g - h, g - i\}$.

Let A, B be complex-membered sets. The functor $A \ominus B$ is defined by:

(Def. 8) $A \ominus B = A \oplus \ominus B$.

Next we state two propositions:

(65) $A \ominus B = \{c_1 - c_2 : c_1 \in A \ \wedge \ c_2 \in B\}$.

(66) If $a \in A$ and $b \in B$, then $a - b \in A \ominus B$.

Let A be an empty set and let B be a complex-membered set. One can check that $A \ominus B$ is empty and $B \ominus A$ is empty.

Let A, B be complex-membered non empty sets. One can verify that $A \ominus B$ is non empty.

Let A, B be complex-membered sets. One can verify that $A \ominus B$ is complex-membered.

Let A, B be real-membered sets. Note that $A \ominus B$ is real-membered.

Let A, B be rational-membered sets. One can verify that $A \ominus B$ is rational-membered.

Let A, B be integer-membered sets. One can check that $A \ominus B$ is integer-membered.

Let A, B be real-membered sets and let F, G be extended real-membered sets. One can check that $A \ominus B$ and $F \ominus G$ can be identified when $A = F$ and $B = G$.

The following propositions are true:

(67) If $A \subseteq B$ and $C \subseteq D$, then $A \ominus C \subseteq B \ominus D$.

(68) $A \ominus (B \cup C) = (A \ominus B) \cup (A \ominus C)$.

(69) $A \ominus B \cap C \subseteq (A \ominus B) \cap (A \ominus C)$.

(70) $\ominus(A \oplus B) = \ominus A \ominus B$.

(71) $\ominus(A \ominus B) = \ominus A \oplus B$.

(72) $A \oplus (B \ominus C) = (A \oplus B) \ominus C$.

(73) $A \ominus (B \oplus C) = A \ominus B \ominus C$.

(74) $A \ominus (B \ominus C) = (A \ominus B) \oplus C$.

(75) $\{a\} \ominus \{b\} = \{a - b\}$.

(76) $\{a\} \ominus \{s, t\} = \{a - s, a - t\}$.

(77) $\{a, b\} \ominus \{s\} = \{a - s, b - s\}$.

(78) $\{a, b\} \ominus \{s, t\} = \{a - s, a - t, b - s, b - t\}$.

Let F, G be extended real-membered sets. The functor $F \circ G$ is defined as follows:

(Def. 9) $F \circ G = \{w_1 \cdot w_2 : w_1 \in F \ \wedge \ w_2 \in G\}$.

Let us observe that the functor $F \circ G$ is commutative.

Let F be an empty set and let G be an extended real-membered set. One can verify that $F \circ G$ is empty and $G \circ F$ is empty.

Let F, G be extended real-membered sets. Note that $F \circ G$ is extended real-membered.

Next we state the proposition

(79) If $f \in F$ and $g \in G$, then $f \cdot g \in F \circ G$.

Let F, G be extended real-membered non empty sets. Observe that $F \circ G$ is non empty.

One can prove the following propositions:

(80) $(F \circ G) \circ H = F \circ (G \circ H)$.

(81) If $F \subseteq G$ and $H \subseteq I$, then $F \circ H \subseteq G \circ I$.

(82) $F \circ (G \cup H) = F \circ G \cup F \circ H$.

(83) $F \circ (G \cap H) \subseteq (F \circ G) \cap (F \circ H)$.

(84) $F \circ \ominus G = \ominus(F \circ G)$.

(85) $(F \circ G)^{-1} = F^{-1} \circ G^{-1}$.

(86) $\{f\} \circ \{g\} = \{f \cdot g\}$.

(87) $\{f\} \circ \{h, i\} = \{f \cdot h, f \cdot i\}$.

(88) $\{f, g\} \circ \{h, i\} = \{f \cdot h, f \cdot i, g \cdot h, g \cdot i\}$.

Let A, B be complex-membered sets. The functor $A \circ B$ is defined as follows:

(Def. 10) $A \circ B = \{c_1 \cdot c_2 : c_1 \in A \ \wedge \ c_2 \in B\}$.

Let us notice that the functor $A \circ B$ is commutative.

One can prove the following proposition

(89) If $a \in A$ and $b \in B$, then $a \cdot b \in A \circ B$.

Let A be an empty set and let B be a complex-membered set. Note that $A \circ B$ is empty and $B \circ A$ is empty.

Let A, B be complex-membered non empty sets. Note that $A \circ B$ is non empty.

Let A, B be complex-membered sets. Note that $A \circ B$ is complex-membered.

Let A, B be real-membered sets. Note that $A \circ B$ is real-membered.

Let A, B be rational-membered sets. Observe that $A \circ B$ is rational-membered.

Let A, B be integer-membered sets. Observe that $A \circ B$ is integer-membered.

Let A, B be natural-membered sets. Observe that $A \circ B$ is natural-membered.

Let A, B be real-membered sets and let F, G be extended real-membered sets. Note that $A \circ B$ and $F \circ G$ can be identified when $A = F$ and $B = G$.

The following propositions are true:

(90) $(A \circ B) \circ C = A \circ (B \circ C)$.

(91) If $A \subseteq B$ and $C \subseteq D$, then $A \circ C \subseteq B \circ D$.

(92) $A \circ (B \cup C) = A \circ B \cup A \circ C$.

(93) $A \circ (B \cap C) \subseteq (A \circ B) \cap (A \circ C)$.

(94) $A \circ \ominus B = \ominus(A \circ B)$.

(95) $A \circ (B \oplus C) \subseteq A \circ B \oplus A \circ C$.

(96) $A \circ (B \ominus C) \subseteq A \circ B \ominus A \circ C$.

(97) $(A \circ B)^{-1} = A^{-1} \circ B^{-1}$.

(98) $\{a\} \circ \{b\} = \{a \cdot b\}$.

(99) $\{a\} \circ \{s, t\} = \{a \cdot s, a \cdot t\}$.

(100) $\{a, b\} \circ \{s, t\} = \{a \cdot s, a \cdot t, b \cdot s, b \cdot t\}$.

Let F, G be extended real-membered sets. The functor $F \oslash G$ is defined as follows:

(Def. 11) $F \oslash G = F \circ G^{-1}$.

We now state two propositions:

(101) $F \oslash G = \{\frac{w_1}{w_2} : w_1 \in F \ \wedge \ w_2 \in G\}$.

(102) If $f \in F$ and $g \in G$, then $\frac{f}{g} \in F \oslash G$.

Let F be an empty set and let G be an extended real-membered set. One can verify that $F \oslash G$ is empty and $G \oslash F$ is empty.

Let F, G be extended real-membered non empty sets. One can verify that $F \oslash G$ is non empty.

Let F, G be extended real-membered sets. One can verify that $F \oslash G$ is extended real-membered.

Next we state a number of propositions:

(103) If $F \subseteq G$ and $H \subseteq I$, then $F \oslash H \subseteq G \oslash I$.

(104) $(F \cup G) \oslash H = (F \oslash H) \cup (G \oslash H)$.

(105) $F \cap G \oslash H \subseteq (F \oslash H) \cap (G \oslash H)$.

(106) $F \oslash (G \cup H) = (F \oslash G) \cup (F \oslash H)$.

(107) $F \oslash G \cap H \subseteq (F \oslash G) \cap (F \oslash H)$.

(108) $F \circ G \oslash H = F \circ (G \oslash H)$.

(109) $(F \oslash G) \circ H = F \circ H \oslash G$.

(110) $F \oslash G \oslash H = F \oslash G \circ H$.

(111) $\{f\} \oslash \{g\} = \{\frac{f}{g}\}$.

(112) $\{f\} \oslash \{h, i\} = \{\frac{f}{h}, \frac{f}{i}\}$.

(113) $\{f, g\} \oslash \{h\} = \{\frac{f}{h}, \frac{g}{h}\}$.

(114) $\{f, g\} \oslash \{h, i\} = \{\frac{f}{h}, \frac{f}{i}, \frac{g}{h}, \frac{g}{i}\}$.

Let A, B be complex-membered sets. The functor $A \oslash B$ is defined by:

(Def. 12) $A \oslash B = A \circ B^{-1}$.

We now state two propositions:

(115) $A \oslash B = \{\frac{c_1}{c_2} : c_1 \in A \ \wedge \ c_2 \in B\}$.

(116) If $a \in A$ and $b \in B$, then $\frac{a}{b} \in A \oslash B$.

Let A be an empty set and let B be a complex-membered set. One can check that $A \oslash B$ is empty and $B \oslash A$ is empty.

Let A, B be complex-membered non empty sets. Note that $A \oslash B$ is non empty.

Let A, B be complex-membered sets. Note that $A \oslash B$ is complex-membered.

Let A, B be real-membered sets. Observe that $A \oslash B$ is real-membered.

Let A, B be rational-membered sets. One can check that $A \oslash B$ is rational-membered.

Let A, B be real-membered sets and let F, G be extended real-membered sets. One can check that $A \oslash B$ and $F \oslash G$ can be identified when $A = F$ and $B = G$.

We now state a number of propositions:

(117) If $A \subseteq B$ and $C \subseteq D$, then $A \oslash C \subseteq B \oslash D$.

(118) $A \oslash (B \cup C) = (A \oslash B) \cup (A \oslash C)$.

(119) $A \oslash B \cap C \subseteq (A \oslash B) \cap (A \oslash C)$.

(120) $A \oslash \ominus B = \ominus(A \oslash B)$.

(121) $\ominus A \oslash B = \ominus(A \oslash B)$.

(122) $(A \oplus B) \oslash C \subseteq (A \oslash C) \oplus (B \oslash C)$.

(123) $(A \ominus B) \oslash C \subseteq (A \oslash C) \ominus (B \oslash C)$.

(124) $A \circ B \oslash C = A \circ (B \oslash C)$.

(125) $(A \oslash B) \circ C = A \circ C \oslash B$.

(126) $A \oslash B \oslash C = A \oslash B \circ C$.

(127) $A \oslash (B \oslash C) = A \circ C \oslash B$.

(128) $\{a\} \oslash \{b\} = \{\frac{a}{b}\}$.

(129) $\{a\} \oslash \{s, t\} = \{\frac{a}{s}, \frac{a}{t}\}$.

(130) $\{a, b\} \oslash \{s\} = \{\frac{a}{s}, \frac{b}{s}\}$.

(131) $\{a, b\} \oslash \{s, t\} = \{\frac{a}{s}, \frac{a}{t}, \frac{b}{s}, \frac{b}{t}\}$.

Let F be an extended real-membered set and let f be an extended real number. The functor $f \oplus F$ is defined as follows:

(Def. 13) $f \oplus F = \{f\} \oplus F$.

We now state three propositions:

(132) If $g \in G$, then $f + g \in f \oplus G$.

(133) $f \oplus F = \{f + w : w \in F\}$.

(134) If $e \in f \oplus F$, then there exists w such that $e = f + w$ and $w \in F$.

Let F be an empty set and let f be an extended real number. One can check that $f \oplus F$ is empty.

Let F be an extended real-membered non empty set and let f be an extended real number. Observe that $f \oplus F$ is non empty.

Let F be an extended real-membered set and let f be an extended real number. One can check that $f \oplus F$ is extended real-membered.

Next we state several propositions:

(135) If $r \oplus F \subseteq r \oplus G$, then $F \subseteq G$.

(136) If $r \oplus F = r \oplus G$, then $F = G$.

(137) $r \oplus F \cap G = (r \oplus F) \cap (r \oplus G)$.

(138) $(f \oplus F) \setminus (f \oplus G) \subseteq f \oplus (F \setminus G)$.

(139) $r \oplus (F \setminus G) = (r \oplus F) \setminus (r \oplus G)$.

(140) $r \oplus (F \dot{-} G) = (r \oplus F) \dot{-} (r \oplus G)$.

Let A be a complex-membered set and let a be a complex number. The functor $a \oplus A$ is defined as follows:

(Def. 14) $a \oplus A = \{a\} \oplus A$.

We now state three propositions:

(141) If $b \in A$, then $a + b \in a \oplus A$.

(142) $a \oplus A = \{a + c : c \in A\}$.

(143) If $e \in a \oplus A$, then there exists c such that $e = a + c$ and $c \in A$.

Let A be an empty set and let a be a complex number. Observe that $a \oplus A$ is empty.

Let A be a complex-membered non empty set and let a be a complex number. Note that $a \oplus A$ is non empty.

Let A be a complex-membered set and let a be a complex number. Observe that $a \oplus A$ is complex-membered.

Let A be a real-membered set and let a be a real number. One can verify that $a \oplus A$ is real-membered.

Let A be a rational-membered set and let a be a rational number. Note that $a \oplus A$ is rational-membered.

Let A be an integer-membered set and let a be an integer number. One can verify that $a \oplus A$ is integer-membered.

Let A be a natural-membered set and let a be a natural number. Note that $a \oplus A$ is natural-membered.

Let A be a real-membered set, let F be an extended real-membered set, let a be a real number, and let f be an extended real number. Note that $a \oplus A$ and $f \oplus F$ can be identified when $a = f$ and $A = F$.

We now state several propositions:

(144) $A \subseteq B$ iff $a \oplus A \subseteq a \oplus B$.

(145) If $a \oplus A = a \oplus B$, then $A = B$.

(146) $0 \oplus A = A$.

(147) $(a + b) \oplus A = a \oplus (b \oplus A)$.

(148) $a \oplus (A \oplus B) = (a \oplus A) \oplus B$.

(149) $a \oplus A \cap B = (a \oplus A) \cap (a \oplus B)$.

(150) $a \oplus (A \setminus B) = (a \oplus A) \setminus (a \oplus B)$.

(151) $a \oplus (A \dot{-} B) = (a \oplus A) \dot{-} (a \oplus B)$.

Let F be an extended real-membered set and let f be an extended real number. The functor $f \ominus F$ is defined by:

(Def. 15) $f \ominus F = \{f\} \ominus F$.

The following propositions are true:

(152) If $g \in G$, then $f - g \in f \ominus G$.

(153) $f \ominus F = \{f - w : w \in F\}$.

(154) If $e \in f \ominus F$, then there exists w such that $e = f - w$ and $w \in F$.

Let F be an empty set and let f be an extended real number. One can check that $f \ominus F$ is empty.

Let F be an extended real-membered non empty set and let f be an extended real number. One can verify that $f \ominus F$ is non empty.

Let F be an extended real-membered set and let f be an extended real number. Observe that $f \ominus F$ is extended real-membered.

We now state several propositions:

(155) If $r \ominus F \subseteq r \ominus G$, then $F \subseteq G$.

(156) If $r \ominus F = r \ominus G$, then $F = G$.

(157) $r \ominus F \cap G = (r \ominus F) \cap (r \ominus G)$.

(158) $r \ominus (F \setminus G) = (r \ominus F) \setminus (r \ominus G)$.

(159) $r \ominus (F \dot{-} G) = (r \ominus F) \dot{-} (r \ominus G)$.

Let A be a complex-membered set and let a be a complex number. The functor $a \ominus A$ is defined as follows:

(Def. 16) $a \ominus A = \{a\} \ominus A$.

Next we state three propositions:

(160) If $b \in A$, then $a - b \in a \ominus A$.

(161) $a \ominus A = \{a - c : c \in A\}$.

(162) If $e \in a \ominus A$, then there exists c such that $e = a - c$ and $c \in A$.

Let A be an empty set and let a be a complex number. One can verify that $a \ominus A$ is empty.

Let A be a complex-membered non empty set and let a be a complex number. Note that $a \ominus A$ is non empty.

Let A be a complex-membered set and let a be a complex number. Note that $a \ominus A$ is complex-membered.

Let A be a real-membered set and let a be a real number. Note that $a \ominus A$ is real-membered.

Let A be a rational-membered set and let a be a rational number. Note that $a \ominus A$ is rational-membered.

Let A be an integer-membered set and let a be an integer number. Observe that $a \ominus A$ is integer-membered.

Let A be a real-membered set, let F be an extended real-membered set, let a be a real number, and let f be an extended real number. Observe that $a \ominus A$ and $f \ominus F$ can be identified when $a = f$ and $A = F$.

Next we state several propositions:

(163) $A \subseteq B$ iff $a \ominus A \subseteq a \ominus B$.

(164) If $a \ominus A = a \ominus B$, then $A = B$.

(165) $a \ominus A \cap B = (a \ominus A) \cap (a \ominus B)$.

(166) $a \ominus (A \setminus B) = (a \ominus A) \setminus (a \ominus B)$.

(167) $a \ominus (A \dot{-} B) = (a \ominus A) \dot{-} (a \ominus B)$.

Let F be an extended real-membered set and let f be an extended real number. The functor $F \ominus f$ is defined as follows:

(Def. 17) $F \ominus f = F \ominus \{f\}$.

One can prove the following three propositions:

(168) If $g \in G$, then $g - f \in G \ominus f$.

(169) $F \ominus f = \{w - f : w \in F\}$.

(170) If $e \in F \ominus f$, then there exists w such that $e = w - f$ and $w \in F$.

Let F be an empty set and let f be an extended real number. One can verify that $F \ominus f$ is empty.

Let F be an extended real-membered non empty set and let f be an extended real number. Observe that $F \ominus f$ is non empty.

Let F be an extended real-membered set and let f be an extended real number. Note that $F \ominus f$ is extended real-membered.

One can prove the following propositions:

(171) $F \ominus f = \ominus(f \ominus F)$.

(172) $f \ominus F = \ominus(F \ominus f)$.

(173) $F \cap G \ominus r = (F \ominus r) \cap (G \ominus r)$.

(174) $(F \setminus G) \ominus r = (F \ominus r) \setminus (G \ominus r)$.

(175) $(F \dot{-} G) \ominus r = (F \ominus r) \dot{-} (G \ominus r)$.

Let A be a complex-membered set and let a be a complex number. The functor $A \ominus a$ is defined by:

(Def. 18) $A \ominus a = A \ominus \{a\}$.

Next we state three propositions:

(176) If $b \in A$, then $b - a \in A \ominus a$.

(177) $A \ominus a = \{c - a : c \in A\}$.

(178) If $e \in A \ominus a$, then there exists c such that $e = c - a$ and $c \in A$.

Let A be an empty set and let a be a complex number. Observe that $A \ominus a$ is empty.

Let A be a complex-membered non empty set and let a be a complex number. Observe that $A \ominus a$ is non empty.

Let A be a complex-membered set and let a be a complex number. Observe that $A \ominus a$ is complex-membered.

Let A be a real-membered set and let a be a real number. Note that $A \ominus a$ is real-membered.

Let A be a rational-membered set and let a be a rational number. Note that $A \ominus a$ is rational-membered.

Let A be an integer-membered set and let a be an integer number. One can verify that $A \ominus a$ is integer-membered.

Let A be a real-membered set, let F be an extended real-membered set, let a be a real number, and let f be an extended real number. One can verify that $A \ominus a$ and $F \ominus f$ can be identified when $a = f$ and $A = F$.

Next we state several propositions:

(179) $A \subseteq B$ iff $A \ominus a \subseteq B \ominus a$.

(180) If $A \ominus a = B \ominus a$, then $A = B$.

(181) $A \ominus a = \ominus(a \ominus A)$.

(182) $a \ominus A = \ominus(A \ominus a)$.

(183) $A \cap B \ominus a = (A \ominus a) \cap (B \ominus a)$.

(184) $(A \setminus B) \ominus a = (A \ominus a) \setminus (B \ominus a)$.

(185) $(A \dot{-} B) \ominus a = (A \ominus a) \dot{-} (B \ominus a)$.

Let F be an extended real-membered set and let f be an extended real number. The functor $f \circ F$ is defined as follows:

(Def. 19) $f \circ F = \{f\} \circ F$.

The following three propositions are true:

(186) If $g \in G$, then $f \cdot g \in f \circ G$.

(187) $f \circ F = \{f \cdot w : w \in F\}$.

(188) If $e \in f \circ F$, then there exists w such that $e = f \cdot w$ and $w \in F$.

Let F be an empty set and let f be an extended real number. Observe that $f \circ F$ is empty.

Let F be an extended real-membered non empty set and let f be an extended real number. One can verify that $f \circ F$ is non empty.

Let F be an extended real-membered set and let f be an extended real number. Note that $f \circ F$ is extended real-membered.

One can prove the following four propositions:

(189) If $r \neq 0$, then $r \circ (F \cap G) = (r \circ F) \cap (r \circ G)$.

(190) $f \circ F \setminus f \circ G \subseteq f \circ (F \setminus G)$.

(191) If $r \neq 0$, then $r \circ (F \setminus G) = r \circ F \setminus r \circ G$.

(192) If $r \neq 0$, then $r \circ (F \dot{-} G) = r \circ F \dot{-} r \circ G$.

Let A be a complex-membered set and let a be a complex number. The functor $a \circ A$ is defined as follows:

(Def. 20) $a \circ A = \{a\} \circ A$.

We now state three propositions:

(193) If $b \in A$, then $a \cdot b \in a \circ A$.

(194) $a \circ A = \{a \cdot c : c \in A\}$.

(195) If $e \in a \circ A$, then there exists c such that $e = a \cdot c$ and $c \in A$.

Let A be an empty set and let a be a complex number. Note that $a \circ A$ is empty.

Let A be a complex-membered non empty set and let a be a complex number. One can verify that $a \circ A$ is non empty.

Let A be a complex-membered set and let a be a complex number. Note that $a \circ A$ is complex-membered.

Let A be a real-membered set and let a be a real number. Note that $a \circ A$ is real-membered.

Let A be a rational-membered set and let a be a rational number. Observe that $a \circ A$ is rational-membered.

Let A be an integer-membered set and let a be an integer number. Note that $a \circ A$ is integer-membered.

Let A be a natural-membered set and let a be a natural number. One can check that $a \circ A$ is natural-membered.

Let A be a real-membered set, let F be an extended real-membered set, let a be a real number, and let f be an extended real number. Note that $a \circ A$ and $f \circ F$ can be identified when $a = f$ and $A = F$.

One can prove the following propositions:

(196) If $a \neq 0$ and $a \circ A \subseteq a \circ B$, then $A \subseteq B$.

(197) If $a \neq 0$ and $a \circ A = a \circ B$, then $A = B$.

(198) If $a \neq 0$, then $a \circ (A \cap B) = (a \circ A) \cap (a \circ B)$.

(199) If $a \neq 0$, then $a \circ (A \setminus B) = a \circ A \setminus a \circ B$.

(200) If $a \neq 0$, then $a \circ (A \dot{-} B) = a \circ A \dot{-} a \circ B$.

(201) $0 \circ A \subseteq \{0\}$.

(202) If $A \neq \emptyset$, then $0 \circ A = \{0\}$.

(203) $1 \circ A = A$.

(204) $(a \cdot b) \circ A = a \circ (b \circ A)$.

(205) $a \circ (A \circ B) = (a \circ A) \circ B$.

(206) $(a + b) \circ A \subseteq a \circ A \oplus b \circ A$.

(207) $(a - b) \circ A \subseteq a \circ A \ominus b \circ A$.

(208) $a \circ (B \oplus C) = a \circ B \oplus a \circ C$.

(209) $a \circ (B \ominus C) = a \circ B \ominus a \circ C$.

Let F be an extended real-membered set and let f be an extended real number. The functor $f \oslash F$ is defined by:

(Def. 21) $f \oslash F = \{f\} \oslash F$.

We now state three propositions:

(210) If $g \in G$, then $\frac{f}{g} \in f \oslash G$.

(211) $f \oslash F = \{\frac{f}{w} : w \in F\}$.

(212) If $e \in f \oslash F$, then there exists w such that $e = \frac{f}{w}$ and $w \in F$.

Let F be an empty set and let f be an extended real number. Note that $f \oslash F$ is empty.

Let F be an extended real-membered non empty set and let f be an extended real number. One can verify that $f \oslash F$ is non empty.

Let F be an extended real-membered set and let f be an extended real number. Observe that $f \oslash F$ is extended real-membered.

Let A be a complex-membered set and let a be a complex number. The functor $a \oslash A$ is defined by:

(Def. 22) $a \oslash A = \{a\} \oslash A$.

One can prove the following three propositions:

(213) If $b \in A$, then $\frac{a}{b} \in a \oslash A$.

(214) $a \oslash A = \{\frac{a}{c} : c \in A\}$.

(215) If $e \in a \oslash A$, then there exists c such that $e = \frac{a}{c}$ and $c \in A$.

Let A be an empty set and let a be a complex number. One can check that $a \oslash A$ is empty.

Let A be a complex-membered non empty set and let a be a complex number. Note that $a \oslash A$ is non empty.

Let A be a complex-membered set and let a be a complex number. One can check that $a \oslash A$ is complex-membered.

Let A be a real-membered set and let a be a real number. One can check that $a \oslash A$ is real-membered.

Let A be a rational-membered set and let a be a rational number. One can verify that $a \oslash A$ is rational-membered.

Let A be a real-membered set, let F be an extended real-membered set, let a be a real number, and let f be an extended real number. Observe that $a \oslash A$ and $f \oslash F$ can be identified when $a = f$ and $A = F$.

The following propositions are true:

(216) If $a \neq 0$ and $a \oslash A \subseteq a \oslash B$, then $A \subseteq B$.

(217) If $a \neq 0$ and $a \oslash A = a \oslash B$, then $A = B$.

(218) If $a \neq 0$, then $a \oslash A \cap B = (a \oslash A) \cap (a \oslash B)$.

(219) If $a \neq 0$, then $a \oslash (A \setminus B) = (a \oslash A) \setminus (a \oslash B)$.

(220) If $a \neq 0$, then $a \oslash (A \dot{-} B) = (a \oslash A) \dot{-} (a \oslash B)$.

(221) $(a + b) \oslash A \subseteq (a \oslash A) \oplus (b \oslash A)$.

(222) $(a - b) \oslash A \subseteq (a \oslash A) \ominus (b \oslash A)$.

Let F be an extended real-membered set and let f be an extended real number. The functor $F \oslash f$ is defined by:

(Def. 23) $F \oslash f = F \oslash \{f\}$.

We now state three propositions:

(223) If $g \in G$, then $\frac{g}{f} \in G \oslash f$.

(224) $F \oslash f = \{\frac{w}{f} : w \in F\}$.

(225) If $e \in F \oslash f$, then there exists w such that $e = \frac{w}{f}$ and $w \in F$.

Let F be an empty set and let f be an extended real number. Note that $F \oslash f$ is empty.

Let F be an extended real-membered non empty set and let f be an extended real number. Observe that $F \oslash f$ is non empty.

Let F be an extended real-membered set and let f be an extended real number. Note that $F \oslash f$ is extended real-membered.

Let A be a complex-membered set and let a be a complex number. The functor $A \oslash a$ is defined by:

(Def. 24) $A \oslash a = A \oslash \{a\}$.

One can prove the following three propositions:

(226) If $b \in A$, then $\frac{b}{a} \in A \oslash a$.

(227) $A \oslash a = \{\frac{c}{a} : c \in A\}$.

(228) If $e \in A \oslash a$, then there exists c such that $e = \frac{c}{a}$ and $c \in A$.

Let A be an empty set and let a be a complex number. Note that $A \oslash a$ is empty.

Let A be a complex-membered non empty set and let a be a complex number. Note that $A \oslash a$ is non empty.

Let A be a complex-membered set and let a be a complex number. One can check that $A \oslash a$ is complex-membered.

Let A be a real-membered set and let a be a real number. One can check that $A \oslash a$ is real-membered.

Let A be a rational-membered set and let a be a rational number. Observe that $A \oslash a$ is rational-membered.

Let A be a real-membered set, let F be an extended real-membered set, let a be a real number, and let f be an extended real number. Note that $A \oslash a$ and $F \oslash f$ can be identified when $a = f$ and $A = F$.

The following propositions are true:

(229) If $a \neq 0$ and $A \oslash a \subseteq B \oslash a$, then $A \subseteq B$.

(230) If $a \neq 0$ and $A \oslash a = B \oslash a$, then $A = B$.

(231) If $a \neq 0$, then $A \cap B \oslash a = (A \oslash a) \cap (B \oslash a)$.

(232) If $a \neq 0$, then $(A \setminus B) \oslash a = (A \oslash a) \setminus (B \oslash a)$.

(233) If $a \neq 0$, then $(A \dot{-} B) \oslash a = (A \oslash a) \dot{-} (B \oslash a)$.

(234) $(A \oplus B) \oslash a = (A \oslash a) \oplus (B \oslash a)$.

(235) $(A \ominus B) \oslash a = (A \oslash a) \ominus (B \oslash a)$.

References

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

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

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

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

Received December 19, 2008

FORMALIZED MATHEMATICS
Vol. **17**, No. **2**, Pages 117–122, **2009**

Solution of Cubic and Quartic Equations

Marco Riccardi
Casella Postale 49
54038 Montignoso, Italy

Summary. In this article, the principal n-th root of a complex number is defined, the Vieta's formulas for polynomial equations of degree 2, 3 and 4 are formalized. The solution of quadratic equations, the Cardan's solution of cubic equations and the Descartes-Euler solution of quartic equations in terms of their complex coefficients are also presented [5].

MML identifier: `POLYEQ_5`, version: `7.11.02 4.120.1050`

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

1. Preliminaries

In this paper a, b denote complex numbers.

The following propositions are true:

(1) $a \cdot a = a^2$.

(2) $a \cdot a \cdot a = a^3$.

(3) $a \cdot a \cdot a \cdot a = a^4$.

(4) $(a-b)^2 = (a^2 - 2 \cdot a \cdot b) + b^2$.

(5) $(a-b)^3 = ((a^3 - 3 \cdot a^2 \cdot b) + 3 \cdot b^2 \cdot a) - b^3$.

(6) $(a-b)^4 = (((a^4 - 4 \cdot a^3 \cdot b) + 6 \cdot a^2 \cdot b^2) - 4 \cdot b^3 \cdot a) + b^4$.

Let n be a natural number and let r be a real number. We introduce $r^{1/n}$ as a synonym of $\sqrt[n]{r}$.

Let n be a non zero natural number and let z be a complex number. The functor $\sqrt[n]{z}$ yielding a complex number is defined as follows:

(Def. 1) $\sqrt[n]{z} = |z|^{1/n} \cdot (\cos(\frac{\operatorname{Arg} z}{n}) + \sin(\frac{\operatorname{Arg} z}{n}) \cdot i)$.

ISSN 1426–2630(p), 1898-9934(e)

In the sequel z is a complex number and n_0 is a non zero natural number.

The following propositions are true:

(7) $\sqrt[n_0]{z^{n_0}} = z$.

(8) For every real number r such that $r \geq 0$ holds $\sqrt[n_0]{r} = r^{1/n_0}$.

(9) For every real number r such that $r > 0$ holds $\sqrt[n_0]{\frac{z}{r}} = \frac{\sqrt[n_0]{z}}{\sqrt[n_0]{r}}$.

(10) $z^2 = a$ iff $z = \sqrt[2]{a}$ or $z = -\sqrt[2]{a}$.

2. Solution of Quadratic Equations

In the sequel a_0, a_1, a_2, s_1, s_2 denote complex numbers.

We now state two propositions:

(11) If $a_1 = -(s_1 + s_2)$ and $a_0 = s_1 \cdot s_2$, then $z^2 + a_1 \cdot z + a_0 = 0$ iff $z = s_1$ or $z = s_2$.

(12) If $a_2 \neq 0$, then $a_2 \cdot z^2 + a_1 \cdot z + a_0 = 0$ iff $z = -\frac{a_1}{2 \cdot a_2} + \frac{\sqrt[2]{\Delta(a_0,a_1,a_2)}}{2 \cdot a_2}$ or $z = -\frac{a_1}{2 \cdot a_2} - \frac{\sqrt[2]{\Delta(a_0,a_1,a_2)}}{2 \cdot a_2}$.

3. Solution of Cubic Equations

In the sequel a_3, x, q, r, s, s_3 are complex numbers.

We now state four propositions:

(13) Suppose $z = x - \frac{a_2}{3}$ and $q = \frac{3 \cdot a_1 - {a_2}^2}{9}$ and $r = \frac{9 \cdot a_2 \cdot a_1 - 2 \cdot {a_2}^3 - 27 \cdot a_0}{54}$. Then $z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0 = 0$ if and only if $(x^3 + 3 \cdot q \cdot x) - 2 \cdot r = 0$.

(14) If $a_2 = -(s_1 + s_2 + s_3)$ and $a_1 = s_1 \cdot s_2 + s_1 \cdot s_3 + s_2 \cdot s_3$ and $a_0 = -s_1 \cdot s_2 \cdot s_3$, then $z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0 = 0$ iff $z = s_1$ or $z = s_2$ or $z = s_3$.

(15) Suppose $q = \frac{3 \cdot a_1 - {a_2}^2}{9}$ and $q \neq 0$ and $r = \frac{9 \cdot a_2 \cdot a_1 - 2 \cdot {a_2}^3 - 27 \cdot a_0}{54}$ and $s = \sqrt[2]{q^3 + r^2}$ and $s_1 = \sqrt[3]{r + s}$ and $s_2 = -\frac{q}{s_1}$. Then $z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0 = 0$ if and only if one of the following conditions is satisfied:

(i) $z = (s_1 + s_2) - \frac{a_2}{3}$, or

(ii) $z = (-\frac{s_1 + s_2}{2} - \frac{a_2}{3}) + \frac{(s_1 - s_2) \cdot \sqrt[2]{3} \cdot i}{2}$, or

(iii) $z = -\frac{s_1 + s_2}{2} - \frac{a_2}{3} - \frac{(s_1 - s_2) \cdot \sqrt[2]{3} \cdot i}{2}$.

(16) Suppose $q = \frac{3 \cdot a_1 - {a_2}^2}{9}$ and $q = 0$ and $r = \frac{9 \cdot a_2 \cdot a_1 - 2 \cdot {a_2}^3 - 27 \cdot a_0}{54}$ and $s_1 = \sqrt[3]{2 \cdot r}$. Then $z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0 = 0$ if and only if one of the following conditions is satisfied:

(i) $z = s_1 - \frac{a_2}{3}$, or

(ii) $z = (-\frac{s_1}{2} - \frac{a_2}{3}) + \frac{s_1 \cdot \sqrt[2]{3} \cdot i}{2}$, or

(iii) $z = -\frac{s_1}{2} - \frac{a_2}{3} - \frac{s_1 \cdot \sqrt[2]{3} \cdot i}{2}$.

Let a_0, a_1, a_2 be complex numbers. The functor $\rho_1(a_0, a_1, a_2)$ yielding a complex number is defined as follows:

(Def. 2)(i) There exist r, s_1 such that $r = \frac{9 \cdot a_2 \cdot a_1 - 2 \cdot a_2{}^3 - 27 \cdot a_0}{54}$ and $s_1 = \sqrt[3]{2 \cdot r}$ and $\rho_1(a_0, a_1, a_2) = s_1 - \frac{a_2}{3}$ if $3 \cdot a_1 - a_2{}^2 = 0$,

(ii) there exist q, r, s, s_1, s_2 such that $q = \frac{3 \cdot a_1 - a_2{}^2}{9}$ and $r = \frac{9 \cdot a_2 \cdot a_1 - 2 \cdot a_2{}^3 - 27 \cdot a_0}{54}$ and $s = \sqrt[2]{q^3 + r^2}$ and $s_1 = \sqrt[3]{r + s}$ and $s_2 = -\frac{q}{s_1}$ and $\rho_1(a_0, a_1, a_2) = (s_1 + s_2) - \frac{a_2}{3}$, otherwise.

The functor $\rho_2(a_0, a_1, a_2)$ yielding a complex number is defined as follows:

(Def. 3)(i) There exist r, s_1 such that $r = \frac{9 \cdot a_2 \cdot a_1 - 2 \cdot a_2{}^3 - 27 \cdot a_0}{54}$ and $s_1 = \sqrt[3]{2 \cdot r}$ and $\rho_2(a_0, a_1, a_2) = (-\frac{s_1}{2} - \frac{a_2}{3}) + \frac{s_1 \cdot \sqrt[2]{3} \cdot i}{2}$ if $3 \cdot a_1 - a_2{}^2 = 0$,

(ii) there exist q, r, s, s_1, s_2 such that $q = \frac{3 \cdot a_1 - a_2{}^2}{9}$ and $r = \frac{9 \cdot a_2 \cdot a_1 - 2 \cdot a_2{}^3 - 27 \cdot a_0}{54}$ and $s = \sqrt[2]{q^3 + r^2}$ and $s_1 = \sqrt[3]{r + s}$ and $s_2 = -\frac{q}{s_1}$ and $\rho_2(a_0, a_1, a_2) = (-\frac{s_1 + s_2}{2} - \frac{a_2}{3}) + \frac{(s_1 - s_2) \cdot \sqrt[2]{3} \cdot i}{2}$, otherwise.

The functor $\rho_3(a_0, a_1, a_2)$ yielding a complex number is defined as follows:

(Def. 4)(i) There exist r, s_1 such that $r = \frac{9 \cdot a_2 \cdot a_1 - 2 \cdot a_2{}^3 - 27 \cdot a_0}{54}$ and $s_1 = \sqrt[3]{2 \cdot r}$ and $\rho_3(a_0, a_1, a_2) = -\frac{s_1}{2} - \frac{a_2}{3} - \frac{s_1 \cdot \sqrt[2]{3} \cdot i}{2}$ if $3 \cdot a_1 - a_2{}^2 = 0$,

(ii) there exist q, r, s, s_1, s_2 such that $q = \frac{3 \cdot a_1 - a_2{}^2}{9}$ and $r = \frac{9 \cdot a_2 \cdot a_1 - 2 \cdot a_2{}^3 - 27 \cdot a_0}{54}$ and $s = \sqrt[2]{q^3 + r^2}$ and $s_1 = \sqrt[3]{r + s}$ and $s_2 = -\frac{q}{s_1}$ and $\rho_3(a_0, a_1, a_2) = -\frac{s_1 + s_2}{2} - \frac{a_2}{3} - \frac{(s_1 - s_2) \cdot \sqrt[2]{3} \cdot i}{2}$, otherwise.

Next we state four propositions:

(17) $\rho_1(a_0, a_1, a_2) + \rho_2(a_0, a_1, a_2) + \rho_3(a_0, a_1, a_2) = -a_2$.

(18) $\rho_1(a_0, a_1, a_2) \cdot \rho_2(a_0, a_1, a_2) + \rho_1(a_0, a_1, a_2) \cdot \rho_3(a_0, a_1, a_2) + \rho_2(a_0, a_1, a_2) \cdot \rho_3(a_0, a_1, a_2) = a_1$.

(19) $\rho_1(a_0, a_1, a_2) \cdot \rho_2(a_0, a_1, a_2) \cdot \rho_3(a_0, a_1, a_2) = -a_0$.

(20) If $a_3 \neq 0$, then $a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0 = 0$ iff $z = \rho_1(\frac{a_0}{a_3}, \frac{a_1}{a_3}, \frac{a_2}{a_3})$ or $z = \rho_2(\frac{a_0}{a_3}, \frac{a_1}{a_3}, \frac{a_2}{a_3})$ or $z = \rho_3(\frac{a_0}{a_3}, \frac{a_1}{a_3}, \frac{a_2}{a_3})$.

4. Solution of Quartic Equations

In the sequel a_4, p, s_4 denote complex numbers.

The following propositions are true:

(21) Suppose $z = x - \frac{a_3}{4}$ and $p = \frac{8 \cdot a_2 - 3 \cdot a_3{}^2}{32}$ and $q = \frac{(8 \cdot a_1 - 4 \cdot a_2 \cdot a_3) + a_3{}^3}{64}$ and $r = \frac{((256 \cdot a_0 - 64 \cdot a_3 \cdot a_1) + 16 \cdot a_3{}^2 \cdot a_2) - 3 \cdot a_3{}^4}{1024}$. Then $z^4 + a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0 = 0$ if and only if $x^4 + 4 \cdot p \cdot x^2 + 8 \cdot q \cdot x + 4 \cdot r = 0$.

(22) Suppose $a_3 = -(s_1 + s_2 + s_3 + s_4)$ and $a_2 = s_1 \cdot s_2 + s_1 \cdot s_3 + s_1 \cdot s_4 + s_2 \cdot s_3 + s_2 \cdot s_4 + s_3 \cdot s_4$ and $a_1 = -(s_1 \cdot s_2 \cdot s_3 + s_1 \cdot s_2 \cdot s_4 + s_1 \cdot s_3 \cdot s_4 + s_2 \cdot s_3 \cdot s_4)$ and $a_0 = s_1 \cdot s_2 \cdot s_3 \cdot s_4$. Then $z^4 + a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0 = 0$ if and only if $z = s_1$ or $z = s_2$ or $z = s_3$ or $z = s_4$.

(23) Suppose $q \neq 0$ and $s_1 = \sqrt[2]{\rho_1(-q^2, p^2 - r, 2 \cdot p)}$ and $s_2 = \sqrt[2]{\rho_2(-q^2, p^2 - r, 2 \cdot p)}$ and $s_3 = -\frac{q}{s_1 \cdot s_2}$. Then $z^4 + 4 \cdot p \cdot z^2 + 8 \cdot q \cdot z + 4 \cdot r = 0$ if and only if $z = s_1 + s_2 + s_3$ or $z = s_1 - s_2 - s_3$ or $z = (-s_1 + s_2) - s_3$ or $z = (-s_1 - s_2) + s_3$.

(24) Suppose that $p = \frac{8 \cdot a_2 - 3 \cdot {a_3}^2}{32}$ and $q = \frac{(8 \cdot a_1 - 4 \cdot a_2 \cdot a_3) + {a_3}^3}{64}$ and $q \neq 0$ and $r = \frac{((256 \cdot a_0 - 64 \cdot a_3 \cdot a_1) + 16 \cdot {a_3}^2 \cdot a_2) - 3 \cdot {a_3}^4}{1024}$ and $s_1 = \sqrt[2]{\rho_1(-q^2, p^2 - r, 2 \cdot p)}$ and $s_2 = \sqrt[2]{\rho_2(-q^2, p^2 - r, 2 \cdot p)}$ and $s_3 = -\frac{q}{s_1 \cdot s_2}$. Then $z^4 + a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0 = 0$ if and only if $z = (s_1 + s_2 + s_3) - \frac{a_3}{4}$ or $z = s_1 - s_2 - s_3 - \frac{a_3}{4}$ or $z = (-s_1 + s_2) - s_3 - \frac{a_3}{4}$ or $z = ((-s_1 - s_2) + s_3) - \frac{a_3}{4}$.

(25) Suppose $p = \frac{8 \cdot a_2 - 3 \cdot {a_3}^2}{32}$ and $q = \frac{(8 \cdot a_1 - 4 \cdot a_2 \cdot a_3) + {a_3}^3}{64}$ and $q = 0$ and $r = \frac{((256 \cdot a_0 - 64 \cdot a_3 \cdot a_1) + 16 \cdot {a_3}^2 \cdot a_2) - 3 \cdot {a_3}^4}{1024}$ and $s_1 = \sqrt[2]{p^2 - r}$. Then $z^4 + a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0 = 0$ if and only if one of the following conditions is satisfied:

(i) $z = \sqrt[2]{-2 \cdot (p - s_1)} - \frac{a_3}{4}$, or

(ii) $z = -\sqrt[2]{-2 \cdot (p - s_1)} - \frac{a_3}{4}$, or

(iii) $z = \sqrt[2]{-2 \cdot (p + s_1)} - \frac{a_3}{4}$, or

(iv) $z = -\sqrt[2]{-2 \cdot (p + s_1)} - \frac{a_3}{4}$.

Let a_0, a_1, a_2, a_3 be complex numbers. The functor $\rho_1(a_0, a_1, a_2, a_3)$ yielding a complex number is defined by:

(Def. 5)(i) There exist p, r, s_1 such that $p = \frac{8 \cdot a_2 - 3 \cdot {a_3}^2}{32}$ and $r = \frac{((256 \cdot a_0 - 64 \cdot a_3 \cdot a_1) + 16 \cdot {a_3}^2 \cdot a_2) - 3 \cdot {a_3}^4}{1024}$ and $s_1 = \sqrt[2]{p^2 - r}$ and $\rho_1(a_0, a_1, a_2, a_3) = \sqrt[2]{-2 \cdot (p - s_1)} - \frac{a_3}{4}$ if $(8 \cdot a_1 - 4 \cdot a_2 \cdot a_3) + {a_3}^3 = 0$,

(ii) there exist p, q, r, s_1, s_2, s_3 such that $p = \frac{8 \cdot a_2 - 3 \cdot {a_3}^2}{32}$ and $q = \frac{(8 \cdot a_1 - 4 \cdot a_2 \cdot a_3) + {a_3}^3}{64}$ and $r = \frac{((256 \cdot a_0 - 64 \cdot a_3 \cdot a_1) + 16 \cdot {a_3}^2 \cdot a_2) - 3 \cdot {a_3}^4}{1024}$ and $s_1 = \sqrt[2]{\rho_1(-q^2, p^2 - r, 2 \cdot p)}$ and $s_2 = \sqrt[2]{\rho_2(-q^2, p^2 - r, 2 \cdot p)}$ and $s_3 = -\frac{q}{s_1 \cdot s_2}$ and $\rho_1(a_0, a_1, a_2, a_3) = (s_1 + s_2 + s_3) - \frac{a_3}{4}$, otherwise.

The functor $\rho_2(a_0, a_1, a_2, a_3)$ yielding a complex number is defined by:

(Def. 6)(i) There exist p, r, s_1 such that $p = \frac{8 \cdot a_2 - 3 \cdot {a_3}^2}{32}$ and $r = \frac{((256 \cdot a_0 - 64 \cdot a_3 \cdot a_1) + 16 \cdot {a_3}^2 \cdot a_2) - 3 \cdot {a_3}^4}{1024}$ and $s_1 = \sqrt[2]{p^2 - r}$ and $\rho_2(a_0, a_1, a_2, a_3) = -\sqrt[2]{-2 \cdot (p - s_1)} - \frac{a_3}{4}$ if $(8 \cdot a_1 - 4 \cdot a_2 \cdot a_3) + {a_3}^3 = 0$,

(ii) there exist p, q, r, s_1, s_2, s_3 such that $p = \frac{8 \cdot a_2 - 3 \cdot {a_3}^2}{32}$ and $q = \frac{(8 \cdot a_1 - 4 \cdot a_2 \cdot a_3) + {a_3}^3}{64}$ and $r = \frac{((256 \cdot a_0 - 64 \cdot a_3 \cdot a_1) + 16 \cdot {a_3}^2 \cdot a_2) - 3 \cdot {a_3}^4}{1024}$ and $s_1 = \sqrt[2]{\rho_1(-q^2, p^2 - r, 2 \cdot p)}$ and $s_2 = \sqrt[2]{\rho_2(-q^2, p^2 - r, 2 \cdot p)}$ and $s_3 = -\frac{q}{s_1 \cdot s_2}$ and $\rho_2(a_0, a_1, a_2, a_3) = ((-s_1 - s_2) + s_3) - \frac{a_3}{4}$, otherwise.

The functor $\rho_3(a_0, a_1, a_2, a_3)$ yielding a complex number is defined by:

(Def. 7)(i) There exist p, r, s_1 such that $p = \frac{8 \cdot a_2 - 3 \cdot {a_3}^2}{32}$ and $r = \frac{((256 \cdot a_0 - 64 \cdot a_3 \cdot a_1) + 16 \cdot {a_3}^2 \cdot a_2) - 3 \cdot {a_3}^4}{1024}$ and $s_1 = \sqrt[2]{p^2 - r}$ and $\rho_3(a_0, a_1, a_2, a_3) = \sqrt[2]{-2 \cdot (p + s_1)} - \frac{a_3}{4}$ if $(8 \cdot a_1 - 4 \cdot a_2 \cdot a_3) + {a_3}^3 = 0$,

(ii) there exist p, q, r, s_1, s_2, s_3 such that $p = \frac{8 \cdot a_2 - 3 \cdot {a_3}^2}{32}$ and

$q = \frac{(8 \cdot a_1 - 4 \cdot a_2 \cdot a_3) + {a_3}^3}{64}$ and $r = \frac{((256 \cdot a_0 - 64 \cdot a_3 \cdot a_1) + 16 \cdot {a_3}^2 \cdot a_2) - 3 \cdot {a_3}^4}{1024}$ and $s_1 = \sqrt[2]{\rho_1(-q^2, p^2 - r, 2 \cdot p)}$ and $s_2 = \sqrt[2]{\rho_2(-q^2, p^2 - r, 2 \cdot p)}$ and $s_3 = -\frac{q}{s_1 \cdot s_2}$ and $\rho_3(a_0, a_1, a_2, a_3) = (-s_1 + s_2) - s_3 - \frac{a_3}{4}$, otherwise.

The functor $\rho_4(a_0, a_1, a_2, a_3)$ yielding a complex number is defined by:

(Def. 8)(i) There exist p, r, s_1 such that $p = \frac{8 \cdot a_2 - 3 \cdot {a_3}^2}{32}$ and $r = \frac{((256 \cdot a_0 - 64 \cdot a_3 \cdot a_1) + 16 \cdot {a_3}^2 \cdot a_2) - 3 \cdot {a_3}^4}{1024}$ and $s_1 = \sqrt[2]{p^2 - r}$ and $\rho_4(a_0, a_1, a_2, a_3) = -\sqrt[2]{-2 \cdot (p + s_1)} - \frac{a_3}{4}$ if $(8 \cdot a_1 - 4 \cdot a_2 \cdot a_3) + {a_3}^3 = 0$,

(ii) there exist p, q, r, s_1, s_2, s_3 such that $p = \frac{8 \cdot a_2 - 3 \cdot {a_3}^2}{32}$ and $q = \frac{(8 \cdot a_1 - 4 \cdot a_2 \cdot a_3) + {a_3}^3}{64}$ and $r = \frac{((256 \cdot a_0 - 64 \cdot a_3 \cdot a_1) + 16 \cdot {a_3}^2 \cdot a_2) - 3 \cdot {a_3}^4}{1024}$ and $s_1 = \sqrt[2]{\rho_1(-q^2, p^2 - r, 2 \cdot p)}$ and $s_2 = \sqrt[2]{\rho_2(-q^2, p^2 - r, 2 \cdot p)}$ and $s_3 = -\frac{q}{s_1 \cdot s_2}$ and $\rho_4(a_0, a_1, a_2, a_3) = s_1 - s_2 - s_3 - \frac{a_3}{4}$, otherwise.

One can prove the following propositions:

(26) $\rho_1(a_0, a_1, a_2, a_3) + \rho_2(a_0, a_1, a_2, a_3) + \rho_3(a_0, a_1, a_2, a_3) + \rho_4(a_0, a_1, a_2, a_3) = -a_3$.

(27) $\rho_1(a_0, a_1, a_2, a_3) \cdot \rho_2(a_0, a_1, a_2, a_3) + \rho_1(a_0, a_1, a_2, a_3) \cdot \rho_3(a_0, a_1, a_2, a_3) + \rho_1(a_0, a_1, a_2, a_3) \cdot \rho_4(a_0, a_1, a_2, a_3) + \rho_2(a_0, a_1, a_2, a_3) \cdot \rho_3(a_0, a_1, a_2, a_3) + \rho_2(a_0, a_1, a_2, a_3) \cdot \rho_4(a_0, a_1, a_2, a_3) + \rho_3(a_0, a_1, a_2, a_3) \cdot \rho_4(a_0, a_1, a_2, a_3) = a_2$.

(28) $\rho_1(a_0, a_1, a_2, a_3) \cdot \rho_2(a_0, a_1, a_2, a_3) \cdot \rho_3(a_0, a_1, a_2, a_3) + \rho_1(a_0, a_1, a_2, a_3) \cdot \rho_2(a_0, a_1, a_2, a_3) \cdot \rho_4(a_0, a_1, a_2, a_3) + \rho_1(a_0, a_1, a_2, a_3) \cdot \rho_3(a_0, a_1, a_2, a_3) \cdot \rho_4(a_0, a_1, a_2, a_3) + \rho_2(a_0, a_1, a_2, a_3) \cdot \rho_3(a_0, a_1, a_2, a_3) \cdot \rho_4(a_0, a_1, a_2, a_3) = -a_1$.

(29) $\rho_1(a_0, a_1, a_2, a_3) \cdot \rho_2(a_0, a_1, a_2, a_3) \cdot \rho_3(a_0, a_1, a_2, a_3) \cdot \rho_4(a_0, a_1, a_2, a_3) = a_0$.

(30) Suppose $a_4 \neq 0$. Then $a_4 \cdot z^4 + a_3 \cdot z^3 + a_2 \cdot z^2 + a_1 \cdot z + a_0 = 0$ if and only if $z = \rho_1(\frac{a_0}{a_4}, \frac{a_1}{a_4}, \frac{a_2}{a_4}, \frac{a_3}{a_4})$ or $z = \rho_2(\frac{a_0}{a_4}, \frac{a_1}{a_4}, \frac{a_2}{a_4}, \frac{a_3}{a_4})$ or $z = \rho_3(\frac{a_0}{a_4}, \frac{a_1}{a_4}, \frac{a_2}{a_4}, \frac{a_3}{a_4})$ or $z = \rho_4(\frac{a_0}{a_4}, \frac{a_1}{a_4}, \frac{a_2}{a_4}, \frac{a_3}{a_4})$.

References

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

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

[3] Yuzhong Ding and Xiquan Liang. Solving roots of polynomial equation of degree 2 and 3 with complex coefficients. *Formalized Mathematics*, 12(**2**):85–92, 2004.

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

[5] G.A. Korn and T.M. Korn. *Mathematical Handbook for Scientists and Engineers.* Dover Publication, New York, 2000.

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

[7] Robert Milewski. Trigonometric form of complex numbers. *Formalized Mathematics*, 9(**3**):455–460, 2001.

[8] Jan Popiołek. Quadratic inequalities. *Formalized Mathematics*, 2(**4**):507–509, 1991.

[9] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.

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

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

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

Received March 3, 2009

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 123–128, 2009

The Perfect Number Theorem and Wilson's Theorem

Marco Riccardi
Casella Postale 49
54038 Montignoso, Italy

Summary. This article formalizes proofs of some elementary theorems of number theory (see [1, 26]): Wilson's theorem (that n is prime iff $n > 1$ and $(n-1)! \cong -1 \pmod{n}$), that all primes (1 mod 4) equal the sum of two squares, and two basic theorems of Euclid and Euler about perfect numbers. The article also formally defines Euler's sum of divisors function ϕ, proves that ϕ is multiplicative and that $\sum_{k|n} \phi(k) = n$.

MML identifier: NAT_5, version: 7.11.02 4.120.1050

The notation and terminology used in this paper are introduced in the following articles: [14], [38], [28], [32], [39], [11], [40], [13], [33], [12], [5], [4], [2], [6], [10], [37], [36], [25], [3], [15], [19], [35], [24], [30], [18], [34], [16], [9], [22], [21], [41], [17], [20], [7], [31], [29], [8], [23], and [27].

1. Preliminaries

We adopt the following convention: k, n, m, l, p denote natural numbers and n_0, m_0 denote non zero natural numbers.

We now state several propositions:

(1) $2^{n+1} < 2^{n+2} - 1$.

(2) If n_0 is even, then there exist k, m such that m is odd and $k > 0$ and $n_0 = 2^k \cdot m$.

(3) If $n = 2^k$ and m is odd, then n and m are relative prime.

(4) $\{n\}$ is a finite subset of $\mathbb{N}$.

(5) $\{n, m\}$ is a finite subset of $\mathbb{N}$.

ISSN 1426–2630(p), 1898-9934(e)

In the sequel f is a finite sequence and x, X, Y are sets.

The following four propositions are true:

(6) If f is one-to-one, then $f_{\restriction n}$ is one-to-one.

(7) If f is one-to-one and $n \in \operatorname{dom} f$, then $f(n) \notin \operatorname{rng}(f_{\restriction n})$.

(8) If $x \in \operatorname{rng} f$ and $x \notin \operatorname{rng}(f_{\restriction n})$, then $x = f(n)$.

(9) Let f_1 be a finite sequence of elements of $\mathbb{N}$ and f_2 be a finite sequence of elements of X. If $\operatorname{rng} f_1 \subseteq \operatorname{dom} f_2$, then $f_2 \cdot f_1$ is a finite sequence of elements of X.

In the sequel f_1, f_2, f_3 are finite sequences of elements of $\mathbb{R}$.

Next we state four propositions:

(10) If $X \cup Y = \operatorname{dom} f_1$ and X misses Y and $f_2 = f_1 \cdot \operatorname{Sgm} X$ and $f_3 = f_1 \cdot \operatorname{Sgm} Y$, then $\sum f_1 = \sum f_2 + \sum f_3$.

(11) If $f_2 = f_1 \cdot \operatorname{Sgm} X$ and $\operatorname{dom} f_1 \setminus {f_1}^{-1}(\{0\}) \subseteq X \subseteq \operatorname{dom} f_1$, then $\sum f_1 = \sum f_2$.

(12) $\sum f_1 = \sum (f_1 - \{0\})$.

(13) Every finite sequence of elements of $\mathbb{N}$ is a finite sequence of elements of $\mathbb{R}$.

In the sequel n_1, n_2, m_1, m_2 denote natural numbers.

We now state several propositions:

(14) If $n_1 \in \operatorname{NatDivisors} n$ and $m_1 \in \operatorname{NatDivisors} m$ and n and m are relative prime, then n_1 and m_1 are relative prime.

(15) If $n_1 \in \operatorname{NatDivisors} n$ and $m_1 \in \operatorname{NatDivisors} m$ and $n_2 \in \operatorname{NatDivisors} n$ and $m_2 \in \operatorname{NatDivisors} m$ and n and m are relative prime and $n_1 \cdot m_1 = n_2 \cdot m_2$, then $n_1 = n_2$ and $m_1 = m_2$.

(16) If $n_1 \in \operatorname{NatDivisors} n_0$ and $m_1 \in \operatorname{NatDivisors} m_0$, then $n_1 \cdot m_1 \in \operatorname{NatDivisors}(n_0 \cdot m_0)$.

(17) If n_0 and m_0 are relative prime, then $k \gcd n_0 {\cdot} m_0 = (k \gcd n_0) {\cdot} (k \gcd m_0)$.

(18) If n_0 and m_0 are relative prime and $k \in \operatorname{NatDivisors}(n_0 \cdot m_0)$, then there exist n_1, m_1 such that $n_1 \in \operatorname{NatDivisors} n_0$ and $m_1 \in \operatorname{NatDivisors} m_0$ and $k = n_1 \cdot m_1$.

(19) If p is prime, then $\operatorname{NatDivisors}(p^n) = \{p^k; k$ ranges over elements of $\mathbb{N}$: $k \leq n\}$.

(20) If $0 \neq l$ and $p > l$ and $p > n_1$ and $p > n_2$ and $l \cdot n_1 \bmod p = l \cdot n_2 \bmod p$ and p is prime, then $n_1 = n_2$.

(21) If p is prime, then $p\text{-count}(n_0 \gcd m_0) = \min(p\text{-count}(n_0), p\text{-count}(m_0))$.

2. Wilson's Theorem

One can prove the following proposition

(22) n is prime iff $((n -' 1)! + 1) \bmod n = 0$ and $n > 1$.

3. All Primes Congruent to 1 Modulo 4 are the Sum of Two Squares

The following proposition is true

(23) If p is prime and $p \bmod 4 = 1$, then there exist n, m such that $p = n^{\mathbf{2}}+m^{\mathbf{2}}$.

4. The Sum of Divisors Function

Let I be a set, let f be a function from I into $\mathbb{N}$, and let J be a finite subset of I. Then $f{\restriction}J$ is a bag of J.

Let I be a set, let f be a function from I into $\mathbb{N}$, and let J be a finite subset of I. Observe that $\sum(f{\restriction}J)$ is natural.

The following propositions are true:

(24) Let f be a function from $\mathbb{N}$ into $\mathbb{N}$, F be a function from $\mathbb{N}$ into $\mathbb{R}$, and J be a finite subset of $\mathbb{N}$. If $f = F$ and there exists k such that $J \subseteq \operatorname{Seg} k$, then $\sum(f{\restriction}J) = \sum \operatorname{FuncSeq}(F, \operatorname{Sgm} J)$.

(25) Let I be a non empty set, F be a partial function from I to $\mathbb{R}$, f be a function from I into $\mathbb{N}$, and J be a finite subset of I. If $f = F$, then $\sum(f{\restriction}J) = \sum_{\kappa=0}^{J} F(\kappa)$.

We use the following convention: I, j are sets, f, g are functions from I into $\mathbb{N}$, and J, K are finite subsets of I.

Next we state three propositions:

(26) If J misses K, then $\sum(f{\restriction}(J \cup K)) = \sum(f{\restriction}J) + \sum(f{\restriction}K)$.

(27) $\sum(f{\restriction}(\{j\})) = f(j)$.

(28) $\sum((\cdot_{\mathbb{N}} \cdot (f \times g)){\restriction}(J \times K)) = \sum(f{\restriction}J) \cdot \sum(g{\restriction}K)$.

Let k be a natural number. The functor $\operatorname{EXP} k$ yields a function from $\mathbb{N}$ into $\mathbb{N}$ and is defined by:

(Def. 1) For every natural number n holds $(\operatorname{EXP} k)(n) = n^k$.

Let k, n be natural numbers. The functor $\sigma_k(n)$ yielding an element of $\mathbb{N}$ is defined by:

(Def. 2)(i) For every non zero natural number m such that $n = m$ holds $\sigma_k(n) = \sum(\operatorname{EXP} k{\restriction}\operatorname{NatDivisors} m)$ if $n \neq 0$,

(ii) $\sigma_k(n) = 0$, otherwise.

Let k be a natural number. The functor Σk yields a function from $\mathbb{N}$ into $\mathbb{N}$ and is defined as follows:

(Def. 3) For every natural number n holds $(\Sigma k)(n) = \sigma_k(n)$.

Let n be a natural number. The functor $\sigma(n)$ yielding an element of $\mathbb{N}$ is defined by:

(Def. 4) $\sigma(n) = \sigma_1(n)$.

Next we state several propositions:

(29) $\sigma_k(1) = 1$.

(30) If p is prime, then $\sigma(p^n) = \frac{p^{n+1}-1}{p-1}$.

(31) If $m \mid n_0$ and $n_0 \neq m \neq 1$, then $1 + m + n_0 \leq \sigma(n_0)$.

(32) If $m \mid n_0$ and $k \mid n_0$ and $n_0 \neq m$ and $n_0 \neq k$ and $m \neq 1$ and $k \neq 1$ and $m \neq k$, then $1 + m + k + n_0 \leq \sigma(n_0)$.

(33) If $\sigma(n_0) = n_0 + m$ and $m \mid n_0$ and $n_0 \neq m$, then $m = 1$ and n_0 is prime.

Let f be a function from $\mathbb{N}$ into $\mathbb{N}$. We say that f is multiplicative if and only if:

(Def. 5) For all non zero natural numbers n_0, m_0 such that n_0 and m_0 are relative prime holds $f(n_0 \cdot m_0) = f(n_0) \cdot f(m_0)$.

Next we state four propositions:

(34) Let f, F be functions from $\mathbb{N}$ into $\mathbb{N}$. Suppose f is multiplicative and for every n_0 holds $F(n_0) = \sum(f \restriction \mathrm{NatDivisors}\, n_0)$. Then F is multiplicative.

(35) $\mathrm{EXP}\, k$ is multiplicative.

(36) Σk is multiplicative.

(37) If n_0 and m_0 are relative prime, then $\sigma(n_0 \cdot m_0) = \sigma(n_0) \cdot \sigma(m_0)$.

5. Two Basic Theorems on Perfect Numbers

Let n_0 be a non zero natural number. We say that n_0 is perfect if and only if:

(Def. 6) $\sigma(n_0) = 2 \cdot n_0$.

We now state two propositions:

(38) If $2^p -' 1$ is prime and $n_0 = 2^{p -' 1} \cdot (2^p -' 1)$, then n_0 is perfect.

(39) If n_0 is even and perfect, then there exists a natural number p such that $2^p -' 1$ is prime and $n_0 = 2^{p -' 1} \cdot (2^p -' 1)$.

6. A Formula Involving Euler's ϕ Function

The function ϕ from $\mathbb{N}$ into $\mathbb{N}$ is defined as follows:

(Def. 7) For every element k of $\mathbb{N}$ holds $\phi(k) = \mathrm{Euler}\, k$.

The following proposition is true

(40) $\sum(\phi \restriction \mathrm{NatDivisors}\, n_0) = n_0$.

References

[1] M. Aigner and G. M. Ziegler. *Proofs from THE BOOK.* Springer-Verlag, Berlin Heidelberg New York, 2004.

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

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

[4] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 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] Józef Białas. Infimum and supremum of the set of real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):163–171, 1991.

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

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

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

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

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

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

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

[15] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

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

[17] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6(**4**):549–551, 1997.

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

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

[20] Krzysztof Hryniewiecki. Recursive definitions. *Formalized Mathematics*, 1(**2**):321–328, 1990.

[21] Magdalena Jastrzębska and Adam Grabowski. On the properties of the Möbius function. *Formalized Mathematics*, 14(**1**):29–36, 2006, doi:10.2478/v10037-006-0005-0.

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

[23] Jarosław Kotowicz and Yuji Sakai. Properties of partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 3(**2**):279–288, 1992.

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

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

[26] W. J. LeVeque. *Fundamentals of Number Theory.* Dover Publication, New York, 1996.

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

[28] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[29] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**):49–58, 2004.
[30] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.
[31] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[32] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[33] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[34] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[35] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[36] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[37] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.
[38] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[39] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[40] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[41] Hiroshi Yamazaki, Yasunari Shidama, and Yatsuka Nakamura. Bessel's inequality. *Formalized Mathematics*, 11(**2**):169–173, 2003.

Received March 3, 2009

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 129–136, 2009

Probability on Finite Set and Real-Valued Random Variables

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In the various branches of science, probability and randomness provide us with useful theoretical frameworks. The *Formalized Mathematics* has already published some articles concerning the probability: [23], [24], [25], and [30]. In order to apply those articles, we shall give some theorems concerning the probability and the real-valued random variables to prepare for further studies.

MML identifier: `RANDOM_1`, version: `7.11.02 4.120.1050`

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

1. Probability on Finite Set

One can prove the following four propositions:

(1) Let X be a non empty set, S_1 be a σ-field of subsets of X, M be a σ-measure on S_1, f be a partial function from X to $\overline{\mathbb{R}}$, E be an element of S_1, and a be a real number. Suppose f is integrable on M and $E \subseteq \operatorname{dom} f$ and $M(E) < +\infty$ and for every element x of X such that $x \in E$ holds $a \leq f(x)$. Then $\overline{\mathbb{R}}(a) \cdot M(E) \leq \int f \restriction E \, \mathrm{d}M$.

(2) Let X be a non empty set, S_1 be a σ-field of subsets of X, M be a σ-measure on S_1, f be a partial function from X to $\mathbb{R}$, E be an element of S_1, and a be a real number. Suppose f is integrable on M and $E \subseteq \operatorname{dom} f$ and $M(E) < +\infty$ and for every element x of X such that $x \in E$ holds $a \leq f(x)$. Then $\overline{\mathbb{R}}(a) \cdot M(E) \leq \int f \restriction E \, \mathrm{d}M$.

ISSN 1426–2630(p), 1898-9934(e)

(3) Let X be a non empty set, S_1 be a σ-field of subsets of X, M be a σ-measure on S_1, f be a partial function from X to $\overline{\mathbb{R}}$, E be an element of S_1, and a be a real number. Suppose f is integrable on M and $E \subseteq \operatorname{dom} f$ and $M(E) < +\infty$ and for every element x of X such that $x \in E$ holds $f(x) \leq a$. Then $\int f{\restriction}E \, \mathrm{d}M \leq \overline{\mathbb{R}}(a) \cdot M(E)$.

(4) Let X be a non empty set, S_1 be a σ-field of subsets of X, M be a σ-measure on S_1, f be a partial function from X to $\mathbb{R}$, E be an element of S_1, and a be a real number. Suppose f is integrable on M and $E \subseteq \operatorname{dom} f$ and $M(E) < +\infty$ and for every element x of X such that $x \in E$ holds $f(x) \leq a$. Then $\int f{\restriction}E \, \mathrm{d}M \leq \overline{\mathbb{R}}(a) \cdot M(E)$.

2. Random Variables

For simplicity, we follow the rules: O is a non empty set, r is a real number, S is a σ-field of subsets of O, P is a probability on S, and E is a finite non empty set.

Let E be a non empty set. We introduce the trivial σ-field of E as a synonym of 2^E. Then the trivial σ-field of E is a σ-field of subsets of E.

Next we state a number of propositions:

(5) Let O be a non empty finite set and f be a partial function from O to $\mathbb{R}$. Then there exists a finite sequence F of separated subsets of the trivial σ-field of O and there exists a finite sequence s of elements of $\operatorname{dom} f$ such that
$\operatorname{dom} f = \bigcup \operatorname{rng} F$ and $\operatorname{dom} F = \operatorname{dom} s$ and s is one-to-one and $\operatorname{rng} s = \operatorname{dom} f$ and $\operatorname{len} s = \overline{\overline{\operatorname{dom} f}}$ and for every natural number k such that $k \in \operatorname{dom} F$ holds $F(k) = \{s(k)\}$ and for every natural number n and for all elements x, y of O such that $n \in \operatorname{dom} F$ and $x, y \in F(n)$ holds $f(x) = f(y)$.

(6) Let O be a non empty finite set and f be a partial function from O to $\mathbb{R}$. Then

(i) f is simple function in the trivial σ-field of O, and

(ii) $\operatorname{dom} f$ is an element of the trivial σ-field of O.

(7) Let O be a non empty finite set, M be a σ-measure on the trivial σ-field of O, and f be a partial function from O to $\mathbb{R}$. If $\operatorname{dom} f \neq \emptyset$ and $M(\operatorname{dom} f) < +\infty$, then f is integrable on M.

(8) Let O be a non empty finite set and f be a partial function from O to $\mathbb{R}$. Then there exists an element X of the trivial σ-field of O such that $\operatorname{dom} f = X$ and f is measurable on X.

(9) Let O be a non empty finite set, M be a σ-measure on the trivial σ-field of O, f be a function from O into $\mathbb{R}$, x be a finite sequence of elements of $\overline{\mathbb{R}}$, and s be a finite sequence of elements of O. Suppose $M(O) < +\infty$ and

s is one-to-one and $\operatorname{rng} s = O$ and $\operatorname{len} s = \overline{\overline{O}}$. Then there exists a finite sequence F of separated subsets of the trivial σ-field of O and there exists a finite sequence a of elements of $\mathbb{R}$ such that

(i) $\operatorname{dom} f = \bigcup \operatorname{rng} F$,

(ii) $\operatorname{dom} a = \operatorname{dom} s$,

(iii) $\operatorname{dom} F = \operatorname{dom} s$,

(iv) for every natural number k such that $k \in \operatorname{dom} F$ holds $F(k) = \{s(k)\}$, and

(v) for every natural number n and for all elements x, y of O such that $n \in \operatorname{dom} F$ and $x, y \in F(n)$ holds $f(x) = f(y)$.

(10) Let O be a non empty finite set, M be a σ-measure on the trivial σ-field of O, f be a function from O into $\mathbb{R}$, x be a finite sequence of elements of $\overline{\mathbb{R}}$, and s be a finite sequence of elements of O. Suppose that

(i) $M(O) < +\infty$,

(ii) $\operatorname{len} x = \overline{\overline{O}}$,

(iii) s is one-to-one,

(iv) $\operatorname{rng} s = O$,

(v) $\operatorname{len} s = \overline{\overline{O}}$, and

(vi) for every natural number n such that $n \in \operatorname{dom} x$ holds $x(n) = \overline{\mathbb{R}}(f(s(n))) \cdot M(\{s(n)\})$.

Then $\int f \,\mathrm{d}M = \sum x$.

(11) Let O be a non empty finite set, M be a σ-measure on the trivial σ-field of O, and f be a function from O into $\mathbb{R}$. Suppose $M(O) < +\infty$. Then there exists a finite sequence x of elements of $\overline{\mathbb{R}}$ and there exists a finite sequence s of elements of O such that

(i) $\operatorname{len} x = \overline{\overline{O}}$,

(ii) s is one-to-one,

(iii) $\operatorname{rng} s = O$,

(iv) $\operatorname{len} s = \overline{\overline{O}}$,

(v) for every natural number n such that $n \in \operatorname{dom} x$ holds $x(n) = \overline{\mathbb{R}}(f(s(n))) \cdot M(\{s(n)\})$, and

(vi) $\int f \,\mathrm{d}M = \sum x$.

(12) Let O be a non empty finite set, P be a probability on the trivial σ-field of O, f be a function from O into $\mathbb{R}$, x be a finite sequence of elements of $\mathbb{R}$, and s be a finite sequence of elements of O. Suppose that

(i) $\operatorname{len} x = \overline{\overline{O}}$,

(ii) s is one-to-one,

(iii) $\operatorname{rng} s = O$,

(iv) $\operatorname{len} s = \overline{\overline{O}}$, and

(v) for every natural number n such that $n \in \operatorname{dom} x$ holds $x(n) = f(s(n)) \cdot P(\{s(n)\})$.

Then $\int f \, \mathrm{d}\,\mathrm{P2M}\,P = \sum x$.

(13) Let O be a non empty finite set, P be a probability on the trivial σ-field of O, and f be a function from O into $\mathbb{R}$. Then there exists a finite sequence F of elements of $\mathbb{R}$ and there exists a finite sequence s of elements of O such that

(i) $\mathrm{len}\,F = \overline{\overline{O}}$,

(ii) s is one-to-one,

(iii) $\mathrm{rng}\,s = O$,

(iv) $\mathrm{len}\,s = \overline{\overline{O}}$,

(v) for every natural number n such that $n \in \mathrm{dom}\,F$ holds $F(n) = f(s(n)) \cdot P(\{s(n)\})$, and

(vi) $\int f \, \mathrm{d}\,\mathrm{P2M}\,P = \sum F$.

(14) Let E be a finite non empty set and A be a sequence of subsets of E. Suppose A is non-increasing. Then there exists an element N of $\mathbb{N}$ such that for every element m of $\mathbb{N}$ such that $N \leq m$ holds $A(N) = A(m)$.

(15) Let E be a finite non empty set and A be a sequence of subsets of E. Suppose A is non-increasing. Then there exists an element N of $\mathbb{N}$ such that for every element m of $\mathbb{N}$ such that $N \leq m$ holds $\mathrm{Intersection}\,A = A(m)$.

(16) Let E be a finite non empty set and A be a sequence of subsets of E. Suppose A is non-decreasing. Then there exists an element N of $\mathbb{N}$ such that for every element m of $\mathbb{N}$ such that $N \leq m$ holds $A(N) = A(m)$.

(17) Let E be a finite non empty set and A be a sequence of subsets of E. Suppose A is non-decreasing. Then there exists a natural number N such that for every natural number m such that $N \leq m$ holds $\bigcup A = A(m)$.

Let us consider E. The trivial probability of E yielding a probability on the trivial σ-field of E is defined as follows:

(Def. 1) For every event A_1 of E holds (the trivial probability of E)$(A_1) = \mathrm{P}(A_1)$.

Let us consider O, S. A function from O into $\mathbb{R}$ is said to be a real-valued random variable of S if:

(Def. 2) There exists an element X of S such that $X = O$ and it is measurable on X.

In the sequel f, g are real-valued random variables of S.

Next we state the proposition

(18) $f + g$ is a real-valued random variable of S.

Let us consider O, S, f, g. Then $f + g$ is a real-valued random variable of S.

We now state the proposition

(19) $f - g$ is a real-valued random variable of S.

Let us consider O, S, f, g. Then $f - g$ is a real-valued random variable of S.

Next we state the proposition

(20) For every real number r holds $r\,f$ is a real-valued random variable of S.

Let us consider O, S, f and let r be a real number. Then $r\,f$ is a real-valued random variable of S.

Next we state two propositions:

(21) For all partial functions f, g from O to $\mathbb{R}$ holds $\overline{\mathbb{R}}(f)\,\overline{\mathbb{R}}(g) = \overline{\mathbb{R}}(f\,g)$.

(22) $f\,g$ is a real-valued random variable of S.

Let us consider O, S, f, g. Then $f\,g$ is a real-valued random variable of S.

Next we state two propositions:

(23) For every real number r such that $0 \leq r$ and f is non-negative holds f^r is a real-valued random variable of S.

(24) $|f|$ is a real-valued random variable of S.

Let us consider O, S, f. Then $|f|$ is a real-valued random variable of S.

We now state the proposition

(25) For every real number r such that $0 \leq r$ holds $|f|^r$ is a real-valued random variable of S.

Let us consider O, S, f, P. We say that f is integrable on P if and only if:

(Def. 3) f is integrable on P2M P.

Let us consider O, S, P and let f be a real-valued random variable of S. Let us assume that f is integrable on P. The functor $E_P\{f\}$ yielding an element of $\mathbb{R}$ is defined as follows:

(Def. 4) $E_P\{f\} = \int f \,\mathrm{d}\,\mathrm{P2M}\,P$.

One can prove the following propositions:

(26) If f is integrable on P and g is integrable on P, then $E_P\{f+g\} = E_P\{f\} + E_P\{g\}$.

(27) If f is integrable on P, then $E_P\{r\,f\} = r \cdot E_P\{f\}$.

(28) If f is integrable on P and g is integrable on P, then $E_P\{f-g\} = E_P\{f\} - E_P\{g\}$.

(29) For every non empty finite set O holds every function from O into $\mathbb{R}$ is a real-valued random variable of the trivial σ-field of O.

(30) Let O be a non empty finite set, P be a probability on the trivial σ-field of O, and X be a real-valued random variable of the trivial σ-field of O. Then X is integrable on P.

(31) Let O be a non empty finite set, P be a probability on the trivial σ-field of O, X be a real-valued random variable of the trivial σ-field of O, F be a finite sequence of elements of $\mathbb{R}$, and s be a finite sequence of elements of O. Suppose that

(i) $\operatorname{len} F = \overline{\overline{O}}$,

(ii) s is one-to-one,

(iii) $\operatorname{rng} s = O$,

(iv) $\operatorname{len} s = \overline{\overline{O}}$, and

(v) for every natural number n such that $n \in \operatorname{dom} F$ holds $F(n) = X(s(n)) \cdot P(\{s(n)\})$.

Then $E_P\{X\} = \sum F$.

(32) Let O be a non empty finite set, P be a probability on the trivial σ-field of O, and X be a real-valued random variable of the trivial σ-field of O. Then there exists a finite sequence F of elements of $\mathbb{R}$ and there exists a finite sequence s of elements of O such that

(i) $\operatorname{len} F = \overline{\overline{O}}$,

(ii) s is one-to-one,

(iii) $\operatorname{rng} s = O$,

(iv) $\operatorname{len} s = \overline{\overline{O}}$,

(v) for every natural number n such that $n \in \operatorname{dom} F$ holds $F(n) = X(s(n)) \cdot P(\{s(n)\})$, and

(vi) $E_P\{X\} = \sum F$.

(33) Let O be a non empty finite set, P be a probability on the trivial σ-field of O, and X be a real-valued random variable of the trivial σ-field of O. Then there exists a finite sequence F of elements of $\mathbb{R}$ and there exists a finite sequence s of elements of O such that

(i) $\operatorname{len} F = \overline{\overline{O}}$,

(ii) s is one-to-one,

(iii) $\operatorname{rng} s = O$,

(iv) $\operatorname{len} s = \overline{\overline{O}}$,

(v) for every natural number n such that $n \in \operatorname{dom} F$ holds $F(n) = X(s(n)) \cdot P(\{s(n)\})$, and

(vi) $E_P\{X\} = \sum F$.

(34) Let O be a non empty finite set, X be a real-valued random variable of the trivial σ-field of O, G be a finite sequence of elements of $\mathbb{R}$, and s be a finite sequence of elements of O. Suppose $\operatorname{len} G = \overline{\overline{O}}$ and s is one-to-one and $\operatorname{rng} s = O$ and $\operatorname{len} s = \overline{\overline{O}}$ and for every natural number n such that $n \in \operatorname{dom} G$ holds $G(n) = X(s(n))$. Then $E_{\text{the trivial probability of } O}\{X\} = \frac{\sum G}{\overline{\overline{O}}}$.

(35) Let O be a non empty finite set and X be a real-valued random variable of the trivial σ-field of O. Then there exists a finite sequence G of elements of $\mathbb{R}$ and there exists a finite sequence s of elements of O such that

(i) $\operatorname{len} G = \overline{\overline{O}}$,

(ii) s is one-to-one,

(iii) $\operatorname{rng} s = O$,

(iv) $\operatorname{len} s = \overline{\overline{O}}$,

(v) for every natural number n such that $n \in \operatorname{dom} G$ holds $G(n) = X(s(n))$, and

(vi) $E_{\text{the trivial probability of } O}\{X\} = \frac{\sum G}{\overline{\overline{O}}}$.

(36) Let X be a real-valued random variable of S. Suppose $0 < r$ and X is non-negative and X is integrable on P. Then $P(\{t \in O\colon r \leq X(t)\}) \leq \frac{E_P\{X\}}{r}$.

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] Józef Białas. Infimum and supremum of the set of real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):163–171, 1991.

[6] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.

[7] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.

[8] Józef Białas. Some properties of the intervals. *Formalized Mathematics*, 5(**1**):21–26, 1996.

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

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

[13] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

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

[15] Noboru Endou and Yasunari Shidama. Integral of measurable function. *Formalized Mathematics*, 14(**2**):53–70, 2006, doi:10.2478/v10037-006-0008-x.

[16] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Basic properties of extended real numbers. *Formalized Mathematics*, 9(**3**):491–494, 2001.

[17] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definitions and basic properties of measurable functions. *Formalized Mathematics*, 9(**3**):495–500, 2001.

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

[19] Grigory E. Ivanov. Definition of convex function and Jensen's inequality. *Formalized Mathematics*, 11(**4**):349–354, 2003.

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

[21] Jarosław Kotowicz and Yuji Sakai. Properties of partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 3(**2**):279–288, 1992.

[22] Keiko Narita, Noboru Endou, and Yasunari Shidama. Integral of complex-valued measurable function. *Formalized Mathematics*, 16(**4**):319–324, 2008, doi:10.2478/v10037-008-0039-6.

[23] Andrzej Nędzusiak. Probability. *Formalized Mathematics*, 1(**4**):745–749, 1990.

[24] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.

[25] Jan Popiołek. Introduction to probability. *Formalized Mathematics*, 1(**4**):755–760, 1990.

[26] Yasunari Shidama and Noboru Endou. Integral of real-valued measurable function. *Formalized Mathematics*, 14(**4**):143–152, 2006, doi:10.2478/v10037-006-0018-8.

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

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

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

[30] Bo Zhang, Hiroshi Yamazaki, and Yatsuka Nakamura. The relevance of measure and probability, and definition of completeness of probability. *Formalized Mathematics*, 14(**4**):225–229, 2006, doi:10.2478/v10037-006-0026-8.

Received March 17, 2009

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 137–145, 2009

Lebesgue's Convergence Theorem of Complex-Valued Function

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 formalized Lebesgue's Convergence theorem of complex-valued function. We proved Lebesgue's Convergence Theorem of real-valued function using the theorem of extensional real-valued function. Then applying the former theorem to real part and imaginary part of complex-valued functional sequences, we proved Lebesgue's Convergence Theorem of complex-valued function. We also defined partial sums of real-valued functional sequences and complex-valued functional sequences and showed their properties. In addition, we proved properties of complex-valued simple functions.

MML identifier: MESFUN9C, version: 7.11.02 4.120.1050

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

1. Partial Sums of Real-Valued Functional Sequences

For simplicity, we follow the rules: X denotes a non empty set, S denotes a σ-field of subsets of X, M denotes a σ-measure on S, E denotes an element of S, F denotes a sequence of partial functions from X into $\mathbb{R}$, f denotes a partial function from X to $\mathbb{R}$, s denotes a sequence of real numbers, n, m denote natural numbers, x denotes an element of X, and z, D denote sets.

ISSN 1426–2630(p), 1898-9934(e)

Let X, Y be sets, let F be a sequence of partial functions from X into Y, and let D be a set. The functor $F \restriction D$ yielding a sequence of partial functions from X into Y is defined as follows:

(Def. 1) For every natural number n holds $(F \restriction D)(n) = F(n){\restriction}D$.

One can prove the following propositions:

(1) If $x \in D$ and $F\#x$ is convergent, then $(F \restriction D)\#x$ is convergent.

(2) Let X, Y, D be sets and F be a sequence of partial functions from X into Y. If F has the same dom, then $F \restriction D$ has the same dom.

(3) If $D \subseteq \operatorname{dom} F(0)$ and for every element x of X such that $x \in D$ holds $F\#x$ is convergent, then $\lim F{\restriction}D = \lim(F \restriction D)$.

(4) Suppose F has the same dom and $E \subseteq \operatorname{dom} F(0)$ and for every natural number m holds $F(m)$ is measurable on E. Then $(F \restriction E)(n)$ is measurable on E.

(5) $(\sum_{\alpha=0}^{\kappa}(\overline{\mathbb{R}}(s))(\alpha))_{\kappa\in\mathbb{N}} = \overline{\mathbb{R}}((\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}})$.

(6) Suppose that for every element x of X such that $x \in E$ holds $F\#x$ is summable. Let x be an element of X. If $x \in E$, then $(F \restriction E)\#x$ is summable.

Let X be a non empty set and let F be a sequence of partial functions from X into $\mathbb{R}$. The functor $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}$ yielding a sequence of partial functions from X into $\mathbb{R}$ is defined by:

(Def. 2) $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(0) = F(0)$ and for every element n of $\mathbb{N}$ holds $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n+1) = (\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n) + F(n+1)$.

Next we state a number of propositions:

(7) $(\sum_{\alpha=0}^{\kappa}(\overline{\mathbb{R}}(F))(\alpha))_{\kappa\in\mathbb{N}} = \overline{\mathbb{R}}((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}})$.

(8) If $z \in \operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)$ and $m \leq n$, then $z \in \operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(m)$ and $z \in \operatorname{dom} F(m)$.

(9) $\overline{\mathbb{R}}(F)$ is additive.

(10) $\operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n) = \bigcap\{\operatorname{dom} F(k); k$ ranges over elements of $\mathbb{N}$: $k \leq n\}$.

(11) If F has the same dom, then $\operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n) = \operatorname{dom} F(0)$.

(12) If F has the same dom and $D \subseteq \operatorname{dom} F(0)$ and $x \in D$, then $(\sum_{\alpha=0}^{\kappa}(F\#x)(\alpha))_{\kappa\in\mathbb{N}}(n) = ((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\#x)(n)$.

(13) If F has the same dom and $D \subseteq \operatorname{dom} F(0)$ and $x \in D$, then $(\sum_{\alpha=0}^{\kappa}(F\#x)(\alpha))_{\kappa\in\mathbb{N}}$ is convergent iff $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\#x$ is convergent.

(14) If F has the same dom and $\operatorname{dom} f \subseteq \operatorname{dom} F(0)$ and $x \in \operatorname{dom} f$ and $f(x) = \sum(F\#x)$, then $f(x) = \lim((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\#x)$.

(15) If for every natural number m holds $F(m)$ is simple function in S, then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)$ is simple function in S.

(16) If for every natural number n holds $F(n)$ is measurable on E, then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(m)$ is measurable on E.

(17) Let X be a non empty set and F be a sequence of partial functions from X into $\mathbb{R}$. If F has the same dom, then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}$ has the same dom.

(18) Suppose that

(i) $\operatorname{dom} F(0) = E$,

(ii) F has the same dom,

(iii) for every natural number n holds $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)$ is measurable on E, and

(iv) for every element x of X such that $x \in E$ holds $F\#x$ is summable.

Then $\lim((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}})$ is measurable on E.

(19) Suppose that for every natural number n holds $F(n)$ is integrable on M. Let m be a natural number. Then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(m)$ is integrable on M.

2. Partial Sums of Complex-Valued Functional Sequences

In the sequel F denotes a sequence of partial functions from X into $\mathbb{C}$, f denotes a partial function from X to $\mathbb{C}$, and A denotes a set.

We now state several propositions:

(20) $\Re(f){\restriction}A = \Re(f{\restriction}A)$ and $\Im(f){\restriction}A = \Im(f{\restriction}A)$.

(21) $\Re(F \restriction D) = \Re(F) \restriction D$.

(22) $\Im(F \restriction D) = \Im(F) \restriction D$.

(23) If F has the same dom and $D \subseteq \operatorname{dom} F(0)$ and $x \in D$, then if $F\#x$ is convergent, then $(F \restriction D)\#x$ is convergent.

(24) F has the same dom iff $\Re(F)$ has the same dom.

(25) $\Re(F)$ has the same dom iff $\Im(F)$ has the same dom.

(26) If F has the same dom and $D = \operatorname{dom} F(0)$ and for every element x of X such that $x \in D$ holds $F\#x$ is convergent, then $\lim F{\restriction}D = \lim(F \restriction D)$.

(27) Suppose F has the same dom and $E \subseteq \operatorname{dom} F(0)$ and for every natural number m holds $F(m)$ is measurable on E. Then $(F \restriction E)(n)$ is measurable on E.

(28) Suppose $E \subseteq \operatorname{dom} F(0)$ and F has the same dom and for every element x of X such that $x \in E$ holds $F\#x$ is summable. Let x be an element of X. If $x \in E$, then $(F \restriction E)\#x$ is summable.

Let X be a non empty set and let F be a sequence of partial functions from X into $\mathbb{C}$. The functor $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}$ yielding a sequence of partial functions from X into $\mathbb{C}$ is defined as follows:

(Def. 3) $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(0) = F(0)$ and for every natural number n holds $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n+1) = (\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n) + F(n+1)$.

Next we state a number of propositions:

(29) $(\sum_{\alpha=0}^{\kappa} \Re(F)(\alpha))_{\kappa\in\mathbb{N}} = \Re((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa}$, $(\sum_{\alpha=0}^{\kappa} \Im(F)(\alpha))_{\kappa\in\mathbb{N}} = \Im((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}})$.

(30) If $z \in \mathrm{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)$ and $m \leq n$, then $z \in \mathrm{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(m)$ and $z \in \mathrm{dom}\, F(m)$.

(31) $\mathrm{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n) = \bigcap\{\mathrm{dom}\, F(k); k$ ranges over elements of $\mathbb{N}$: $k \leq n\}$.

(32) If F has the same dom, then $\mathrm{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n) = \mathrm{dom}\, F(0)$.

(33) If F has the same dom and $D \subseteq \mathrm{dom}\, F(0)$ and $x \in D$, then $(\sum_{\alpha=0}^{\kappa}(F\#x)(\alpha))_{\kappa\in\mathbb{N}}(n) = ((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\#x)(n)$.

(34) If F has the same dom, then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}$ has the same dom.

(35) If F has the same dom and $D \subseteq \mathrm{dom}\, F(0)$ and $x \in D$, then $(\sum_{\alpha=0}^{\kappa}(F\#x)(\alpha))_{\kappa\in\mathbb{N}}$ is convergent iff $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\#x$ is convergent.

(36) If F has the same dom and $\mathrm{dom}\, f \subseteq \mathrm{dom}\, F(0)$ and $x \in \mathrm{dom}\, f$ and $F\#x$ is summable and $f(x) = \sum(F\#x)$, then $f(x) = \lim((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\#x)$.

(37) If for every natural number m holds $F(m)$ is simple function in S, then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)$ is simple function in S.

(38) If for every natural number n holds $F(n)$ is measurable on E, then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(m)$ is measurable on E.

(39) Suppose that

(i) $\mathrm{dom}\, F(0) = E$,

(ii) F has the same dom,

(iii) for every natural number n holds $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(n)$ is measurable on E, and

(iv) for every element x of X such that $x \in E$ holds $F\#x$ is summable.

Then $\lim((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}})$ is measurable on E.

(40) Suppose that for every natural number n holds $F(n)$ is integrable on M. Let m be a natural number. Then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}(m)$ is integrable on M.

3. Selected Properties of Complex-Valued Simple Functions

In the sequel f, g are partial functions from X to $\mathbb{C}$ and A is an element of S.

The following propositions are true:

(41) If f is simple function in S, then f is measurable on A.

(42) If f is simple function in S, then $f{\restriction}A$ is simple function in S.

(43) If f is simple function in S, then $\operatorname{dom} f$ is an element of S.

(44) If f is simple function in S and g is simple function in S, then $f+g$ is simple function in S.

(45) For every complex number c such that f is simple function in S holds $c\,f$ is simple function in S.

4. Lebesgue's Convergence Theorem of Complex-Valued Function

In the sequel F is a sequence of partial functions from X into $\overline{\mathbb{R}}$ with the same dom and P is a partial function from X to $\overline{\mathbb{R}}$.

Next we state the proposition

(46) Suppose that

(i) $E = \operatorname{dom} F(0)$,

(ii) $E = \operatorname{dom} P$,

(iii) for every natural number n holds $F(n)$ is measurable on E,

(iv) P is integrable on M,

(v) for every element x of X and for every natural number n such that $x \in E$ holds $|F(n)|(x) \leq P(x)$, and

(vi) for every element x of X such that $x \in E$ holds $F\#x$ is convergent.

Then $\lim F$ is integrable on M.

In the sequel F denotes a sequence of partial functions from X into $\mathbb{R}$ with the same dom and f, P denote partial functions from X to $\mathbb{R}$.

We now state two propositions:

(47) Suppose that

(i) $E = \operatorname{dom} F(0)$,

(ii) $E = \operatorname{dom} P$,

(iii) for every natural number n holds $F(n)$ is measurable on E,

(iv) P is integrable on M,

(v) for every element x of X and for every natural number n such that $x \in E$ holds $|F(n)|(x) \leq P(x)$, and

(vi) for every element x of X such that $x \in E$ holds $F\#x$ is convergent.

Then $\lim F$ is integrable on M.

(48) Suppose that

(i) $E = \operatorname{dom} F(0)$,

(ii) $E = \operatorname{dom} P$,

(iii) for every natural number n holds $F(n)$ is measurable on E,

(iv) P is integrable on M, and

(v) for every element x of X and for every natural number n such that $x \in E$ holds $|F(n)|(x) \leq P(x)$.

Then there exists a sequence I of real numbers such that

(vi) for every natural number n holds $I(n) = \int F(n)\,\mathrm{d}M$, and

(vii) if for every element x of X such that $x \in E$ holds $F\#x$ is convergent, then I is convergent and $\lim I = \int \lim F\,\mathrm{d}M$.

Let X be a set and let F be a sequence of partial functions from X into $\mathbb{R}$. We say that F is uniformly bounded if and only if the condition (Def. 4) is satisfied.

(Def. 4) There exists a real number K such that for every natural number n and for every element x of X if $x \in \operatorname{dom} F(0)$, then $|F(n)(x)| \leq K$.

We now state the proposition

(49) Suppose that

(i) $M(E) < +\infty$,

(ii) $E = \operatorname{dom} F(0)$,

(iii) for every natural number n holds $F(n)$ is measurable on E,

(iv) F is uniformly bounded, and

(v) for every element x of X such that $x \in E$ holds $F\#x$ is convergent.

Then

(vi) for every natural number n holds $F(n)$ is integrable on M,

(vii) $\lim F$ is integrable on M, and

(viii) there exists a sequence I of extended reals such that for every natural number n holds $I(n) = \int F(n)\,\mathrm{d}M$ and I is convergent and $\lim I = \int \lim F\,\mathrm{d}M$.

Let X be a set, let F be a sequence of partial functions from X into $\mathbb{R}$, and let f be a partial function from X to $\mathbb{R}$. We say that F is uniformly convergent to f if and only if the conditions (Def. 5) are satisfied.

(Def. 5)(i) F has the same dom,

(ii) $\operatorname{dom} F(0) = \operatorname{dom} f$, and

(iii) for every real number e such that $e > 0$ there exists a natural number N such that for every natural number n and for every element x of X such that $n \geq N$ and $x \in \operatorname{dom} F(0)$ holds $|F(n)(x) - f(x)| < e$.

The following proposition is true

(50) Suppose that

(i) $M(E) < +\infty$,

(ii) $E = \operatorname{dom} F(0)$,

(iii) for every natural number n holds $F(n)$ is integrable on M, and

(iv) F is uniformly convergent to f.

Then

(v) f is integrable on M, and

(vi) there exists a sequence I of extended reals such that for every natural number n holds $I(n) = \int F(n)\,\mathrm{d}M$ and I is convergent and $\lim I = \int f\,\mathrm{d}M$.

In the sequel F denotes a sequence of partial functions from X into $\mathbb{C}$ with the same dom and f denotes a partial function from X to $\mathbb{C}$.

The following propositions are true:

(51) Suppose that

(i) $E = \operatorname{dom} F(0)$,

(ii) $E = \operatorname{dom} P$,

(iii) for every natural number n holds $F(n)$ is measurable on E,

(iv) P is integrable on M,

(v) for every element x of X and for every natural number n such that $x \in E$ holds $|F(n)|(x) \leq P(x)$, and

(vi) for every element x of X such that $x \in E$ holds $F\#x$ is convergent.

Then $\lim F$ is integrable on M.

(52) Suppose that

(i) $E = \operatorname{dom} F(0)$,

(ii) $E = \operatorname{dom} P$,

(iii) for every natural number n holds $F(n)$ is measurable on E,

(iv) P is integrable on M, and

(v) for every element x of X and for every natural number n such that $x \in E$ holds $|F(n)|(x) \leq P(x)$.

Then there exists a complex sequence I such that

(vi) for every natural number n holds $I(n) = \int F(n)\,\mathrm{d}M$, and

(vii) if for every element x of X such that $x \in E$ holds $F\#x$ is convergent, then I is convergent and $\lim I = \int \lim F\,\mathrm{d}M$.

Let X be a set and let F be a sequence of partial functions from X into $\mathbb{C}$. We say that F is uniformly bounded if and only if the condition (Def. 6) is satisfied.

(Def. 6) There exists a real number K such that for every natural number n and for every element x of X if $x \in \operatorname{dom} F(0)$, then $|F(n)(x)| \leq K$.

Next we state the proposition

(53) Suppose that

(i) $M(E) < +\infty$,

(ii) $E = \operatorname{dom} F(0)$,

(iii) for every natural number n holds $F(n)$ is measurable on E,

(iv) F is uniformly bounded, and

(v) for every element x of X such that $x \in E$ holds $F\#x$ is convergent.

Then

(vi) for every natural number n holds $F(n)$ is integrable on M,

(vii) $\lim F$ is integrable on M, and

(viii) there exists a complex sequence I such that for every natural number n holds $I(n) = \int F(n)\,\mathrm{d}M$ and I is convergent and $\lim I = \int \lim F\,\mathrm{d}M$.

Let X be a set, let F be a sequence of partial functions from X into $\mathbb{C}$, and let f be a partial function from X to $\mathbb{C}$. We say that F is uniformly convergent to f if and only if the conditions (Def. 7) are satisfied.

(Def. 7)(i) F has the same dom,

(ii) $\operatorname{dom} F(0) = \operatorname{dom} f$, and

(iii) for every real number e such that $e > 0$ there exists a natural number N such that for every natural number n and for every element x of X such that $n \geq N$ and $x \in \operatorname{dom} F(0)$ holds $|F(n)(x) - f(x)| < e$.

Next we state the proposition

(54) Suppose that

(i) $M(E) < +\infty$,

(ii) $E = \operatorname{dom} F(0)$,

(iii) for every natural number n holds $F(n)$ is integrable on M, and

(iv) F is uniformly convergent to f.

Then

(v) f is integrable on M, and

(vi) there exists a complex sequence I such that for every natural number n holds $I(n) = \int F(n)\,\mathrm{d}M$ and I is convergent and $\lim I = \int f\,\mathrm{d}M$.

References

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

[2] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.

[3] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.

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

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

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

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

[8] 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.

[9] Noboru Endou and Yasunari Shidama. Integral of measurable function. *Formalized Mathematics*, 14(**2**):53–70, 2006, doi:10.2478/v10037-006-0008-x.

[10] Noboru Endou, Yasunari Shidama, and Keiko Narita. Egoroff's theorem. *Formalized Mathematics*, 16(**1**):57–63, 2008, doi:10.2478/v10037-008-0009-z.

[11] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definitions and basic properties of measurable functions. *Formalized Mathematics*, 9(**3**):495–500, 2001.

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

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

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

[15] Keiko Narita, Noboru Endou, and Yasunari Shidama. Integral of complex-valued measurable function. *Formalized Mathematics*, 16(**4**):319–324, 2008, doi:10.2478/v10037-008-0039-6.

[16] Keiko Narita, Noboru Endou, and Yasunari Shidama. The measurability of complex-valued functional sequences. *Formalized Mathematics*, 17(**2**):89–97, 2009, doi: 10.2478/v10037-009-0010-1.

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

[18] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.

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

[20] Beata Perkowska. Functional sequence from a domain to a domain. *Formalized Mathematics*, 3(**1**):17–21, 1992.

[21] Konrad Raczkowski and Andrzej Nędzusiak. Series. *Formalized Mathematics*, 2(**4**):449–452, 1991.

[22] Yasunari Shidama and Noboru Endou. Integral of real-valued measurable function. *Formalized Mathematics*, 14(**4**):143–152, 2006, doi:10.2478/v10037-006-0018-8.

[23] Yasunari Shidama and Artur Korniłowicz. Convergence and the limit of complex sequences. Series. *Formalized Mathematics*, 6(**3**):403–410, 1997.

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

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

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

Received March 17, 2009

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 147–149, 2009

The Cauchy-Riemann Differential Equations of Complex Functions

Hiroshi Yamazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Chanapat Pacharapokin
Shinshu University
Nagano, Japan

Yatsuka Nakamura
Shinshu University
Nagano, Japan

Summary. In this article we prove Cauchy-Riemann differential equations of complex functions. These theorems give necessary and sufficient condition for differentiable function.

MML identifier: CFDIFF_2, version: 7.11.02 4.125.1059

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

Let f be a partial function from $\mathbb{C}$ to $\mathbb{C}$. The functor $\Re(f)$ yields a partial function from $\mathbb{C}$ to $\mathbb{R}$ and is defined by:

(Def. 1) $\mathrm{dom}\, f = \mathrm{dom}\, \Re(f)$ and for every complex number z such that $z \in \mathrm{dom}\, \Re(f)$ holds $\Re(f)(z) = \Re(f_z)$.

Let f be a partial function from $\mathbb{C}$ to $\mathbb{C}$. The functor $\Im(f)$ yielding a partial function from $\mathbb{C}$ to $\mathbb{R}$ is defined by:

(Def. 2) $\mathrm{dom}\, f = \mathrm{dom}\, \Im(f)$ and for every complex number z such that $z \in \mathrm{dom}\, \Im(f)$ holds $\Im(f)(z) = \Im(f_z)$.

We now state several propositions:

(1) For every partial function f from $\mathbb{C}$ to $\mathbb{C}$ such that f is total holds $\mathrm{dom}\, \Re(f) = \mathbb{C}$ and $\mathrm{dom}\, \Im(f) = \mathbb{C}$.

ISSN 1426–2630(p), 1898-9934(e)

(2) Let f be a partial function from $\mathbb{C}$ to $\mathbb{C}$, u, v be partial functions from $\mathcal{R}^2$ to $\mathbb{R}$, z_0 be a complex number, x_0, y_0 be real numbers, and x_1 be an element of $\mathcal{R}^2$. Suppose that

(i) for all real numbers x, y such that $x+y\cdot i \in \operatorname{dom} f$ holds $\langle x, y\rangle \in \operatorname{dom} u$ and $u(\langle x, y\rangle) = \Re(f)(x + y \cdot i)$,

(ii) for all real numbers x, y such that $x+y\cdot i \in \operatorname{dom} f$ holds $\langle x, y\rangle \in \operatorname{dom} v$ and $v(\langle x, y\rangle) = \Im(f)(x + y \cdot i)$,

(iii) $z_0 = x_0 + y_0 \cdot i$,

(iv) $x_1 = \langle x_0, y_0\rangle$, and

(v) f is differentiable in z_0.

Then

(vi) u is partially differentiable in x_1 w.r.t. coordinate 1 and partially differentiable in x_1 w.r.t. coordinate 2,

(vii) v is partially differentiable in x_1 w.r.t. coordinate 1 and partially differentiable in x_1 w.r.t. coordinate 2,

(viii) $\Re(f'(z_0)) = \operatorname{partdiff}(u, x_1, 1)$,

(ix) $\Re(f'(z_0)) = \operatorname{partdiff}(v, x_1, 2)$,

(x) $\Im(f'(z_0)) = -\operatorname{partdiff}(u, x_1, 2)$, and

(xi) $\Im(f'(z_0)) = \operatorname{partdiff}(v, x_1, 1)$.

(3) For every sequence s of real numbers holds s is convergent and $\lim s = 0$ iff $|s|$ is convergent and $\lim|s| = 0$.

(4) Let X be a real normed space and s be a sequence of X. Then s is convergent and $\lim s = 0_X$ if and only if $\|s\|$ is convergent and $\lim\|s\| = 0$.

(5) Let u be a partial function from $\mathcal{R}^2$ to $\mathbb{R}$, x_0, y_0 be real numbers, and x_1 be an element of $\mathcal{R}^2$. Suppose $x_1 = \langle x_0, y_0\rangle$ and $\langle u\rangle$ is differentiable in x_1. Then

(i) u is partially differentiable in x_1 w.r.t. coordinate 1 and partially differentiable in x_1 w.r.t. coordinate 2,

(ii) $\langle \operatorname{partdiff}(u, x_1, 1)\rangle = \langle u\rangle'(x_1)(\langle 1, 0\rangle)$, and

(iii) $\langle \operatorname{partdiff}(u, x_1, 2)\rangle = \langle u\rangle'(x_1)(\langle 0, 1\rangle)$.

(6) Let f be a partial function from $\mathbb{C}$ to $\mathbb{C}$, u, v be partial functions from $\mathcal{R}^2$ to $\mathbb{R}$, z_0 be a complex number, x_0, y_0 be real numbers, and x_1 be an element of $\mathcal{R}^2$. Suppose that for all real numbers x, y such that $\langle x, y\rangle \in \operatorname{dom} v$ holds $x+y\cdot i \in \operatorname{dom} f$ and for all real numbers x, y such that $x+y\cdot i \in \operatorname{dom} f$ holds $\langle x, y\rangle \in \operatorname{dom} u$ and $u(\langle x, y\rangle) = \Re(f)(x + y \cdot i)$ and for all real numbers x, y such that $x+y\cdot i \in \operatorname{dom} f$ holds $\langle x, y\rangle \in \operatorname{dom} v$ and $v(\langle x, y\rangle) = \Im(f)(x+y\cdot i)$ and $z_0 = x_0 + y_0 \cdot i$ and $x_1 = \langle x_0, y_0\rangle$ and $\langle u\rangle$ is differentiable in x_1 and $\langle v\rangle$ is differentiable in x_1 and $\operatorname{partdiff}(u, x_1, 1) = \operatorname{partdiff}(v, x_1, 2)$ and $\operatorname{partdiff}(u, x_1, 2) = -\operatorname{partdiff}(v, x_1, 1)$. Then f is differentiable in z_0 and u is partially differentiable in x_1 w.r.t. coordinate 1 and partially differentiable in x_1 w.r.t. coordinate 2 and v is partially differentiable in

x_1 w.r.t. coordinate 1 and partially differentiable in x_1 w.r.t. coordinate 2 and $\Re(f'(z_0)) = \mathrm{partdiff}(u, x_1, 1)$ and $\Re(f'(z_0)) = \mathrm{partdiff}(v, x_1, 2)$ and $\Im(f'(z_0)) = -\mathrm{partdiff}(u, x_1, 2)$ and $\Im(f'(z_0)) = \mathrm{partdiff}(v, x_1, 1)$.

References

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

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

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

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

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

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

[9] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

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

[11] Noboru Endou and Yasunari Shidama. Completeness of the real Euclidean space. *Formalized Mathematics*, 13(**4**):577–580, 2005.

[12] Noboru Endou, Yasunari Shidama, and Keiichi Miyajima. Partial differentiation on normed linear spaces $\mathcal{R}^n$. *Formalized Mathematics*, 15(**2**):65–72, 2007, doi:10.2478/v10037-007-0008-5.

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

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

[15] Chanapat Pacharapokin, Hiroshi Yamazaki, Yasunari Shidama, and Yatsuka Nakamura. Complex function differentiability. *Formalized Mathematics*, 17(**2**):67–72, 2009, doi: 10.2478/v10037-009-0007-9.

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

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

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

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

[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 April 7, 2009

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 151–155, 2009

Properties of Primes and Multiplicative Group of a Field

Kenichi Arai
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. In the [16] has been proven that the multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$ is a cyclic group. Likewise, finite subgroup of the multiplicative group of a field is a cyclic group. However, finite subgroup of the multiplicative group of a field being a cyclic group has not yet been proven. Therefore, it is of importance to prove that finite subgroup of the multiplicative group of a field is a cyclic group.

Meanwhile, in cryptographic system like RSA, in which security basis depends upon the difficulty of factorization of given numbers into prime factors, it is important to employ integers that are difficult to be factorized into prime factors. If both p and $2p + 1$ are prime numbers, we call p as Sophie Germain prime, and $2p + 1$ as safe prime. It is known that the product of two safe primes is a composite number that is difficult for some factoring algorithms to factorize into prime factors. In addition, safe primes are also important in cryptography system because of their use in discrete logarithm based techniques like Diffie-Hellman key exchange. If p is a safe prime, the multiplicative group of numbers modulo p has a subgroup of large prime order. However, no definitions have not been established yet with the safe prime and Sophie Germain prime. So it is important to give definitions of the Sophie Germain prime and safe prime.

In this article, we prove finite subgroup of the multiplicative group of a field is a cyclic group, and, further, define the safe prime and Sophie Germain prime, and prove several facts about them. In addition, we define Mersenne number (M_n), and some facts about Mersenne numbers and prime numbers are proven.

MML identifier: GR_CY_3, version: 7.11.02 4.125.1059

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

ISSN 1426–2630(p), 1898-9934(e)

1. Properties of Primes

The following proposition is true

(1) For all prime numbers p, q and for every natural number k such that $k \mid p \cdot q$ holds $k = 1$ or $k = p$ or $k = q$ or $k = p \cdot q$.

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

(Def. 1) There exists a prime number s such that $2 \cdot s + 1 = p$.

Let us note that there exists a prime number which is safe.

The following propositions are true:

(2) For every safe prime number p holds $p \geq 5$.

(3) For every safe prime number p holds $p \bmod 2 = 1$.

(4) For every safe prime number p such that $p \neq 7$ holds $p \bmod 3 = 2$.

(5) For every safe prime number p such that $p \neq 5$ holds $p \bmod 4 = 3$.

(6) For every safe prime number p such that $p \neq 7$ holds $p \bmod 6 = 5$.

(7) For every safe prime number p such that $p > 7$ holds $p \bmod 12 = 11$.

(8) For every safe prime number p such that $p > 5$ holds $p \bmod 8 = 3$ or $p \bmod 8 = 7$.

Let p be a natural number. We say that p is Sophie Germain if and only if:

(Def. 2) $2 \cdot p + 1$ is a prime number.

Let us mention that there exists a prime number which is Sophie Germain.

The following propositions are true:

(9) For every Sophie Germain prime number p such that $p > 2$ holds $p \bmod 4 = 1$ or $p \bmod 4 = 3$.

(10) For every safe prime number p there exists a Sophie Germain prime number q such that $p = 2 \cdot q + 1$.

(11) For every safe prime number p there exists a Sophie Germain prime number q such that $\mathrm{Euler}\, p = 2 \cdot q$.

(12) Let p_1, p_2 be safe prime numbers and N be a natural number. Suppose $p_1 \neq p_2$ and $N = p_1 \cdot p_2$. Then there exist Sophie Germain prime numbers q_1, q_2 such that $\mathrm{Euler}\, N = 4 \cdot q_1 \cdot q_2$.

(13) For every safe prime number p there exists a Sophie Germain prime number q such that $\mathrm{Card}\, \mathbb{Z}/p\mathbb{Z}^* = 2 \cdot q$.

(14) Let G be a cyclic finite group and n, m be natural numbers. Suppose $\mathrm{Card}\, G = n \cdot m$. Then there exists an element a of G such that $\mathrm{ord}(a) = n$ and $\mathrm{gr}(\{a\})$ is a strict subgroup of G.

(15) Let p be a safe prime number. Then there exists a Sophie Germain prime number q and there exist strict subgroups H_1, H_2, H_3, H_4 of $\mathbb{Z}/p\mathbb{Z}^*$ such that $\mathrm{Card}\, H_1 = 1$ and $\mathrm{Card}\, H_2 = 2$ and $\mathrm{Card}\, H_3 = q$ and $\mathrm{Card}\, H_4 = 2 \cdot q$

and for every strict subgroup H of $\mathbb{Z}/p\mathbb{Z}^*$ holds $H = H_1$ or $H = H_2$ or $H = H_3$ or $H = H_4$.

Let n be a natural number. The functor M_n yields a natural number and is defined as follows:

(Def. 3) $M_n = 2^n - 1$.

Next we state a number of propositions:

(16) $M_0 = 0$.

(17) $M_1 = 1$.

(18) $M_2 = 3$.

(19) $M_3 = 7$.

(20) $M_5 = 31$.

(21) $M_7 = 127$.

(22) $M_{11} = 23 \cdot 89$.

(23) For every prime number p such that $p \neq 2$ holds $M_p \bmod 2 \cdot p = 1$.

(24) For every prime number p such that $p \neq 2$ holds $M_p \bmod 8 = 7$.

(25) For every Sophie Germain prime number p such that $p > 2$ and $p \bmod 4 = 3$ there exists a safe prime number q such that $q \mid M_p$.

(26) Let p be a Sophie Germain prime number. If $p > 2$ and p mod $4 = 1$, then there exists a safe prime number q such that $M_p \bmod q = q - 2$.

(27) For all natural numbers a, n such that $a > 1$ holds $a - 1 \mid a^n - 1$.

(28) For all natural numbers a, p such that $p > 1$ and $a^p - 1$ is a prime number holds $a = 2$ and p is a prime number.

(29) For every natural number p such that $p > 1$ and M_p is a prime number holds p is a prime number.

(30) For every integer a and for all natural numbers x, n holds a^x mod $n = (a \text{ mod } n)^x$ mod n.

(31) For all integers x, y, n such that x and n are relative prime and $x \equiv y \pmod{n}$ holds y and n are relative prime.

(32) Let a, x be natural numbers and p be a prime number. Suppose a and p are relative prime and $a \equiv x \cdot x \pmod{p}$. Then x and p are relative prime.

(33) Let a, x be integers and p be a prime number. Suppose a and p are relative prime and $a \equiv x \cdot x \pmod{p}$. Then x and p are relative prime.

(34) For all integers a, b and for all natural numbers n, x such that $a \equiv b \pmod{n}$ and $n \neq 0$ holds $a^x \equiv b^x \pmod{n}$.

(35) For every integer a and for every prime number n such that $a \cdot a \bmod n = 1$ holds $a \equiv 1 \pmod{n}$ or $a \equiv -1 \pmod{n}$.

2. Multiplicative Group of a Field

The following proposition is true

(36) For every prime number p holds $\mathbb{Z}/p\mathbb{Z}^* = \mathrm{MultGroup}(\mathbb{Z}_p^{\mathrm{R}})$.

Let F be a commutative skew field. One can verify that MultGroup(F) is commutative.

The following two propositions are true:

(37) Let F be a commutative skew field, x be an element of MultGroup(F), and x_1 be an element of F. If $x = x_1$, then $x^{-1} = {x_1}^{-1}$.

(38) For every commutative skew field F holds every finite subgroup of MultGroup(F) is a cyclic group.

References

[1] Broderick Arneson and Piotr Rudnicki. Primitive roots of unity and cyclotomic polynomials. *Formalized Mathematics*, 12(**1**):59–67, 2004.

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

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

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

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

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

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

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

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

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

[11] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6(**4**):549–551, 1997.

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

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

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

[15] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.

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

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

[18] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.

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

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

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

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

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

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

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

Received April 7, 2009

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 157–162, 2009

Hopf Extension Theorem of Measure

Noboru Endou
Gifu National College of Technology
Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. The authors have presented some articles about Lebesgue type integration theory. In our previous articles [12, 13, 26], we assumed that some σ-additive measure existed and that a function was measurable on that measure. However the existence of such a measure is not trivial. In general, because the construction of a finite additive measure is comparatively easy, to induce a σ-additive measure a finite additive measure is used. This is known as an E. Hopf's extension theorem of measure [15].

MML identifier: MEASURE8, version: 7.11.02 4.125.1059

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

1. The Outer Measure Induced by the Finite Additive Measure

For simplicity, we follow the rules: X denotes a set, F denotes a field of subsets of X, M denotes a measure on F, A, B denote subsets of X, S_1 denotes a sequence of subsets of X, s_1, s_2, s_3 denote sequences of extended reals, and n, k denote natural numbers.

We now state three propositions:

(1) $\operatorname{Ser} s_1 = (\sum_{\alpha=0}^{\kappa}(s_1)(\alpha))_{\kappa\in\mathbb{N}}$.

(2)[1] If s_1 is non-negative, then s_1 is summable and $\overline{\sum} s_1 = \sum s_1$.

[1] The translation of Mizar functor SUM introduced in [4] was changed from $\sum$ to $\overline{\sum}$.

ISSN 1426–2630(p), 1898-9934(e)

(3) Suppose s_2 is non-negative and s_3 is non-negative and for every natural number n holds $s_1(n) = s_2(n)+s_3(n)$. Then s_1 is non-negative and $\overline{\sum} s_1 = \overline{\sum} s_2 + \overline{\sum} s_3$ and $\sum s_1 = \sum s_2 + \sum s_3$.

Let us consider X, F. One can check that there exists a function from $\mathbb{N}$ into F which is disjoint valued.

Let us consider X, F. A finite sequence of elements of 2^X is said to be a finite sequence of elements of F if:

(Def. 1) For every natural number k such that $k \in \operatorname{dom} \mathrm{it}$ holds $\mathrm{it}(k) \in F$.

Let us consider X, F. Observe that there exists a finite sequence of elements of F which is disjoint valued.

Let us consider X, F. A disjoint valued finite set sequence of F is a disjoint valued finite sequence of elements of F.

Let us consider X, F. A sequence of separated subsets of F is a disjoint valued function from $\mathbb{N}$ into F.

Let us consider X, F. A sequence of subsets of X is said to be a set sequence of F if:

(Def. 2) For every natural number n holds $\mathrm{it}(n) \in F$.

Let us consider X, A, F. A set sequence of F is said to be a covering of A in F if:

(Def. 3) $A \subseteq \bigcup \operatorname{rng} \mathrm{it}$.

In the sequel F_1 denotes a set sequence of F and C_1 denotes a covering of A in F.

Let us consider X, F, F_1, n. Then $F_1(n)$ is an element of F.

Let us consider X, F, S_1. A function from $\mathbb{N}$ into $(2^X)^{\mathbb{N}}$ is said to be a covering of S_1 in F if:

(Def. 4) For every element n of $\mathbb{N}$ holds $\mathrm{it}(n)$ is a covering of $S_1(n)$ in F.

In the sequel C_2 is a covering of S_1 in F.

Let us consider X, F, M, F_1. The functor $\mathrm{vol}(M, F_1)$ yielding a sequence of extended reals is defined as follows:

(Def. 5) For every n holds $(\mathrm{vol}(M, F_1))(n) = M(F_1(n))$.

One can prove the following proposition

(4) $\mathrm{vol}(M, F_1)$ is non-negative.

Let us consider X, F, S_1, C_2 and let n be an element of $\mathbb{N}$. Then $C_2(n)$ is a covering of $S_1(n)$ in F.

Let us consider X, F, S_1, M, C_2. The functor $\mathrm{Volume}(M, C_2)$ yielding a sequence of extended reals is defined as follows:

(Def. 6) For every element n of $\mathbb{N}$ holds $(\mathrm{Volume}(M, C_2))(n) = \overline{\sum} \mathrm{vol}(M, C_2(n))$.

The following proposition is true

(5) $0 \leq (\mathrm{Volume}(M, C_2))(n)$.

Let us consider X, F, M, A. The functor $\mathrm{Svc}(M,A)$ yielding a subset of $\overline{\mathbb{R}}$ is defined as follows:

(Def. 7) For every extended real number x holds $x \in \mathrm{Svc}(M,A)$ iff there exists a covering C_1 of A in F such that $x = \overline{\sum}\mathrm{vol}(M, C_1)$.

Let us consider X, A, F, M. Observe that $\mathrm{Svc}(M,A)$ is non empty.

Let us consider X, F, M. The Caratheodory measure determined by M is a function from 2^X into $\overline{\mathbb{R}}$ and is defined by:

(Def. 8) For every subset A of X holds (the Caratheodory measure determined by $M)(A) = \inf \mathrm{Svc}(M,A)$.

The function InvPairFunc from $\mathbb{N}$ into $\mathbb{N} \times \mathbb{N}$ is defined by:

(Def. 9) $\mathrm{InvPairFunc} = \mathrm{PairFunc}^{-1}$.

Let us consider X, F, S_1, C_2. The functor $\mathrm{On}\, C_2$ yielding a covering of $\bigcup \mathrm{rng}\, S_1$ in F is defined by:

(Def. 10) For every natural number n holds $(\mathrm{On}\, C_2)(n) = C_2(\mathrm{pr1}(\mathrm{InvPairFunc})(n))(\mathrm{pr2}(\mathrm{InvPairFunc})(n))$.

The following propositions are true:

(6) Let k be an element of $\mathbb{N}$. Then there exists a natural number m such that for every sequence S_1 of subsets of X and for every covering C_2 of S_1 in F holds $(\sum_{\alpha=0}^{\kappa}(\mathrm{vol}(M, \mathrm{On}\, C_2))(\alpha))_{\kappa\in\mathbb{N}}(k) \leq (\sum_{\alpha=0}^{\kappa}(\mathrm{Volume}(M, C_2))(\alpha))_{\kappa\in\mathbb{N}}(m)$.

(7) $\inf \mathrm{Svc}(M, \bigcup \mathrm{rng}\, S_1) \leq \overline{\sum}\mathrm{Volume}(M, C_2)$.

(8) If $A \in F$, then $A, \emptyset_X$ followed by $\emptyset_X$ is a covering of A in F.

(9) Let X be a set, F be a field of subsets of X, M be a measure on F, and A be a set. If $A \in F$, then (the Caratheodory measure determined by $M)(A) \leq M(A)$.

(10) The Caratheodory measure determined by M is non-negative.

(11) (The Caratheodory measure determined by $M)(\emptyset) = 0$.

(12) If $A \subseteq B$, then (the Caratheodory measure determined by $M)(A) \leq$ (the Caratheodory measure determined by $M)(B)$.

(13) (The Caratheodory measure determined by $M)(\bigcup \mathrm{rng}\, S_1) \leq \overline{\sum}($(the Caratheodory measure determined by $M) \cdot S_1)$.

(14) The Caratheodory measure determined by M is a Caratheodor's measure on X.

Let X be a set, let F be a field of subsets of X, and let M be a measure on F. Then the Caratheodory measure determined by M is a Caratheodor's measure on X.

2. Hopf Extension Theorem

Let X be a set, let F be a field of subsets of X, and let M be a measure on F. We say that M is completely-additive if and only if:

(Def. 11) For every sequence F_1 of separated subsets of F such that $\bigcup \operatorname{rng} F_1 \in F$ holds $\overline{\sum}(M \cdot F_1) = M(\bigcup \operatorname{rng} F_1)$.

The following propositions are true:

(15) The partial unions of F_1 are a set sequence of F.

(16) The partial diff-unions of F_1 are a set sequence of F.

(17) Suppose $A \in F$. Then there exists a sequence F_1 of separated subsets of F such that $A = \bigcup \operatorname{rng} F_1$ and for every natural number n holds $F_1(n) \subseteq C_1(n)$.

(18) Suppose M is completely-additive. Let A be a set. If $A \in F$, then $M(A) =$ (the Caratheodory measure determined by $M)(A)$.

In the sequel C is a Caratheodor's measure on X.

The following propositions are true:

(19) If for every subset B of X holds $C(B \cap A) + C(B \cap (X \setminus A)) \leq C(B)$, then $A \in \sigma$-Field(C).

(20) $F \subseteq \sigma$-Field(the Caratheodory measure determined by M).

(21) Let X be a set, F be a field of subsets of X, F_1 be a set sequence of F, and M be a function from F into $\overline{\mathbb{R}}$. Then $M \cdot F_1$ is a sequence of extended reals.

Let X be a set, let F be a field of subsets of X, let F_1 be a set sequence of F, and let g be a function from F into $\overline{\mathbb{R}}$. Then $g \cdot F_1$ is a sequence of extended reals.

We now state the proposition

(22) Let X be a set, S be a σ-field of subsets of X, S_2 be a sequence of subsets of S, and M be a function from S into $\overline{\mathbb{R}}$. Then $M \cdot S_2$ is a sequence of extended reals.

Let X be a set, let S be a σ-field of subsets of X, let S_2 be a sequence of subsets of S, and let g be a function from S into $\overline{\mathbb{R}}$. Then $g \cdot S_2$ is a sequence of extended reals.

We now state several propositions:

(23) Let F, G be functions from $\mathbb{N}$ into $\overline{\mathbb{R}}$ and n be a natural number. Suppose that for every natural number m such that $m \leq n$ holds $F(m) \leq G(m)$. Then $(\operatorname{Ser} F)(n) \leq (\operatorname{Ser} G)(n)$.

(24) For all X, C and for every sequence s_1 of separated subsets of σ-Field(C) holds $\bigcup \operatorname{rng} s_1 \in \sigma$-Field$(C)$ and $C(\bigcup \operatorname{rng} s_1) = \sum(C \cdot s_1)$.

(25) For all X, C and for every sequence s_1 of subsets of σ-Field(C) holds $\bigcup s_1 \in \sigma$-Field(C).

(26) Let X be a non empty set, S be a σ-field of subsets of X, M be a σ-measure on S, and S_2 be a sequence of subsets of S. If S_2 is non-decreasing, then $\lim(M \cdot S_2) = M(\lim S_2)$.

(27) If F_1 is non-decreasing, then $M \cdot F_1$ is non-decreasing.

(28) If F_1 is descending, then $M \cdot F_1$ is non-increasing.

(29) Let X be a set, S be a σ-field of subsets of X, M be a σ-measure on S, and S_2 be a sequence of subsets of S. If S_2 is non-decreasing, then $M \cdot S_2$ is non-decreasing.

(30) Let X be a set, S be a σ-field of subsets of X, M be a σ-measure on S, and S_2 be a sequence of subsets of S. If S_2 is descending, then $M \cdot S_2$ is non-increasing.

(31) Let X be a non empty set, S be a σ-field of subsets of X, M be a σ-measure on S, and S_2 be a sequence of subsets of S. If S_2 is descending and $M(S_2(0)) < +\infty$, then $\lim(M \cdot S_2) = M(\lim S_2)$.

Let X be a set, let F be a field of subsets of X, let S be a σ-field of subsets of X, let m be a measure on F, and let M be a σ-measure on S. We say that M is an extension of m if and only if:

(Def. 12) For every set A such that $A \in F$ holds $M(A) = m(A)$.

We now state four propositions:

(32) Let X be a non empty set, F be a field of subsets of X, and m be a measure on F. If there exists a σ-measure on $\sigma(F)$ which is an extension of m, then m is completely-additive.

(33) Let X be a non empty set, F be a field of subsets of X, and m be a measure on F. Suppose m is completely-additive. Then there exists a σ-measure M on $\sigma(F)$ such that M is an extension of m and $M = \sigma$-Meas(the Caratheodory measure determined by $m) \restriction \sigma(F)$.

(34) If for every n holds $M(F_1(n)) < +\infty$, then $M(($the partial unions of $F_1)(k)) < +\infty$.

(35) Let X be a non empty set, F be a field of subsets of X, and m be a measure on F. Suppose that

(i) m is completely-additive, and

(ii) there exists a set sequence A_1 of F such that for every natural number n holds $m(A_1(n)) < +\infty$ and $X = \bigcup \operatorname{rng} A_1$.

Let M be a σ-measure on $\sigma(F)$. Suppose M is an extension of m. Then $M = \sigma$-Meas(the Caratheodory measure determined by $m) \restriction \sigma(F)$.

References

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

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

[3] Józef Białas. Infimum and supremum of the set of real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):163–171, 1991.

[4] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.

[5] Józef Białas. Several properties of the σ-additive measure. *Formalized Mathematics*, 2(**4**):493–497, 1991.

[6] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.

[7] Józef Białas. Properties of Caratheodor's measure. *Formalized Mathematics*, 3(**1**):67–70, 1992.

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

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

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

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

[12] 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.

[13] Noboru Endou and Yasunari Shidama. Integral of measurable function. *Formalized Mathematics*, 14(**2**):53–70, 2006, doi:10.2478/v10037-006-0008-x.

[14] Adam Grabowski. On the Kuratowski limit operators. *Formalized Mathematics*, 11(**4**):399–409, 2003.

[15] P. R. Halmos. *Measure Theory.* Springer-Verlag, 1987.

[16] Krzysztof Hryniewiecki. Recursive definitions. *Formalized Mathematics*, 1(**2**):321–328, 1990.

[17] Franz Merkl. Dynkin's lemma in measure theory. *Formalized Mathematics*, 9(**3**):591–595, 2001.

[18] Andrzej Nędzusiak. Probability. *Formalized Mathematics*, 1(**4**):745–749, 1990.

[19] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.

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

[21] Karol Pąk. The Nagata-Smirnov theorem. Part II. *Formalized Mathematics*, 12(**3**):385–389, 2004.

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

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

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

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

[26] Hiroshi Yamazaki, Noboru Endou, Yasunari Shidama, and Hiroyuki Okazaki. Inferior limit, superior limit and convergence of sequences of extended real numbers. *Formalized Mathematics*, 15(**4**):231–236, 2007, doi:10.2478/v10037-007-0026-3.

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

Received April 7, 2009

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 163–171, 2009

Labelled State Transition Systems

Michał Trybulec
YAC Software
Warsaw, Poland

Summary. This article introduces labelled state transition systems, where transitions may be labelled by words from a given alphabet. Reduction relations from [4] are used to define transitions between states, acceptance of words, and reachable states. Deterministic transition systems are also defined.

MML identifier: `REWRITE3`, version: `7.11.02 4.125.1059`

The notation and terminology used here are introduced in the following papers: [1], [8], [2], [11], [6], [17], [7], [9], [16], [15], [14], [4], [10], [13], [3], [12], and [5].

1. Preliminaries

For simplicity, we use the following convention: x, x_1, x_2, y, y_1, y_2, z, z_1, z_2, X, X_1, X_2 are sets, E is a non empty set, e is an element of E, u, v, v_1, v_2, w, w_1, w_2 are elements of E^ω, F, F_1, F_2 are subsets of E^ω, and k, l are natural numbers.

Next we state a number of propositions:

(1) For every finite sequence p such that $k \in \operatorname{dom} p$ holds $(\langle x \rangle \frown p)(k+1) = p(k)$.

(2) For every finite sequence p such that $p \neq \emptyset$ there exists a finite sequence q and there exists x such that $p = q \frown \langle x \rangle$ and $\operatorname{len} p = \operatorname{len} q + 1$.

(3) For every finite sequence p such that $k \in \operatorname{dom} p$ and $k + 1 \notin \operatorname{dom} p$ holds $\operatorname{len} p = k$.

(4) Let R be a binary relation, P be a reduction sequence w.r.t. R, and q_1, q_2 be finite sequences. Suppose $P = q_1 \frown q_2$ and $\operatorname{len} q_1 > 0$ and $\operatorname{len} q_2 > 0$. Then q_1 is a reduction sequence w.r.t. R and q_2 is a reduction sequence w.r.t. R.

ISSN 1426–2630(p), 1898-9934(e)

(5) Let R be a binary relation and P be a reduction sequence w.r.t. R. Suppose $\operatorname{len} P > 1$. Then there exists a reduction sequence Q w.r.t. R such that $\langle P(1)\rangle \mathbin{^\frown} Q = P$ and $\operatorname{len} Q + 1 = \operatorname{len} P$.

(6) Let R be a binary relation and P be a reduction sequence w.r.t. R. Suppose $\operatorname{len} P > 1$. Then there exists a reduction sequence Q w.r.t. R such that $Q \mathbin{^\frown} \langle P(\operatorname{len} P)\rangle = P$ and $\operatorname{len} Q + 1 = \operatorname{len} P$.

(7) Let R be a binary relation and P be a reduction sequence w.r.t. R. Suppose $\operatorname{len} P > 1$. Then there exists a reduction sequence Q w.r.t. R such that $\operatorname{len} Q + 1 = \operatorname{len} P$ and for every k such that $k \in \operatorname{dom} Q$ holds $Q(k) = P(k+1)$.

(8) For every binary relation R such that $\langle x, y\rangle$ is a reduction sequence w.r.t. R holds $\langle x,\, y\rangle \in R$.

(9) If $w = u \mathbin{^\frown} v$, then $\operatorname{len} u \leq \operatorname{len} w$ and $\operatorname{len} v \leq \operatorname{len} w$.

(10) If $w = u \mathbin{^\frown} v$ and $u \neq \langle\rangle_E$ and $v \neq \langle\rangle_E$, then $\operatorname{len} u < \operatorname{len} w$ and $\operatorname{len} v < \operatorname{len} w$.

(11) If $w_1 \mathbin{^\frown} v_1 = w_2 \mathbin{^\frown} v_2$ and if $\operatorname{len} w_1 = \operatorname{len} w_2$ or $\operatorname{len} v_1 = \operatorname{len} v_2$, then $w_1 = w_2$ and $v_1 = v_2$.

(12) If $w_1 \mathbin{^\frown} v_1 = w_2 \mathbin{^\frown} v_2$ and if $\operatorname{len} w_1 \leq \operatorname{len} w_2$ or $\operatorname{len} v_1 \geq \operatorname{len} v_2$, then there exists u such that $w_1 \mathbin{^\frown} u = w_2$ and $v_1 = u \mathbin{^\frown} v_2$.

(13) If $w_1 \mathbin{^\frown} v_1 = w_2 \mathbin{^\frown} v_2$, then there exists u such that $w_1 \mathbin{^\frown} u = w_2$ and $v_1 = u \mathbin{^\frown} v_2$ or there exists u such that $w_2 \mathbin{^\frown} u = w_1$ and $v_2 = u \mathbin{^\frown} v_1$.

Let us consider X. We consider transition-systems over X as extensions of 1-sorted structure as systems

⟨ a carrier, a transition ⟩,

where the carrier is a set and the transition is a relation between the carrier× X and the carrier.

2. Transition Systems over Subsets of E^ω

Let us consider E, F and let $\mathfrak{T}$ be a transition-system over F. We say that $\mathfrak{T}$ is deterministic if and only if the conditions (Def. 1) are satisfied.

(Def. 1)(i) The transition of $\mathfrak{T}$ is a function,

(ii) $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$), and

(iii) for every element s of $\mathfrak{T}$ and for all u, v such that $u \neq v$ and $\langle s,\, u\rangle \in \operatorname{dom}$ (the transition of $\mathfrak{T}$) and $\langle s,\, v\rangle \in \operatorname{dom}$ (the transition of $\mathfrak{T}$) it is not true that there exists w such that $u \mathbin{^\frown} w = v$ or $v \mathbin{^\frown} w = u$.

The following proposition is true

(14) For every transition-system $\mathfrak{T}$ over F such that dom (the transition of $\mathfrak{T}$) $= \emptyset$ holds $\mathfrak{T}$ is deterministic.

Let us consider E, F. Note that there exists a transition-system over F which is strict, non empty, finite, and deterministic.

3. Productions

Let us consider X, let $\mathfrak{T}$ be a transition-system over X, and let us consider x, y, z. The predicate $x, y \rightarrow_{\mathfrak{T}} z$ is defined by:

(Def. 2) $\langle\langle x, y\rangle, z\rangle \in$ the transition of $\mathfrak{T}$.

We now state several propositions:

(15) Let $\mathfrak{T}$ be a transition-system over X. Suppose $x, y \rightarrow_{\mathfrak{T}} z$. Then
 (i) $x \in \mathfrak{T}$,
 (ii) $y \in X$,
 (iii) $z \in \mathfrak{T}$,
 (iv) $x \in \operatorname{dom}\operatorname{dom}$ (the transition of $\mathfrak{T}$),
 (v) $y \in \operatorname{rng}\operatorname{dom}$ (the transition of $\mathfrak{T}$), and
 (vi) $z \in \operatorname{rng}$ (the transition of $\mathfrak{T}$).

(16) Let $\mathfrak{T}_1$ be a transition-system over X_1 and $\mathfrak{T}_2$ be a transition-system over X_2. Suppose the transition of $\mathfrak{T}_1 =$ the transition of $\mathfrak{T}_2$. If $x, y \rightarrow_{\mathfrak{T}_1} z$, then $x, y \rightarrow_{\mathfrak{T}_2} z$.

(17) Let $\mathfrak{T}$ be a transition-system over F. Suppose the transition of $\mathfrak{T}$ is a function. If $x, y \rightarrow_{\mathfrak{T}} z_1$ and $x, y \rightarrow_{\mathfrak{T}} z_2$, then $z_1 = z_2$.

(18) For every deterministic transition-system $\mathfrak{T}$ over F such that $\langle\rangle_E \notin \operatorname{rng}\operatorname{dom}$ (the transition of $\mathfrak{T}$) holds $x, \langle\rangle_E \not\rightarrow_{\mathfrak{T}} y$.

(19) Let $\mathfrak{T}$ be a deterministic transition-system over F. If $u \neq v$ and $x, u \rightarrow_{\mathfrak{T}} z_1$ and $x, v \rightarrow_{\mathfrak{T}} z_2$, then it is not true that there exists w such that $u ^\frown w = v$ or $v ^\frown w = u$.

4. Direct Transitions

Let us consider E, F, let $\mathfrak{T}$ be a transition-system over F, and let us consider x_1, x_2, y_1, y_2. The predicate $x_1, x_2 \Rightarrow_{\mathfrak{T}} y_1, y_2$ is defined by:

(Def. 3) There exist v, w such that $v = y_2$ and $x_1, w \rightarrow_{\mathfrak{T}} y_1$ and $x_2 = w ^\frown v$.

One can prove the following propositions:

(20) Let $\mathfrak{T}$ be a transition-system over F. Suppose $x_1, x_2 \Rightarrow_{\mathfrak{T}} y_1, y_2$. Then x_1, $y_1 \in \mathfrak{T}$ and x_2, $y_2 \in E^\omega$ and $x_1 \in \operatorname{dom}\operatorname{dom}$ (the transition of $\mathfrak{T}$) and $y_1 \in \operatorname{rng}$ (the transition of $\mathfrak{T}$).

(21) Let $\mathfrak{T}_1$ be a transition-system over F_1 and $\mathfrak{T}_2$ be a transition-system over F_2. Suppose the transition of $\mathfrak{T}_1 =$ the transition of $\mathfrak{T}_2$ and $x_1, x_2 \Rightarrow_{\mathfrak{T}_1} y_1, y_2$. Then $x_1, x_2 \Rightarrow_{\mathfrak{T}_2} y_1, y_2$.

(22) For every transition-system $\mathfrak{T}$ over F such that $x, u \Rightarrow_{\mathfrak{T}} y, v$ there exists w such that $x, w \rightarrow_{\mathfrak{T}} y$ and $u = w \frown v$.

(23) For every transition-system $\mathfrak{T}$ over F holds $x, y \rightarrow_{\mathfrak{T}} z$ iff $x, y \Rightarrow_{\mathfrak{T}} z, \langle\rangle_E$.

(24) For every transition-system $\mathfrak{T}$ over F holds $x, v \rightarrow_{\mathfrak{T}} y$ iff $x, v \frown w \Rightarrow_{\mathfrak{T}} y, w$.

(25) For every transition-system $\mathfrak{T}$ over F such that $x, u \Rightarrow_{\mathfrak{T}} y, v$ holds $x, u \frown w \Rightarrow_{\mathfrak{T}} y, v \frown w$.

(26) For every transition-system $\mathfrak{T}$ over F such that $x, u \Rightarrow_{\mathfrak{T}} y, v$ holds $\operatorname{len} u \geq \operatorname{len} v$.

(27) Let $\mathfrak{T}$ be a transition-system over F. Suppose the transition of $\mathfrak{T}$ is a function. If $x_1, x_2 \Rightarrow_{\mathfrak{T}} y_1, z$ and $x_1, x_2 \Rightarrow_{\mathfrak{T}} y_2, z$, then $y_1 = y_2$.

(28) For every transition-system $\mathfrak{T}$ over F such that $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$) holds $x, z \not\Rightarrow_{\mathfrak{T}} y, z$.

(29) For every transition-system $\mathfrak{T}$ over F such that $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$) holds if $x, u \Rightarrow_{\mathfrak{T}} y, v$, then $\operatorname{len} u > \operatorname{len} v$.

(30) For every deterministic transition-system $\mathfrak{T}$ over F such that $x_1, x_2 \Rightarrow_{\mathfrak{T}} y_1, z_1$ and $x_1, x_2 \Rightarrow_{\mathfrak{T}} y_2, z_2$ holds $y_1 = y_2$ and $z_1 = z_2$.

5. Reduction Relation

In the sequel $\mathfrak{T}$ is a non empty transition-system over F, s, t are elements of $\mathfrak{T}$, and S is a subset of $\mathfrak{T}$.

Let us consider E, F, $\mathfrak{T}$. The functor $\Rightarrow_{\mathfrak{T}}$ yields a binary relation on (the carrier of $\mathfrak{T}$) $\times E^{\omega}$ and is defined by:

(Def. 4) $\langle\langle x_1, x_2\rangle, \langle y_1, y_2\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$ iff $x_1, x_2 \Rightarrow_{\mathfrak{T}} y_1, y_2$.

One can prove the following propositions:

(31) If $\langle x, y\rangle \in \Rightarrow_{\mathfrak{T}}$, then there exist s, v, t, w such that $x = \langle s, v\rangle$ and $y = \langle t, w\rangle$.

(32) Suppose $\langle\langle x_1, x_2\rangle, \langle y_1, y_2\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$. Then $x_1, y_1 \in \mathfrak{T}$ and $x_2, y_2 \in E^{\omega}$ and $x_1 \in \operatorname{dom} \operatorname{dom}$ (the transition of $\mathfrak{T}$) and $y_1 \in \operatorname{rng}$ (the transition of $\mathfrak{T}$).

(33) If $x \in \Rightarrow_{\mathfrak{T}}$, then there exist s, t, v, w such that $x = \langle\langle s, v\rangle, \langle t, w\rangle\rangle$.

(34) Let $\mathfrak{T}_1$ be a non empty transition-system over F_1 and $\mathfrak{T}_2$ be a non empty transition-system over F_2. Suppose the carrier of $\mathfrak{T}_1$ = the carrier of $\mathfrak{T}_2$ and the transition of $\mathfrak{T}_1$ = the transition of $\mathfrak{T}_2$. Then $\Rightarrow_{\mathfrak{T}_1} = \Rightarrow_{\mathfrak{T}_2}$.

(35) If $\langle\langle x_1, x_2\rangle, \langle y_1, y_2\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$, then there exist v, w such that $v = y_2$ and $x_1, w \rightarrow_{\mathfrak{T}} y_1$ and $x_2 = w \frown v$.

(36) If $\langle\langle x, u\rangle, \langle y, v\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$, then there exists w such that $x, w \rightarrow_{\mathfrak{T}} y$ and $u = w \frown v$.

(37) $x, y \rightarrow_{\mathfrak{T}} z$ iff $\langle\langle x, y\rangle, \langle z, \langle\rangle_E\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$.

(38) $x, v \rightarrow_{\mathfrak{T}} y$ iff $\langle\langle x, v \frown w\rangle, \langle y, w\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$.

(39) If $\langle\langle x, u\rangle, \langle y, v\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$, then $\langle\langle x, u \frown w\rangle, \langle y, v \frown w\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$.

(40) If $\langle\langle x, u\rangle, \langle y, v\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$, then $\operatorname{len} u \geq \operatorname{len} v$.

(41) If the transition of $\mathfrak{T}$ is a function, then if $\langle x, \langle y_1, z\rangle\rangle, \langle x, \langle y_2, z\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$, then $y_1 = y_2$.

(42) If $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$), then if $\langle\langle x, u\rangle, \langle y, v\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$, then $\operatorname{len} u > \operatorname{len} v$.

(43) If $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$), then $\langle\langle x, z\rangle, \langle y, z\rangle\rangle \notin \Rightarrow_{\mathfrak{T}}$.

(44) If $\mathfrak{T}$ is deterministic, then if $\langle x, y_1\rangle, \langle x, y_2\rangle \in \Rightarrow_{\mathfrak{T}}$, then $y_1 = y_2$.

(45) If $\mathfrak{T}$ is deterministic, then if $\langle x, \langle y_1, z_1\rangle\rangle, \langle x, \langle y_2, z_2\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$, then $y_1 = y_2$ and $z_1 = z_2$.

(46) If $\mathfrak{T}$ is deterministic, then $\Rightarrow_{\mathfrak{T}}$ is function-like.

6. Reduction Sequences

Let us consider x, E. The functor $\dim_2(x, E)$ yields an element of E^ω and is defined as follows:

(Def. 5) $\dim_2(x, E) = \begin{cases} x_{\mathbf{2}}, & \text{if there exist } y, u \text{ such that } x = \langle y, u\rangle, \\ \emptyset, & \text{otherwise.} \end{cases}$

Next we state a number of propositions:

(47) Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$ and given k. If $k, k+1 \in \operatorname{dom} P$, then there exist s, v, t, w such that $P(k) = \langle s, v\rangle$ and $P(k+1) = \langle t, w\rangle$.

(48) Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$ and given k. If $k, k+1 \in \operatorname{dom} P$, then $P(k) = \langle P(k)_{\mathbf{1}}, P(k)_{\mathbf{2}}\rangle$ and $P(k+1) = \langle P(k+1)_{\mathbf{1}}, P(k+1)_{\mathbf{2}}\rangle$.

(49) Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$ and given k. Suppose $k, k+1 \in \operatorname{dom} P$. Then

(i) $P(k)_{\mathbf{1}} \in \mathfrak{T}$,

(ii) $P(k)_{\mathbf{2}} \in E^\omega$,

(iii) $P(k+1)_{\mathbf{1}} \in \mathfrak{T}$,

(iv) $P(k+1)_{\mathbf{2}} \in E^\omega$,

(v) $P(k)_{\mathbf{1}} \in \operatorname{dom} \operatorname{dom}$ (the transition of $\mathfrak{T}$), and

(vi) $P(k+1)_{\mathbf{1}} \in \operatorname{rng}$ (the transition of $\mathfrak{T}$).

(50) Let $\mathfrak{T}_1$ be a non empty transition-system over F_1 and $\mathfrak{T}_2$ be a non empty transition-system over F_2. Suppose the carrier of $\mathfrak{T}_1$ = the carrier of $\mathfrak{T}_2$ and the transition of $\mathfrak{T}_1$ = the transition of $\mathfrak{T}_2$. Then every reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}_1}$ is a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}_2}$.

(51) Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$. If there exist x, u such that $P(1) = \langle x, u\rangle$, then for every k such that $k \in \operatorname{dom} P$ holds $\dim_2(P(k), E) = P(k)_{\mathbf{2}}$.

(52) Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$. If $P(\operatorname{len} P) = \langle y, w\rangle$, then for every k such that $k \in \operatorname{dom} P$ there exists u such that $P(k)_{\mathbf{2}} = u \frown w$.

(53) For every reduction sequence P w.r.t. $\Rightarrow_{\mathfrak{T}}$ such that $P(1) = \langle x, v\rangle$ and $P(\operatorname{len} P) = \langle y, w\rangle$ there exists u such that $v = u \frown w$.

(54) Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$. If $P(1) = \langle x, u\rangle$ and $P(\operatorname{len} P) = \langle y, u\rangle$, then for every k such that $k \in \operatorname{dom} P$ holds $P(k)_{\mathbf{2}} = u$.

(55) Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$ and given k. Suppose k, $k+1 \in \operatorname{dom} P$. Then there exist v, w such that $v = P(k+1)_{\mathbf{2}}$ and $P(k)_{\mathbf{1}}, w \rightarrow_{\mathfrak{T}} P(k+1)_{\mathbf{1}}$ and $P(k)_{\mathbf{2}} = w \frown v$.

(56) Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$ and given k. Suppose k, $k+1 \in \operatorname{dom} P$ and $P(k) = \langle x, u\rangle$ and $P(k+1) = \langle y, v\rangle$. Then there exists w such that $x, w \rightarrow_{\mathfrak{T}} y$ and $u = w \frown v$.

(57) $x, y \rightarrow_{\mathfrak{T}} z$ iff $\langle\langle x, y\rangle, \langle z, \langle\rangle_E\rangle\rangle$ is a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$.

(58) $x, v \rightarrow_{\mathfrak{T}} y$ iff $\langle\langle x, v \frown w\rangle, \langle y, w\rangle\rangle$ is a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$.

(59) For every reduction sequence P w.r.t. $\Rightarrow_{\mathfrak{T}}$ such that $P(1) = \langle x, v\rangle$ and $P(\operatorname{len} P) = \langle y, w\rangle$ holds $\operatorname{len} v \geq \operatorname{len} w$.

(60) Suppose $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$). Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$. If $P(1) = \langle x, u\rangle$ and $P(\operatorname{len} P) = \langle y, u\rangle$, then $\operatorname{len} P = 1$ and $x = y$.

(61) Suppose $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$). Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$. If $P(1)_{\mathbf{2}} = P(\operatorname{len} P)_{\mathbf{2}}$, then $\operatorname{len} P = 1$.

(62) Suppose $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$). Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$. If $P(1) = \langle x, u\rangle$ and $P(\operatorname{len} P) = \langle y, \langle\rangle_E\rangle$, then $\operatorname{len} P \leq \operatorname{len} u + 1$.

(63) Suppose $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$). Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$. If $P(1) = \langle x, \langle e\rangle\rangle$ and $P(\operatorname{len} P) = \langle y, \langle\rangle_E\rangle$, then $\operatorname{len} P = 2$.

(64) Suppose $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$). Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$. If $P(1) = \langle x, v\rangle$ and $P(\operatorname{len} P) = \langle y, w\rangle$, then $\operatorname{len} v > \operatorname{len} w$ or $\operatorname{len} P = 1$ and $x = y$ and $v = w$.

(65) Suppose $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$). Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$ and given k. If k, $k+1 \in \operatorname{dom} P$, then $P(k)_{\mathbf{2}} \neq P(k+1)_{\mathbf{2}}$.

(66) Suppose $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$). Let P be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$ and given k, l. If k, $l \in \operatorname{dom} P$ and $k < l$, then $P(k)_{\mathbf{2}} \neq P(l)_{\mathbf{2}}$.

(67) Suppose $\mathfrak{T}$ is deterministic. Let P, Q be reduction sequences w.r.t. $\Rightarrow_{\mathfrak{T}}$. If $P(1) = Q(1)$, then for every k such that $k \in \operatorname{dom} P$ and $k \in \operatorname{dom} Q$ holds $P(k) = Q(k)$.

(68) If $\mathfrak{T}$ is deterministic, then for all reduction sequences P, Q w.r.t. $\Rightarrow_{\mathfrak{T}}$ such that $P(1) = Q(1)$ and $\operatorname{len} P = \operatorname{len} Q$ holds $P = Q$.

(69) Suppose $\mathfrak{T}$ is deterministic. Let P, Q be reduction sequences w.r.t. $\Rightarrow_{\mathfrak{T}}$. If $P(1) = Q(1)$ and $P(\operatorname{len} P)_{\mathbf{2}} = Q(\operatorname{len} Q)_{\mathbf{2}}$, then $P = Q$.

7. Reductions

The following propositions are true:

(70) If $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x, v\rangle$ to $\langle y, w\rangle$, then there exists u such that $v = u \frown w$.

(71) If $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x, u\rangle$ to $\langle y, v\rangle$, then $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x, u \frown w\rangle$ to $\langle y, v \frown w\rangle$.

(72) If $x, y \rightarrow_{\mathfrak{T}} z$, then $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x, y\rangle$ to $\langle z, \langle\rangle_E\rangle$.

(73) If $x, v \rightarrow_{\mathfrak{T}} y$, then $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x, v \frown w\rangle$ to $\langle y, w\rangle$.

(74) If $x_1, x_2 \Rightarrow_{\mathfrak{T}} y_1, y_2$, then $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x_1, x_2\rangle$ to $\langle y_1, y_2\rangle$.

(75) If $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x, v\rangle$ to $\langle y, w\rangle$, then $\operatorname{len} v \geq \operatorname{len} w$.

(76) If $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x, w\rangle$ to $\langle y, v \frown w\rangle$, then $v = \langle\rangle_E$.

(77) If $\langle\rangle_E \notin$ rng dom (the transition of $\mathfrak{T}$), then if $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x, v\rangle$ to $\langle y, w\rangle$, then $\operatorname{len} v > \operatorname{len} w$ or $x = y$ and $v = w$.

(78) If $\langle\rangle_E \notin$ rng dom (the transition of $\mathfrak{T}$), then if $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x, u\rangle$ to $\langle y, u\rangle$, then $x = y$.

(79) If $\langle\rangle_E \notin$ rng dom (the transition of $\mathfrak{T}$), then if $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x, \langle e\rangle\rangle$ to $\langle y, \langle\rangle_E\rangle$, then $\langle\langle x, \langle e\rangle\rangle, \langle y, \langle\rangle_E\rangle\rangle \in \Rightarrow_{\mathfrak{T}}$.

(80) If $\mathfrak{T}$ is deterministic, then if $\Rightarrow_{\mathfrak{T}}$ reduces x to $\langle y_1, z\rangle$ and $\Rightarrow_{\mathfrak{T}}$ reduces x to $\langle y_2, z\rangle$, then $y_1 = y_2$.

8. Transitions

Let us consider E, F, $\mathfrak{T}$, x_1, x_2, y_1, y_2. The predicate $x_1, x_2 \Rightarrow^*_{\mathfrak{T}} y_1, y_2$ is defined by:

(Def. 6) $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x_1, x_2\rangle$ to $\langle y_1, y_2\rangle$.

Next we state a number of propositions:

(81) Let $\mathfrak{T}_1$ be a non empty transition-system over F_1 and $\mathfrak{T}_2$ be a non empty transition-system over F_2. Suppose the carrier of $\mathfrak{T}_1$ = the carrier of $\mathfrak{T}_2$ and the transition of $\mathfrak{T}_1$ = the transition of $\mathfrak{T}_2$. If $x_1, x_2 \Rightarrow^*_{\mathfrak{T}_1} y_1, y_2$, then $x_1, x_2 \Rightarrow^*_{\mathfrak{T}_2} y_1, y_2$.

(82) $x, y \Rightarrow^*_{\mathfrak{T}} x, y$.

(83) If $x_1, x_2 \Rightarrow^*_{\mathfrak{T}} y_1, y_2$ and $y_1, y_2 \Rightarrow^*_{\mathfrak{T}} z_1, z_2$, then $x_1, x_2 \Rightarrow^*_{\mathfrak{T}} z_1, z_2$.

(84) If $x, y \rightarrow_{\mathfrak{T}} z$, then $x, y \Rightarrow^*_{\mathfrak{T}} z, \langle\rangle_E$.

(85) If $x, v \rightarrow_{\mathfrak{T}} y$, then $x, v \frown w \Rightarrow^*_{\mathfrak{T}} y, w$.

(86) If $x, u \Rightarrow^*_{\mathfrak{T}} y, v$, then $x, u \frown w \Rightarrow^*_{\mathfrak{T}} y, v \frown w$.

(87) If $x_1, x_2 \Rightarrow_{\mathfrak{T}} y_1, y_2$, then $x_1, x_2 \Rightarrow^*_{\mathfrak{T}} y_1, y_2$.

(88) If $x, v \Rightarrow^*_{\mathfrak{T}} y, w$, then there exists u such that $v = u \frown w$.

(89) If $x, v \Rightarrow^*_{\mathfrak{T}} y, w$, then $\operatorname{len} w \leq \operatorname{len} v$.

(90) If $x, w \Rightarrow^*_{\mathfrak{T}} y, v \frown w$, then $v = \langle\rangle_E$.

(91) If $\langle\rangle_E \notin \operatorname{rng}\operatorname{dom}$ (the transition of $\mathfrak{T}$), then $x, u \Rightarrow^*_{\mathfrak{T}} y, u$ iff $x = y$.

(92) If $\langle\rangle_E \notin \operatorname{rng}\operatorname{dom}$ (the transition of $\mathfrak{T}$), then if $x, \langle e\rangle \Rightarrow^*_{\mathfrak{T}} y, \langle\rangle_E$, then $x, \langle e\rangle \Rightarrow_{\mathfrak{T}} y, \langle\rangle_E$.

(93) If $\mathfrak{T}$ is deterministic, then if $x_1, x_2 \Rightarrow^*_{\mathfrak{T}} y_1, z$ and $x_1, x_2 \Rightarrow^*_{\mathfrak{T}} y_2, z$, then $y_1 = y_2$.

9. Acceptance of Words

Let us consider E, F, $\mathfrak{T}$, x_1, x_2, y. The predicate $x_1, x_2 \Rightarrow^*_{\mathfrak{T}} y$ is defined as follows:

(Def. 7) $x_1, x_2 \Rightarrow^*_{\mathfrak{T}} y, \langle\rangle_E$.

The following propositions are true:

(94) Let $\mathfrak{T}_1$ be a non empty transition-system over F_1 and $\mathfrak{T}_2$ be a non empty transition-system over F_2. Suppose the carrier of $\mathfrak{T}_1 =$ the carrier of $\mathfrak{T}_2$ and the transition of $\mathfrak{T}_1 =$ the transition of $\mathfrak{T}_2$. If $x, y \Rightarrow^*_{\mathfrak{T}_1} z$, then $x, y \Rightarrow^*_{\mathfrak{T}_2} z$.

(95) $x, \langle\rangle_E \Rightarrow^*_{\mathfrak{T}} x$.

(96) If $x, u \Rightarrow^*_{\mathfrak{T}} y$, then $x, u \frown v \Rightarrow^*_{\mathfrak{T}} y, v$.

(97) If $x, y \rightarrow_{\mathfrak{T}} z$, then $x, y \Rightarrow^*_{\mathfrak{T}} z$.

(98) If $x_1, x_2 \Rightarrow_{\mathfrak{T}} y, \langle\rangle_E$, then $x_1, x_2 \Rightarrow^*_{\mathfrak{T}} y$.

(99) If $x, u \Rightarrow^*_{\mathfrak{T}} y$ and $y, v \Rightarrow^*_{\mathfrak{T}} z$, then $x, u \frown v \Rightarrow^*_{\mathfrak{T}} z$.

(100) If $\langle\rangle_E \notin \operatorname{rng}\operatorname{dom}$ (the transition of $\mathfrak{T}$), then $x, \langle\rangle_E \Rightarrow^*_{\mathfrak{T}} y$ iff $x = y$.

(101) If $\langle\rangle_E \notin \operatorname{rng}\operatorname{dom}$ (the transition of $\mathfrak{T}$), then if $x, \langle e\rangle \Rightarrow^*_{\mathfrak{T}} y$, then $x, \langle e\rangle \Rightarrow_{\mathfrak{T}} y, \langle\rangle_E$.

(102) If $\mathfrak{T}$ is deterministic, then if $x_1, x_2 \Rightarrow^*_{\mathfrak{T}} y_1$ and $x_1, x_2 \Rightarrow^*_{\mathfrak{T}} y_2$, then $y_1 = y_2$.

10. Reachable States

Let us consider E, F, $\mathfrak{T}$, x, X. The functor $x\text{-succ}_{\mathfrak{T}}(X)$ yields a subset of $\mathfrak{T}$ and is defined by:

(Def. 8) $x\text{-succ}_{\mathfrak{T}}(X) = \{s : \bigvee_t\ (t \in X\ \wedge\ t, x \Rightarrow^*_{\mathfrak{T}} s)\}$.

One can prove the following propositions:

(103) $s \in x\text{-succ}_{\mathfrak{T}}(X)$ iff there exists t such that $t \in X$ and $t, x \Rightarrow^*_{\mathfrak{T}} s$.

(104) If $\langle\rangle_E \notin \operatorname{rng}\operatorname{dom}$ (the transition of $\mathfrak{T}$), then $\langle\rangle_E\text{-succ}_{\mathfrak{T}}(S) = S$.

(105) Let $\mathfrak{T}_1$ be a non empty transition-system over F_1 and $\mathfrak{T}_2$ be a non empty transition-system over F_2. Suppose the carrier of $\mathfrak{T}_1 =$ the carrier of $\mathfrak{T}_2$ and the transition of $\mathfrak{T}_1 =$ the transition of $\mathfrak{T}_2$. Then $x\text{-succ}_{\mathfrak{T}_1}(X) = x\text{-succ}_{\mathfrak{T}_2}(X)$.

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. Reduction relations. *Formalized Mathematics*, 5(**4**):469–478, 1996.

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

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

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

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

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

[10] Karol Pąk. The Catalan numbers. Part II. *Formalized Mathematics*, 14(**4**):153–159, 2006, doi:10.2478/v10037-006-0019-7.

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

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

[13] Michał Trybulec. Formal languages – concatenation and closure. *Formalized Mathematics*, 15(**1**):11–15, 2007, doi:10.2478/v10037-007-0002-y.

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

[15] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.

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

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

Received May 5, 2009

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 173–178, 2009

Probability on Finite and Discrete Set and Uniform Distribution

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. A pseudorandom number generator plays an important role in practice in computer science. For example: computer simulations, cryptology, and so on. A pseudorandom number generator is an algorithm to generate a sequence of numbers that is indistinguishable from the true random number sequence. In this article, we shall formalize the "Uniform Distribution" that is the idealized set of true random number sequences. The basic idea of our formalization is due to [15].

MML identifier: DIST_1, version: 7.11.02 4.125.1059

The notation and terminology used in this paper are introduced in the following papers: [16], [10], [1], [3], [17], [6], [18], [8], [4], [5], [7], [2], [11], [13], [12], [9], [14], and [19].

1. Probability on Finite and Discrete Set

Let S be a non empty finite set and let s be a finite sequence of elements of S. We introduce the certain event of s as a synonym of $\operatorname{dom} s$.

Let S be a non empty finite set and let s be a non empty finite sequence of elements of S. Then the certain event of s is a non empty finite set.

Next we state the proposition

(1) Let S be a non empty finite set and s be a finite sequence of elements of S. Then the certain event of $s = s^{-1}(S)$.

Let S be a non empty finite set, let s be a finite sequence of elements of S, and let x be a set. We introduce $\mathcal{E}_i(s(i) = x)$ as a synonym of $s^{-1}(x)$.

ISSN 1426–2630(p), 1898-9934(e)

Let S be a non empty finite set, let s be a finite sequence of elements of S, and let x be a set. Then $\mathcal{E}_i(s(i) = x)$ is an event of the certain event of s.

Let S be a non empty finite set, let s be a finite sequence of elements of S, and let x be a set. The functor frequency(x, s) yielding a natural number is defined as follows:

(Def. 1) frequency$(x, s) = \overline{\overline{\mathcal{E}_i(s(i) = x)}}$.

One can prove the following propositions:

(2) Let S be a non empty finite set, s be a finite sequence of elements of S, and e be a set. Suppose $e \in$ the certain event of s. Then there exists an element x of S such that $e \in \mathcal{E}_i(s(i) = x)$.

(3) Let S be a non empty finite set and s be a finite sequence of elements of S. Then $\overline{\overline{\text{the certain event of } s}} = \operatorname{len} s$.

Let S be a non empty finite set, let s be a finite sequence of elements of S, and let x be a set. The functor $\mathrm{Prob}_{\mathrm{D}}(x, s)$ yielding a real number is defined as follows:

(Def. 2) $\mathrm{Prob}_{\mathrm{D}}(x, s) = \frac{\text{frequency}(x,s)}{\operatorname{len} s}$.

Next we state the proposition

(4) For every non empty finite set S and for every finite sequence s of elements of S and for every set x holds frequency$(x, s) = \operatorname{len} s \cdot \mathrm{Prob}_{\mathrm{D}}(x, s)$.

Let S be a non empty finite set and let s be a finite sequence of elements of S. The functor FDprobSEQ s yielding a finite sequence of elements of $\mathbb{R}$ is defined by:

(Def. 3) dom FDprobSEQ s = Seg $\overline{\overline{S}}$ and for every natural number n such that $n \in$ dom FDprobSEQ s holds (FDprobSEQ s)(n) = $\mathrm{Prob}_{\mathrm{D}}((\mathrm{CFS}(S))(n), s)$.

The following proposition is true

(5) Let S be a non empty finite set, s be a non empty finite sequence of elements of S, and x be a set. Then $\mathrm{Prob}_{\mathrm{D}}(x, s) = \mathrm{P}(\mathcal{E}_i(s(i) = x))$.

Let S be a non empty finite set and let s, t be finite sequences of elements of S. We say that s and t are probability equivalent if and only if:

(Def. 4) For every set x holds $\mathrm{Prob}_{\mathrm{D}}(x, s) = \mathrm{Prob}_{\mathrm{D}}(x, t)$.

Let us notice that the predicate s and t are probability equivalent is reflexive and symmetric.

The following proposition is true

(6) Let S be a non empty finite set and s, t, u be finite sequences of elements of S. Suppose s and t are probability equivalent and t and u are probability equivalent. Then s and u are probability equivalent.

Let S be a non empty finite set and let s be a finite sequence of elements of S. The equivalence class of s yielding a non empty subset of S^* is defined by the condition (Def. 5).

(Def. 5) The equivalence class of $s = \{t; t$ ranges over finite sequences of elements of S: s and t are probability equivalent$\}$.

Next we state three propositions:

(7) Let S be a non empty finite set and s, t be finite sequences of elements of S. Then s and t are probability equivalent if and only if $t \in$ the equivalence class of s.

(8) Let S be a non empty finite set and s be a finite sequence of elements of S. Then $s \in$ the equivalence class of s.

(9) Let S be a non empty finite set and s, t be finite sequences of elements of S. Then s and t are probability equivalent if and only if the equivalence class of $s =$ the equivalence class of t.

Let S be a non empty finite set. The distribution family of S yielding a non empty family of subsets of S^* is defined by the condition (Def. 6).

(Def. 6) Let A be a subset of S^*. Then $A \in$ the distribution family of S if and only if there exists a finite sequence s of elements of S such that $A =$ the equivalence class of s.

Next we state two propositions:

(10) Let S be a non empty finite set and s, t be finite sequences of elements of S. Then s and t are probability equivalent if and only if FDprobSEQ $s =$ FDprobSEQ t.

(11) Let S be a non empty finite set and s, t be finite sequences of elements of S. If $t \in$ the equivalence class of s, then FDprobSEQ $s =$ FDprobSEQ t.

Let S be a non empty finite set. The functor GenProbSEQ S yields a function from the distribution family of S into $\mathbb{R}^*$ and is defined by the condition (Def. 7).

(Def. 7) Let x be an element of the distribution family of S. Then there exists a finite sequence s of elements of S such that $s \in x$ and (GenProbSEQ S)$(x) =$ FDprobSEQ s.

One can prove the following proposition

(12) Let S be a non empty finite set and s be a finite sequence of elements of S. Then (GenProbSEQ S)(the equivalence class of s) $=$ FDprobSEQ s.

Let S be a non empty finite set. Observe that GenProbSEQ S is one-to-one.

Let S be a non empty finite set and let p be a finite probability distribution finite sequence of elements of $\mathbb{R}$. Let us assume that len $p = \overline{\overline{S}}$ and there exists a finite sequence s of elements of S such that FDprobSEQ $s = p$. The functor distribution(p, S) yielding an element of the distribution family of S is defined by:

(Def. 8) (GenProbSEQ S)(distribution$(p, S)) = p$.

Let S be a non empty finite set and let s be a finite sequence of elements of S. The functor freqSEQ s yields a finite sequence of elements of $\mathbb{N}$ and is defined by:

(Def. 9) $\operatorname{dom} \operatorname{freqSEQ} s = \operatorname{Seg} \overline{\overline{S}}$ and for every natural number n such that $n \in \operatorname{dom} \operatorname{freqSEQ} s$ holds $(\operatorname{freqSEQ} s)(n) = \operatorname{len} s \cdot (\operatorname{FDprobSEQ} s)(n)$.

One can prove the following propositions:

(13) Let S be a non empty finite set, s be a non empty finite sequence of elements of S, and n be a natural number. If $n \in \operatorname{Seg} \overline{\overline{S}}$, then there exists an element x of S such that $(\operatorname{freqSEQ} s)(n) = \operatorname{frequency}(x, s)$ and $x = (\operatorname{CFS}(S))(n)$.

(14) For every non empty finite set S and for every finite sequence s of elements of S holds $\operatorname{freqSEQ} s = \operatorname{len} s \cdot \operatorname{FDprobSEQ} s$.

(15) For every non empty finite set S and for every finite sequence s of elements of S holds $\sum \operatorname{freqSEQ} s = \operatorname{len} s \cdot \sum \operatorname{FDprobSEQ} s$.

(16) Let S be a non empty finite set, s be a non empty finite sequence of elements of S, and n be a natural number. Suppose $n \in \operatorname{dom} s$. Then there exists a natural number m such that $(\operatorname{freqSEQ} s)(m) = \operatorname{frequency}(s(n), s)$ and $s(n) = (\operatorname{CFS}(S))(m)$.

(17) Let n be a natural number, S be a function, and L be a finite sequence of elements of $\mathbb{N}$. Suppose that

(i) S is disjoint valued,

(ii) $\operatorname{dom} S = \operatorname{dom} L$,

(iii) $n = \operatorname{len} L$, and

(iv) for every natural number i such that $i \in \operatorname{dom} S$ holds $S(i)$ is finite and $L(i) = \operatorname{Card} S(i)$.

Then $\bigcup \operatorname{rng} S$ is finite and $\operatorname{Card} \bigcup \operatorname{rng} S = \sum L$.

(18) Let S be a function and L be a finite sequence of elements of $\mathbb{N}$. Suppose S is disjoint valued and $\operatorname{dom} S = \operatorname{dom} L$ and for every natural number i such that $i \in \operatorname{dom} S$ holds $S(i)$ is finite and $L(i) = \operatorname{Card} S(i)$. Then $\bigcup \operatorname{rng} S$ is finite and $\operatorname{Card} \bigcup \operatorname{rng} S = \sum L$.

(19) For every non empty finite set S and for every non empty finite sequence s of elements of S holds $\sum \operatorname{freqSEQ} s = \operatorname{len} s$.

(20) For every non empty finite set S and for every non empty finite sequence s of elements of S holds $\sum \operatorname{FDprobSEQ} s = 1$.

(21) Let S be a non empty finite set and s be a non empty finite sequence of elements of S. Then FDprobSEQ s is finite probability distribution.

Let S be a non empty finite set. A finite probability distribution finite sequence of elements of $\mathbb{R}$ is said to be a probability distribution finite sequence on S if:

(Def. 10) $\operatorname{len} \mathrm{it} = \overline{\overline{S}}$ and there exists a finite sequence s of elements of S such that FDprobSEQ $s = \mathrm{it}$.

The following proposition is true

(22) Let S be a non empty finite set and p be a probability distribution finite sequence on S. Then

(i) p is a finite probability distribution finite sequence of elements of $\mathbb{R}$,

(ii) $\operatorname{len} p = \overline{\overline{S}}$,

(iii) there exists a finite sequence s of elements of S such that FDprobSEQ $s = p$,

(iv) distribution(p, S) is an element of the distribution family of S, and

(v) (GenProbSEQ S)(distribution(p, S)) $= p$.

2. Uniform Distribution

Let S be a non empty finite set and let s be a finite sequence of elements of S. We say that s is uniformly distributed if and only if:

(Def. 11) For every natural number n such that $n \in \operatorname{dom}$ FDprobSEQ s holds (FDprobSEQ s)$(n) = \frac{1}{\overline{\overline{S}}}$.

We now state four propositions:

(23) Let S be a non empty finite set and s be a finite sequence of elements of S. If s is uniformly distributed, then FDprobSEQ s is constant.

(24) Let S be a non empty finite set and s, t be finite sequences of elements of S. Suppose s is uniformly distributed and s and t are probability equivalent. Then t is uniformly distributed.

(25) Let S be a non empty finite set and s, t be finite sequences of elements of S. Suppose s is uniformly distributed and t is uniformly distributed. Then s and t are probability equivalent.

(26) For every non empty finite set S holds CFS(S) is uniformly distributed.

Let S be a non empty finite set. The uniform distribution S yielding an element of the distribution family of S is defined by the condition (Def. 12).

(Def. 12) Let s be a finite sequence of elements of S. Then $s \in$ the uniform distribution S if and only if s is uniformly distributed.

Let S be a non empty finite set. One can check that there exists a probability distribution finite sequence on S which is constant.

Let S be a non empty finite set. The functor UniformFDprobSEQ S yielding a constant probability distribution finite sequence on S is defined as follows:

(Def. 13) UniformFDprobSEQ S = FDprobSEQ CFS(S).

We now state the proposition

(27) For every non empty finite set S holds the uniform distribution $S =$ distribution(UniformFDprobSEQ S, S).

References

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

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

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

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

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

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

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

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

[9] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

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

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

[12] Andrzej Nędzusiak. Probability. *Formalized Mathematics*, 1(**4**):745–749, 1990.

[13] Jan Popiołek. Introduction to probability. *Formalized Mathematics*, 1(**4**):755–760, 1990.

[14] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**):49–58, 2004.

[15] Victor Shoup. A computational introduction to number theory and algebra. *Cambridge University Press*, 2008.

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

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

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

[19] Bo Zhang and Yatsuka Nakamura. The definition of finite sequences and matrices of probability, and addition of matrices of real elements. *Formalized Mathematics*, 14(**3**):101–108, 2006, doi:10.2478/v10037-006-0012-1.

Received May 5, 2009

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 179–185, 2009

Riemann Integral of Functions from $\mathbb{R}$ into $\mathcal{R}^n$

Keiichi Miyajima
Ibaraki University
Hitachi, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we define the Riemann Integral of functions from $\mathbb{R}$ into $\mathcal{R}^n$, and prove the linearity of this operator. The presented method is based on [21].

MML identifier: `INTEGR15`, version: `7.11.02 4.125.1059`

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

1. Preliminaries

Let A be a closed-interval subset of $\mathbb{R}$, let f be a function from A into $\mathbb{R}$, let S be a non empty Division of A, and let D be an element of S. A finite sequence of elements of $\mathbb{R}$ is said to be a middle volume of f and D if it satisfies the conditions (Def. 1).

(Def. 1)(i) $\operatorname{len} \mathrm{it} = \operatorname{len} D$, and

(ii) for every natural number i such that $i \in \operatorname{dom} D$ there exists an element r of $\mathbb{R}$ such that $r \in \operatorname{rng}(f \restriction \operatorname{divset}(D, i))$ and $\mathrm{it}(i) = r \cdot \operatorname{vol}(\operatorname{divset}(D, i))$.

Let A be a closed-interval subset of $\mathbb{R}$, let f be a function from A into $\mathbb{R}$, let S be a non empty Division of A, let D be an element of S, and let F be a middle volume of f and D. The functor middle_sum(f, F) yielding a real number is defined as follows:

(Def. 2) $\text{middle\_sum}(f, F) = \sum F$.

We now state four propositions:

ISSN 1426–2630(p), 1898-9934(e)

(1) Let A be a closed-interval subset of $\mathbb{R}$, f be a function from A into $\mathbb{R}$, S be a non empty Division of A, D be an element of S, and F be a middle volume of f and D. If $f{\restriction}A$ is lower bounded, then $\mathrm{lower\_sum}(f, D) \leq \mathrm{middle\_sum}(f, F)$.

(2) Let A be a closed-interval subset of $\mathbb{R}$, f be a function from A into $\mathbb{R}$, S be a non empty Division of A, D be an element of S, and F be a middle volume of f and D. If $f{\restriction}A$ is upper bounded, then $\mathrm{middle\_sum}(f, F) \leq \mathrm{upper\_sum}(f, D)$.

(3) Let A be a closed-interval subset of $\mathbb{R}$, f be a function from A into $\mathbb{R}$, S be a non empty Division of A, D be an element of S, and e be a real number. Suppose $f{\restriction}A$ is lower bounded and $0 < e$. Then there exists a middle volume F of f and D such that $\mathrm{middle\_sum}(f, F) \leq \mathrm{lower\_sum}(f, D) + e$.

(4) Let A be a closed-interval subset of $\mathbb{R}$, f be a function from A into $\mathbb{R}$, S be a non empty Division of A, D be an element of S, and e be a real number. Suppose $f{\restriction}A$ is upper bounded and $0 < e$. Then there exists a middle volume F of f and D such that $\mathrm{upper\_sum}(f, D) - e \leq \mathrm{middle\_sum}(f, F)$.

Let A be a closed-interval subset of $\mathbb{R}$, let f be a function from A into $\mathbb{R}$, and let T be a DivSequence of A. A function from $\mathbb{N}$ into $\mathbb{R}^*$ is said to be a middle volume sequence of f and T if:

(Def. 3) For every element k of $\mathbb{N}$ holds $\mathrm{it}(k)$ is a middle volume of f and $T(k)$.

Let A be a closed-interval subset of $\mathbb{R}$, let f be a function from A into $\mathbb{R}$, let T be a DivSequence of A, let S be a middle volume sequence of f and T, and let k be an element of $\mathbb{N}$. Then $S(k)$ is a middle volume of f and $T(k)$.

Let A be a closed-interval subset of $\mathbb{R}$, let f be a function from A into $\mathbb{R}$, let T be a DivSequence of A, and let S be a middle volume sequence of f and T. The functor $\mathrm{middle\_sum}(f, S)$ yields a sequence of real numbers and is defined as follows:

(Def. 4) For every element i of $\mathbb{N}$ holds $(\mathrm{middle\_sum}(f, S))(i) = \mathrm{middle\_sum}(f, S(i))$.

One can prove the following propositions:

(5) Let A be a closed-interval subset of $\mathbb{R}$, f be a function from A into $\mathbb{R}$, T be a DivSequence of A, S be a middle volume sequence of f and T, and i be an element of $\mathbb{N}$. If $f{\restriction}A$ is lower bounded, then $(\mathrm{lower\_sum}(f, T))(i) \leq (\mathrm{middle\_sum}(f, S))(i)$.

(6) Let A be a closed-interval subset of $\mathbb{R}$, f be a function from A into $\mathbb{R}$, T be a DivSequence of A, S be a middle volume sequence of f and T, and i be an element of $\mathbb{N}$. If $f{\restriction}A$ is upper bounded, then $(\mathrm{middle\_sum}(f, S))(i) \leq (\mathrm{upper\_sum}(f, T))(i)$.

(7) Let A be a closed-interval subset of $\mathbb{R}$, f be a function from A into $\mathbb{R}$, T be a DivSequence of A, and e be an element of $\mathbb{R}$. Suppose $0 < e$ and $f{\restriction}A$ is lower bounded. Then there exists a middle volume sequence S of

f and T such that for every element i of $\mathbb{N}$ holds $(\mathrm{middle\_sum}(f,S))(i) \leq (\mathrm{lower\_sum}(f,T))(i) + e$.

(8) Let A be a closed-interval subset of $\mathbb{R}$, f be a function from A into $\mathbb{R}$, T be a DivSequence of A, and e be an element of $\mathbb{R}$. Suppose $0 < e$ and $f \restriction A$ is upper bounded. Then there exists a middle volume sequence S of f and T such that for every element i of $\mathbb{N}$ holds $(\mathrm{upper\_sum}(f,T))(i) - e \leq (\mathrm{middle\_sum}(f,S))(i)$.

(9) Let A be a closed-interval subset of $\mathbb{R}$, f be a function from A into $\mathbb{R}$, T be a DivSequence of A, and S be a middle volume sequence of f and T. Suppose f is bounded and f is integrable on A and δ_T is convergent and $\lim(\delta_T) = 0$. Then $\mathrm{middle\_sum}(f,S)$ is convergent and $\lim \mathrm{middle\_sum}(f,S) = \mathrm{integral}\, f$.

(10) Let A be a closed-interval subset of $\mathbb{R}$ and f be a function from A into $\mathbb{R}$. Suppose f is bounded. Then f is integrable on A if and only if there exists a real number I such that for every DivSequence 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 $\mathrm{middle\_sum}(f,S)$ is convergent and $\lim \mathrm{middle\_sum}(f,S) = I$.

Let n be an element of $\mathbb{N}$, let A be a closed-interval subset of $\mathbb{R}$, let f be a function from A into $\mathcal{R}^n$, let S be a non empty Division of A, and let D be an element of S. A finite sequence of elements of $\mathcal{R}^n$ is said to be a middle volume of f and D if it satisfies the conditions (Def. 5).

(Def. 5)(i) $\mathrm{len}\, \mathrm{it} = \mathrm{len}\, D$, and

(ii) for every natural number i such that $i \in \mathrm{dom}\, D$ there exists an element r of $\mathcal{R}^n$ such that $r \in \mathrm{rng}(f \restriction \mathrm{divset}(D,i))$ and $\mathrm{it}(i) = \mathrm{vol}(\mathrm{divset}(D,i)) \cdot r$.

Let n be an element of $\mathbb{N}$, let A be a closed-interval subset of $\mathbb{R}$, let f be a function from A into $\mathcal{R}^n$, let S be a non empty Division of A, let D be an element of S, and let F be a middle volume of f and D. The functor $\mathrm{middle\_sum}(f,F)$ yields an element of $\mathcal{R}^n$ and is defined by the condition (Def. 6).

(Def. 6) Let i be an element of $\mathbb{N}$. Suppose $i \in \mathrm{Seg}\, n$. Then there exists a finite sequence F_1 of elements of $\mathbb{R}$ such that $F_1 = \mathrm{proj}(i,n) \cdot F$ and $(\mathrm{middle\_sum}(f,F))(i) = \sum F_1$.

Let n be an element of $\mathbb{N}$, let A be a closed-interval subset of $\mathbb{R}$, let f be a function from A into $\mathcal{R}^n$, and let T be a DivSequence of A. A function from $\mathbb{N}$ into $(\mathcal{R}^n)^*$ is said to be a middle volume sequence of f and T if:

(Def. 7) For every element k of $\mathbb{N}$ holds $\mathrm{it}(k)$ is a middle volume of f and $T(k)$.

Let n be an element of $\mathbb{N}$, let A be a closed-interval subset of $\mathbb{R}$, let f be a function from A into $\mathcal{R}^n$, let T be a DivSequence of A, let S be a middle volume sequence of f and T, and let k be an element of $\mathbb{N}$. Then $S(k)$ is a middle volume of f and $T(k)$.

Let n be an element of $\mathbb{N}$, let A be a closed-interval subset of $\mathbb{R}$, let f be a function from A into $\mathcal{R}^n$, let T be a DivSequence of A, and let S be a middle volume sequence of f and T. The functor middle_sum(f, S) yields a sequence of $\langle \mathcal{E}^n, \| \cdot \| \rangle$ and is defined as follows:

(Def. 8) For every element i of $\mathbb{N}$ holds $(\text{middle\_sum}(f, S))(i) = \text{middle\_sum}(f, S(i))$.

Let n be an element of $\mathbb{N}$, let Z be a non empty set, and let f, g be partial functions from Z to $\mathcal{R}^n$. The functor $f + g$ yields a partial function from Z to $\mathcal{R}^n$ and is defined by:

(Def. 9) $\text{dom}(f + g) = \text{dom}\, f \cap \text{dom}\, g$ and for every element c of Z such that $c \in \text{dom}(f + g)$ holds $(f + g)_c = f_c + g_c$.

The functor $f - g$ yielding a partial function from Z to $\mathcal{R}^n$ is defined by:

(Def. 10) $\text{dom}(f - g) = \text{dom}\, f \cap \text{dom}\, g$ and for every element c of Z such that $c \in \text{dom}(f - g)$ holds $(f - g)_c = f_c - g_c$.

Let n be an element of $\mathbb{N}$, let r be a real number, let Z be a non empty set, and let f be a partial function from Z to $\mathcal{R}^n$. The functor $r\, f$ yields a partial function from Z to $\mathcal{R}^n$ and is defined by:

(Def. 11) $\text{dom}(r\, f) = \text{dom}\, f$ and for every element c of Z such that $c \in \text{dom}(r\, f)$ holds $(r\, f)_c = r \cdot f_c$.

2. Definition of Riemann Integral of Functions from $\mathbb{R}$ into $\mathcal{R}^n$

Let n be an element of $\mathbb{N}$, let A be a closed-interval subset of $\mathbb{R}$, and let f be a function from A into $\mathcal{R}^n$. We say that f is bounded if and only if:

(Def. 12) For every element i of $\mathbb{N}$ such that $i \in \text{Seg}\, n$ holds $\text{proj}(i, n) \cdot f$ is bounded.

Let n be an element of $\mathbb{N}$, let A be a closed-interval subset of $\mathbb{R}$, and let f be a function from A into $\mathcal{R}^n$. We say that f is integrable if and only if:

(Def. 13) For every element i of $\mathbb{N}$ such that $i \in \text{Seg}\, n$ holds $\text{proj}(i, n) \cdot f$ is integrable on A.

Let n be an element of $\mathbb{N}$, let A be a closed-interval subset of $\mathbb{R}$, and let f be a function from A into $\mathcal{R}^n$. The functor integral f yielding an element of $\mathcal{R}^n$ is defined by:

(Def. 14) $\text{dom}\,\text{integral}\, f = \text{Seg}\, n$ and for every element i of $\mathbb{N}$ such that $i \in \text{Seg}\, n$ holds $(\text{integral}\, f)(i) = \text{integral}\,\text{proj}(i, n) \cdot f$.

One can prove the following propositions:

(11) Let n be an element of $\mathbb{N}$, A be a closed-interval subset of $\mathbb{R}$, f be a function from A into $\mathcal{R}^n$, T be a DivSequence of A, and S be a middle volume sequence of f and T. Suppose f is bounded and integrable and δ_T is convergent and $\lim(\delta_T) = 0$. Then middle_sum(f, S) is convergent and $\lim \text{middle\_sum}(f, S) = \text{integral}\, f$.

(12) Let n be an element of $\mathbb{N}$, A be a closed-interval subset of $\mathbb{R}$, and f be a function from A into $\mathcal{R}^n$. Suppose f is bounded. Then f is integrable if and only if there exists an element I of $\mathcal{R}^n$ such that for every DivSequence 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 $\lim \text{middle\_sum}(f, S) = I$.

Let n be an element of $\mathbb{N}$ and let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. We say that f is bounded if and only if:

(Def. 15) For every element i of $\mathbb{N}$ such that $i \in \operatorname{Seg} n$ holds $\operatorname{proj}(i, n) \cdot f$ is bounded.

Let n be an element of $\mathbb{N}$, let A be a closed-interval subset of $\mathbb{R}$, and let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. We say that f is integrable on A if and only if:

(Def. 16) For every element i of $\mathbb{N}$ such that $i \in \operatorname{Seg} n$ holds $\operatorname{proj}(i, n) \cdot f$ is integrable on A.

Let n be an element of $\mathbb{N}$, let A be a closed-interval subset of $\mathbb{R}$, and let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. The functor $\int\limits_{A} f(x)dx$ yielding an element of $\mathcal{R}^n$ is defined by:

(Def. 17) $\operatorname{dom} \int\limits_{A} f(x)dx = \operatorname{Seg} n$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{Seg} n$ holds $(\int\limits_{A} f(x)dx)(i) = \int\limits_{A} (\operatorname{proj}(i, n) \cdot f)(x)dx$.

We now state two propositions:

(13) Let n be an element of $\mathbb{N}$, A be a closed-interval subset of $\mathbb{R}$, f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$, and g be a function from A into $\mathcal{R}^n$. Suppose $f \restriction A = g$. Then f is integrable on A if and only if g is integrable.

(14) Let n be an element of $\mathbb{N}$, A be a closed-interval subset of $\mathbb{R}$, f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$, and g be a function from A into $\mathcal{R}^n$. If $f \restriction A = g$, then $\int\limits_{A} f(x)dx = \operatorname{integral} g$.

Let a, b be real numbers, let n be an element of $\mathbb{N}$, and let f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. The functor $\int\limits_{a}^{b} f(x)dx$ yielding an element of $\mathcal{R}^n$ is defined as follows:

(Def. 18) $\operatorname{dom} \int\limits_{a}^{b} f(x)dx = \operatorname{Seg} n$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{Seg} n$ holds $(\int\limits_{a}^{b} f(x)dx)(i) = \int\limits_{a}^{b} (\operatorname{proj}(i, n) \cdot f)(x)dx$.

3. Linearity of Integration Operator

Next we state several propositions:

(15) Let n be an element of $\mathbb{N}$, f_1, f_2 be partial functions from $\mathbb{R}$ to $\mathcal{R}^n$, and i be an element of $\mathbb{N}$. If $i \in \operatorname{Seg} n$, then $\operatorname{proj}(i,n) \cdot (f_1 + f_2) = \operatorname{proj}(i,n) \cdot f_1 + \operatorname{proj}(i,n) \cdot f_2$ and $\operatorname{proj}(i,n) \cdot (f_1 - f_2) = \operatorname{proj}(i,n) \cdot f_1 - \operatorname{proj}(i,n) \cdot f_2$.

(16) Let n be an element of $\mathbb{N}$, r be a real number, f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$, and i be an element of $\mathbb{N}$. If $i \in \operatorname{Seg} n$, then $\operatorname{proj}(i,n) \cdot (r\, f) = r\, (\operatorname{proj}(i,n) \cdot f)$.

(17) Let n be an element of $\mathbb{N}$, A be a closed-interval subset of $\mathbb{R}$, and f_1, f_2 be partial functions from $\mathbb{R}$ to $\mathcal{R}^n$. Suppose f_1 is integrable on A and f_2 is integrable on A and $A \subseteq \operatorname{dom} f_1$ and $A \subseteq \operatorname{dom} f_2$ and $f_1 \restriction A$ is bounded and $f_2 \restriction A$ is bounded. Then $f_1 + f_2$ is integrable on A and $f_1 - f_2$ is integrable on A and $\int\limits_A (f_1 + f_2)(x)dx = \int\limits_A f_1(x)dx + \int\limits_A f_2(x)dx$ and $\int\limits_A (f_1 - f_2)(x)dx = \int\limits_A f_1(x)dx - \int\limits_A f_2(x)dx$.

(18) Let n be an element of $\mathbb{N}$, r be a real number, A be a closed-interval subset of $\mathbb{R}$, and f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$. Suppose $A \subseteq \operatorname{dom} f$ and f is integrable on A and $f \restriction A$ is bounded. Then $r\, f$ is integrable on A and $\int\limits_A (r\, f)(x)dx = r \cdot \int\limits_A f(x)dx$.

(19) Let n be an element of $\mathbb{N}$, f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$, A be a closed-interval subset of $\mathbb{R}$, and a, b be real numbers. If $A = [a,b]$, then $\int\limits_A f(x)dx = \int\limits_a^b f(x)dx$.

(20) Let n be an element of $\mathbb{N}$, f be a partial function from $\mathbb{R}$ to $\mathcal{R}^n$, A be a closed-interval subset of $\mathbb{R}$, and a, b be real numbers. If $A = [b,a]$, then $-\int\limits_A f(x)dx = \int\limits_a^b f(x)dx$.

References

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

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

[3] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.

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

[5] Czesław Byliński. Functions 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. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

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

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

[11] Noboru Endou and Yasunari Shidama. Completeness of the real Euclidean space. *Formalized Mathematics*, 13(**4**):577–580, 2005.

[12] Noboru Endou, Yasunari Shidama, and Keiichi Miyajima. Partial differentiation on normed linear spaces $\mathcal{R}^n$. *Formalized Mathematics*, 15(**2**):65–72, 2007, doi:10.2478/v10037-007-0008-5.

[13] 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.

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

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

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

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

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

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

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

[21] Murray R. Spiegel. *Theory and Problems of Vector Analysis.* McGraw-Hill, 1974.

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

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

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

Received May 5, 2009

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 187–192, 2009

Basic Properties of Even and Odd Functions

Bo Li
Qingdao University of Science
and Technology
China

Yanhong Men
Qingdao University of Science
and Technology
China

Summary. In this article we present definitions, basic properties and some examples of even and odd functions [6].

MML identifier: `FUNCT_8`, version: `7.11.02 4.125.1059`

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

1. Even and Odd Functions

In this paper x, r denote real numbers.

Let A be a set. We say that A is symmetrical if and only if:

(Def. 1) For every complex number x such that $x \in A$ holds $-x \in A$.

One can verify that there exists a subset of $\mathbb{C}$ which is symmetrical.

Let us observe that there exists a subset of $\mathbb{R}$ which is symmetrical.

In the sequel A denotes a symmetrical subset of $\mathbb{C}$.

Let R be a binary relation. We say that R has symmetrical domain if and only if:

(Def. 2) $\operatorname{dom} R$ is symmetrical.

One can verify that every binary relation which is empty has also symmetrical domain and there exists a binary relation which has symmetrical domain.

Let R be a binary relation with symmetrical domain. Note that $\operatorname{dom} R$ is symmetrical.

Let X, Y be complex-membered sets and let F be a partial function from X to Y. We say that F is quasi even if and only if:

ISSN 1426–2630(p), 1898-9934(e)

(Def. 3) For every x such that x, $-x \in \operatorname{dom} F$ holds $F(-x) = F(x)$.

Let X, Y be complex-membered sets and let F be a partial function from X to Y. We say that F is even if and only if:

(Def. 4) F is quasi even and has symmetrical domain.

Let X, Y be complex-membered sets. One can check that every partial function from X to Y which is quasi even and has symmetrical domain is also even and every partial function from X to Y which is even is also quasi even and has symmetrical domain.

Let A be a set, let X, Y be complex-membered sets, and let F be a partial function from X to Y. We say that F is even on A if and only if:

(Def. 5) $A \subseteq \operatorname{dom} F$ and $F{\restriction}A$ is even.

Let X, Y be complex-membered sets and let F be a partial function from X to Y. We say that F is quasi odd if and only if:

(Def. 6) For every x such that x, $-x \in \operatorname{dom} F$ holds $F(-x) = -F(x)$.

Let X, Y be complex-membered sets and let F be a partial function from X to Y. We say that F is odd if and only if:

(Def. 7) F is quasi odd and has symmetrical domain.

Let X, Y be complex-membered sets. Note that every partial function from X to Y which is quasi odd and has symmetrical domain is also odd and every partial function from X to Y which is odd is also quasi odd and has symmetrical domain.

Let A be a set, let X, Y be complex-membered sets, and let F be a partial function from X to Y. We say that F is odd on A if and only if:

(Def. 8) $A \subseteq \operatorname{dom} F$ and $F{\restriction}A$ is odd.

In the sequel F, G denote partial functions from $\mathbb{R}$ to $\mathbb{R}$.

One can prove the following propositions:

(1) F is odd on A iff $A \subseteq \operatorname{dom} F$ and for every x such that $x \in A$ holds $F(x) + F(-x) = 0$.

(2) F is even on A iff $A \subseteq \operatorname{dom} F$ and for every x such that $x \in A$ holds $F(x) - F(-x) = 0$.

(3) If F is odd on A and for every x such that $x \in A$ holds $F(x) \neq 0$, then $A \subseteq \operatorname{dom} F$ and for every x such that $x \in A$ holds $\frac{F(x)}{F(-x)} = -1$.

(4) If $A \subseteq \operatorname{dom} F$ and for every x such that $x \in A$ holds $\frac{F(x)}{F(-x)} = -1$, then F is odd on A.

(5) If F is even on A and for every x such that $x \in A$ holds $F(x) \neq 0$, then $A \subseteq \operatorname{dom} F$ and for every x such that $x \in A$ holds $\frac{F(x)}{F(-x)} = 1$.

(6) If $A \subseteq \operatorname{dom} F$ and for every x such that $x \in A$ holds $\frac{F(x)}{F(-x)} = 1$, then F is even on A.

(7) If F is even on A and odd on A, then for every x such that $x \in A$ holds $F(x) = 0$.

(8) If F is even on A, then for every x such that $x \in A$ holds $F(x) = F(|x|)$.

(9) If $A \subseteq \operatorname{dom} F$ and for every x such that $x \in A$ holds $F(x) = F(|x|)$, then F is even on A.

(10) If F is odd on A and G is odd on A, then $F + G$ is odd on A.

(11) If F is even on A and G is even on A, then $F + G$ is even on A.

(12) If F is odd on A and G is odd on A, then $F - G$ is odd on A.

(13) If F is even on A and G is even on A, then $F - G$ is even on A.

(14) If F is odd on A, then $r\,F$ is odd on A.

(15) If F is even on A, then $r\,F$ is even on A.

(16) If F is odd on A, then $-F$ is odd on A.

(17) If F is even on A, then $-F$ is even on A.

(18) If F is odd on A, then F^{-1} is odd on A.

(19) If F is even on A, then F^{-1} is even on A.

(20) If F is odd on A, then $|F|$ is even on A.

(21) If F is even on A, then $|F|$ is even on A.

(22) If F is odd on A and G is odd on A, then $F\,G$ is even on A.

(23) If F is even on A and G is even on A, then $F\,G$ is even on A.

(24) If F is even on A and G is odd on A, then $F\,G$ is odd on A.

(25) If F is even on A, then $r + F$ is even on A.

(26) If F is even on A, then $F - r$ is even on A.

(27) If F is even on A, then $F^{\mathbf{2}}$ is even on A.

(28) If F is odd on A, then $F^{\mathbf{2}}$ is even on A.

(29) If F is odd on A and G is odd on A, then F/G is even on A.

(30) If F is even on A and G is even on A, then F/G is even on A.

(31) If F is odd on A and G is even on A, then F/G is odd on A.

(32) If F is even on A and G is odd on A, then F/G is odd on A.

(33) If F is odd, then $-F$ is odd.

(34) If F is even, then $-F$ is even.

(35) If F is odd, then F^{-1} is odd.

(36) If F is even, then F^{-1} is even.

(37) If F is odd, then $|F|$ is even.

(38) If F is even, then $|F|$ is even.

(39) If F is odd, then $F^{\mathbf{2}}$ is even.

(40) If F is even, then $F^{\mathbf{2}}$ is even.

(41) If F is even, then $r + F$ is even.

(42) If F is even, then $F - r$ is even.

(43) If F is odd, then $r\,F$ is odd.

(44) If F is even, then $r\,F$ is even.

(45) If F is odd and G is odd and $\operatorname{dom} F \cap \operatorname{dom} G$ is symmetrical, then $F + G$ is odd.

(46) If F is even and G is even and $\operatorname{dom} F \cap \operatorname{dom} G$ is symmetrical, then $F + G$ is even.

(47) If F is odd and G is odd and $\operatorname{dom} F \cap \operatorname{dom} G$ is symmetrical, then $F - G$ is odd.

(48) If F is even and G is even and $\operatorname{dom} F \cap \operatorname{dom} G$ is symmetrical, then $F - G$ is even.

(49) If F is odd and G is odd and $\operatorname{dom} F \cap \operatorname{dom} G$ is symmetrical, then $F\,G$ is even.

(50) If F is even and G is even and $\operatorname{dom} F \cap \operatorname{dom} G$ is symmetrical, then $F\,G$ is even.

(51) If F is even and G is odd and $\operatorname{dom} F \cap \operatorname{dom} G$ is symmetrical, then $F\,G$ is odd.

(52) If F is odd and G is odd and $\operatorname{dom} F \cap \operatorname{dom} G$ is symmetrical, then F/G is even.

(53) If F is even and G is even and $\operatorname{dom} F \cap \operatorname{dom} G$ is symmetrical, then F/G is even.

(54) If F is odd and G is even and $\operatorname{dom} F \cap \operatorname{dom} G$ is symmetrical, then F/G is odd.

(55) If F is even and G is odd and $\operatorname{dom} F \cap \operatorname{dom} G$ is symmetrical, then F/G is odd.

2. Some Examples

The function signum from $\mathbb{R}$ into $\mathbb{R}$ is defined as follows:

(Def. 9) For every real number x holds $\operatorname{signum}(x) = \operatorname{sgn} x$.

Let x be a real number. One can check that $\operatorname{signum}(x)$ is real.

We now state a number of propositions:

(56) For every real number x such that $x > 0$ holds $\operatorname{signum}(x) = 1$.

(57) For every real number x such that $x < 0$ holds $\operatorname{signum}(x) = -1$.

(58) $\operatorname{signum}(0) = 0$.

(59) For every real number x holds $\operatorname{signum}(-x) = -\operatorname{signum}(x)$.

(60) For every symmetrical subset A of $\mathbb{R}$ holds signum is odd on A.

(61) For every real number x such that $x \geq 0$ holds $|\square|_{\mathbb{R}}(x) = x$.

(62) For every real number x such that $x < 0$ holds $|\Box|_{\mathbb{R}}(x) = -x$.

(63) For every real number x holds $|\Box|_{\mathbb{R}}(-x) = |\Box|_{\mathbb{R}}(x)$.

(64) For every symmetrical subset A of $\mathbb{R}$ holds $|\Box|_{\mathbb{R}}$ is even on A.

(65) For every symmetrical subset A of $\mathbb{R}$ holds the function sin is odd on A.

(66) For every symmetrical subset A of $\mathbb{R}$ holds the function cos is even on A.

Let us note that the function sin is odd.

Let us note that the function cos is even.

The following two propositions are true:

(67) For every symmetrical subset A of $\mathbb{R}$ holds the function sinh is odd on A.

(68) For every symmetrical subset A of $\mathbb{R}$ holds the function cosh is even on A.

One can check that the function sinh is odd.

Let us mention that the function cosh is even.

We now state a number of propositions:

(69) If $A \subseteq]-\frac{\pi}{2}, \frac{\pi}{2}[$, then the function tan is odd on A.

(70) Suppose $A \subseteq \mathrm{dom}\,(\text{the function tan})$ and for every x such that $x \in A$ holds $(\text{the function cos})(x) \neq 0$. Then the function tan is odd on A.

(71) Suppose $A \subseteq \mathrm{dom}\,(\text{the function cot})$ and for every x such that $x \in A$ holds $(\text{the function sin})(x) \neq 0$. Then the function cot is odd on A.

(72) If $A \subseteq [-1, 1]$, then the function arctan is odd on A.

(73) For every symmetrical subset A of $\mathbb{R}$ holds |the function sin | is even on A.

(74) For every symmetrical subset A of $\mathbb{R}$ holds |the function cos | is even on A.

(75) For every symmetrical subset A of $\mathbb{R}$ holds (the function sin) $^{-1}$ is odd on A.

(76) For every symmetrical subset A of $\mathbb{R}$ holds (the function cos) $^{-1}$ is even on A.

(77) For every symmetrical subset A of $\mathbb{R}$ holds $-$the function sin is odd on A.

(78) For every symmetrical subset A of $\mathbb{R}$ holds $-$the function cos is even on A.

(79) For every symmetrical subset A of $\mathbb{R}$ holds (the function sin)$^{\mathbf{2}}$ is even on A.

(80) For every symmetrical subset A of $\mathbb{R}$ holds (the function cos)$^{\mathbf{2}}$ is even on A.

In the sequel B is a symmetrical subset of $\mathbb{R}$.

One can prove the following four propositions:

(81) If $B \subseteq \operatorname{dom}$ (the function sec), then the function sec is even on B.

(82) If for every real number x such that $x \in B$ holds (the function cos)$(x) \neq 0$, then the function sec is even on B.

(83) If $B \subseteq \operatorname{dom}$ (the function cosec), then the function cosec is odd on B.

(84) If for every real number x such that $x \in B$ holds (the function sin)$(x) \neq 0$, then the function cosec is odd on B.

References

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

[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] Pacharapokin Chanapat, Kanchun, and Hiroshi Yamazaki. Formulas and identities of trigonometric functions. *Formalized Mathematics*, 12(**2**):139–141, 2004.

[6] Chuanzhang Chen. *Mathematical Analysis.* Higher Education Press, Beijing, 1978.

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

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

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

[10] Xiquan Liang and Bing Xie. Inverse trigonometric functions arctan and arccot. *Formalized Mathematics*, 16(**2**):147–158, 2008, doi:10.2478/v10037-008-0021-3.

[11] Takashi Mitsuishi and Yuguang Yang. Properties of the trigonometric function. *Formalized Mathematics*, 8(**1**):103–106, 1999.

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

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

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

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

[16] Peng Wang and Bo Li. Several differentiation formulas of special functions. Part V. *Formalized Mathematics*, 15(**3**):73–79, 2007, doi:10.2478/v10037-007-0009-4.

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

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

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

Received May 25, 2009

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 193–199, 2009

Equivalence of Deterministic and Nondeterministic Epsilon Automata

Michał Trybulec
YAC Software
Warsaw, Poland

Summary. Based on concepts introduced in [14], semiautomata and left-languages, automata and right-languages, and langauges accepted by automata are defined. The powerset construction is defined for transition systems, semiautomata and automata. Finally, the equivalence of deterministic and nondeterministic epsilon automata is shown.

MML identifier: FSM_3, version: 7.11.02 4.125.1059

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

1. Preliminaries

For simplicity, we adopt the following convention: x, y, X denote sets, E denotes a non empty set, e denotes an element of E, u, u_1, v, v_1, v_2, w denote elements of E^{ω}, F denotes a subset of E^{ω}, i, k, l denote natural numbers, $\mathfrak{T}$ denotes a non empty transition-system over F, and S, T denote subsets of $\mathfrak{T}$.

One can prove the following propositions:

(1) If $i \geq k + l$, then $i \geq k$.

(2) For all finite sequences a, b such that $a \frown b = a$ or $b \frown a = a$ holds $b = \emptyset$.

(3) For all finite sequences p, q such that $k \in \operatorname{dom} p$ and $\operatorname{len} p + 1 = \operatorname{len} q$ holds $k + 1 \in \operatorname{dom} q$.

(4) If $\operatorname{len} u = 1$, then there exists e such that $\langle e \rangle = u$ and $e = u(0)$.

ISSN 1426–2630(p), 1898-9934(e)

(5) If $k \neq 0$ and $\operatorname{len} u \leq k+1$, then there exist v_1, v_2 such that $\operatorname{len} v_1 \leq k$ and $\operatorname{len} v_2 \leq k$ and $u = v_1 \mathbin{^\frown} v_2$.

(6) For all finite 0-sequences p, q such that $\langle x \rangle \mathbin{^\frown} p = \langle y \rangle \mathbin{^\frown} q$ holds $x = y$ and $p = q$.

(7) If $\operatorname{len} u > 0$, then there exist e, u_1 such that $u = \langle e \rangle \mathbin{^\frown} u_1$.

Let us consider E. One can verify that $\operatorname{Lex} E$ is non empty.

Next we state three propositions:

(8) $\langle\rangle_E \notin \operatorname{Lex} E$.

(9) $u \in \operatorname{Lex} E$ iff $\operatorname{len} u = 1$.

(10) If $u \neq v$ and u, $v \in \operatorname{Lex} E$, then it is not true that there exists w such that $u \mathbin{^\frown} w = v$ or $w \mathbin{^\frown} u = v$.

2. Transition Systems over Lex E

The following propositions are true:

(11) For every transition-system $\mathfrak{T}$ over $\operatorname{Lex} E$ holds $\langle\rangle_E \notin \operatorname{rng} \operatorname{dom}$ (the transition of $\mathfrak{T}$).

(12) For every transition-system $\mathfrak{T}$ over $\operatorname{Lex} E$ such that the transition of $\mathfrak{T}$ is a function holds $\mathfrak{T}$ is deterministic.

3. Powerset Construction for Transition Systems

Let us consider E, F, $\mathfrak{T}$. The functor $\operatorname{bool} \mathfrak{T}$ yielding a strict transition-system over $\operatorname{Lex} E$ is defined by the conditions (Def. 1).

(Def. 1)(i) The carrier of $\operatorname{bool} \mathfrak{T} = 2^{\text{the carrier of } \mathfrak{T}}$, and

(ii) for all S, w, T holds $\langle\langle S, w\rangle, T\rangle \in$ the transition of $\operatorname{bool} \mathfrak{T}$ iff $\operatorname{len} w = 1$ and $T = w\text{-succ}_{\mathfrak{T}}(S)$.

Let us consider E, F, $\mathfrak{T}$. Note that $\operatorname{bool} \mathfrak{T}$ is non empty and deterministic.

Let us consider E, F and let $\mathfrak{T}$ be a finite non empty transition-system over F. One can check that $\operatorname{bool} \mathfrak{T}$ is finite.

The following two propositions are true:

(13) If $x, \langle e \rangle \Rightarrow^{*}_{\operatorname{bool} \mathfrak{T}} y, \langle\rangle_E$, then $x, \langle e \rangle \Rightarrow_{\operatorname{bool} \mathfrak{T}} y, \langle\rangle_E$.

(14) If $\operatorname{len} w = 1$, then $X = w\text{-succ}_{\mathfrak{T}}(S)$ iff $S, w \Rightarrow^{*}_{\operatorname{bool} \mathfrak{T}} X$.

4. Semiautomata

Let us consider E, F. We consider semiautomata over F as extensions of transition-system over F as systems

⟨ a carrier, a transition, an initial state ⟩,

where the carrier is a set, the transition is a relation between the carrier$\times F$ and the carrier, and the initial state is a subset of the carrier.

Let us consider E, F and let $\mathfrak{S}$ be a semiautomaton over F. We say that $\mathfrak{S}$ is deterministic if and only if:

(Def. 2) The transition-system of $\mathfrak{S}$ is deterministic and Card (the initial state of $\mathfrak{S}$) $= 1$.

Let us consider E, F. One can check that there exists a semiautomaton over F which is strict, non empty, finite, and deterministic.

In the sequel $\mathfrak{S}$ is a non empty semiautomaton over F.

Let us consider E, F, $\mathfrak{S}$. Observe that the transition-system of $\mathfrak{S}$ is non empty.

Let us consider E, F, $\mathfrak{S}$. The functor bool $\mathfrak{S}$ yields a strict semiautomaton over Lex E and is defined by the conditions (Def. 3).

(Def. 3)(i) The transition-system of bool $\mathfrak{S}$ = bool (the transition-system of $\mathfrak{S}$), and

(ii) the initial state of bool $\mathfrak{S} = \{\langle\rangle_E$-succ$_{\mathfrak{S}}$(the initial state of $\mathfrak{S})\}$.

Let us consider E, F, $\mathfrak{S}$. Observe that bool $\mathfrak{S}$ is non empty and deterministic.

The following proposition is true

(15) The carrier of bool $\mathfrak{S} = 2^{\text{the carrier of } \mathfrak{S}}$.

Let us consider E, F and let $\mathfrak{S}$ be a finite non empty semiautomaton over F. Observe that bool $\mathfrak{S}$ is finite.

5. Left-languages

Let us consider E, F, $\mathfrak{S}$ and let Q be a subset of $\mathfrak{S}$. The functor left-Lang Q yields a subset of E^ω and is defined as follows:

(Def. 4) left-Lang $Q = \{w : Q$ meets w-succ$_{\mathfrak{S}}$(the initial state of $\mathfrak{S})\}$.

Next we state the proposition

(16) For every subset Q of $\mathfrak{S}$ holds $w \in$ left-Lang Q iff Q meets w-succ$_{\mathfrak{S}}$(the initial state of $\mathfrak{S}$).

6. Automata

Let us consider E, F. We consider automata over F as extensions of semiautomaton over F as systems

⟨ a carrier, a transition, an initial state, final states ⟩,

where the carrier is a set, the transition is a relation between the carrier$\times F$ and the carrier, the initial state is a subset of the carrier, and the final states constitute a subset of the carrier.

Let us consider E, F and let $\mathfrak{A}$ be an automaton over F. We say that $\mathfrak{A}$ is deterministic if and only if:

(Def. 5) The semiautomaton of $\mathfrak{A}$ is deterministic.

Let us consider E, F. Observe that there exists an automaton over F which is strict, non empty, finite, and deterministic.

In the sequel $\mathfrak{A}$ denotes a non empty automaton over F and p, q denote elements of $\mathfrak{A}$.

Let us consider E, F, $\mathfrak{A}$. One can check that the transition-system of $\mathfrak{A}$ is non empty and the semiautomaton of $\mathfrak{A}$ is non empty.

Let us consider E, F, $\mathfrak{A}$. The functor $\mathrm{bool}\,\mathfrak{A}$ yields a strict automaton over $\mathrm{Lex}\,E$ and is defined by the conditions (Def. 6).

(Def. 6)(i) The semiautomaton of $\mathrm{bool}\,\mathfrak{A} = \mathrm{bool}\,$(the semiautomaton of $\mathfrak{A}$), and

(ii) the final states of $\mathrm{bool}\,\mathfrak{A} = \{Q; Q$ ranges over elements of $\mathrm{bool}\,\mathfrak{A} : Q$ meets the final states of $\mathfrak{A}\}$.

Let us consider E, F, $\mathfrak{A}$. One can check that $\mathrm{bool}\,\mathfrak{A}$ is non empty and deterministic.

The following proposition is true

(17) The carrier of $\mathrm{bool}\,\mathfrak{A} = 2^{\text{the carrier of } \mathfrak{A}}$.

Let us consider E, F and let $\mathfrak{A}$ be a finite non empty automaton over F. Note that $\mathrm{bool}\,\mathfrak{A}$ is finite.

7. Right-languages

Let us consider E, F, $\mathfrak{A}$ and let Q be a subset of $\mathfrak{A}$. The functor right-Lang Q yields a subset of E^{ω} and is defined as follows:

(Def. 7) right-Lang $Q = \{w : w\text{-succ}_{\mathfrak{A}}(Q)$ meets the final states of $\mathfrak{A}\}$.

The following proposition is true

(18) For every subset Q of $\mathfrak{A}$ holds $w \in$ right-Lang Q iff w-$\mathrm{succ}_{\mathfrak{A}}(Q)$ meets the final states of $\mathfrak{A}$.

8. Languages Accepted by Automata

Let us consider E, F, $\mathfrak{A}$. The language generated by $\mathfrak{A}$ yielding a subset of E^{ω} is defined by the condition (Def. 8).

(Def. 8) The language generated by $\mathfrak{A} = \{u : \bigvee_{p,q} (p \in$ the initial state of $\mathfrak{A} \wedge q \in$ the final states of $\mathfrak{A}\ \wedge\ p, u \Rightarrow^{*}_{\mathfrak{A}} q)\}$.

The following propositions are true:

(19) $w \in$ the language generated by $\mathfrak{A}$ if and only if there exist p, q such that $p \in$ the initial state of $\mathfrak{A}$ and $q \in$ the final states of $\mathfrak{A}$ and $p, w \Rightarrow^{*}_{\mathfrak{A}} q$.

(20) $w \in$ the language generated by $\mathfrak{A}$ if and only if w-succ$_{\mathfrak{A}}$(the initial state of $\mathfrak{A}$) meets the final states of $\mathfrak{A}$.

(21) The language generated by $\mathfrak{A}$ = left-Lang (the final states of $\mathfrak{A}$).

(22) The language generated by $\mathfrak{A}$ = right-Lang (the initial state of $\mathfrak{A}$).

9. Equivalence of Deterministic and Nondeterministic Epsilon Automata

In the sequel $\mathfrak{T}$ denotes a non empty transition-system over $\mathrm{Lex}\, E \cup \{\langle\rangle_E\}$.

One can prove the following three propositions:

(23) For every reduction sequence R w.r.t. $\Rightarrow_{\mathfrak{T}}$ such that $R(1)_{\mathbf{2}} = \langle e\rangle \frown u$ and $R(\mathrm{len}\, R)_{\mathbf{2}} = \langle\rangle_E$ holds $R(2)_{\mathbf{2}} = \langle e\rangle \frown u$ or $R(2)_{\mathbf{2}} = u$.

(24) For every reduction sequence R w.r.t. $\Rightarrow_{\mathfrak{T}}$ such that $R(1)_{\mathbf{2}} = u$ and $R(\mathrm{len}\, R)_{\mathbf{2}} = \langle\rangle_E$ holds $\mathrm{len}\, R > \mathrm{len}\, u$.

(25) For every reduction sequence R w.r.t. $\Rightarrow_{\mathfrak{T}}$ such that $R(1)_{\mathbf{2}} = u \frown v$ and $R(\mathrm{len}\, R)_{\mathbf{2}} = \langle\rangle_E$ there exists l such that $l \in \mathrm{dom}\, R$ and $R(l)_{\mathbf{2}} = v$.

Let us consider E, u, v. The functor chop(u, v) yielding an element of E^{ω} is defined by:

(Def. 9)(i) For every w such that $w \frown v = u$ holds chop$(u, v) = w$ if there exists w such that $w \frown v = u$,

(ii) chop$(u, v) = u$, otherwise.

The following propositions are true:

(26) Let p be a reduction sequence w.r.t. $\Rightarrow_{\mathfrak{T}}$. Suppose $p(1) = \langle x,\ u \frown w\rangle$ and $p(\mathrm{len}\, p) = \langle y,\ v \frown w\rangle$. Then there exists a reduction sequence q w.r.t. $\Rightarrow_{\mathfrak{T}}$ such that $q(1) = \langle x,\ u\rangle$ and $q(\mathrm{len}\, q) = \langle y,\ v\rangle$.

(27) If $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x,\ u \frown w\rangle$ to $\langle y,\ v \frown w\rangle$, then $\Rightarrow_{\mathfrak{T}}$ reduces $\langle x,\ u\rangle$ to $\langle y,\ v\rangle$.

(28) If $x, u \frown w \Rightarrow^{*}_{\mathfrak{T}} y, v \frown w$, then $x, u \Rightarrow^{*}_{\mathfrak{T}} y, v$.

(29) For all elements p, q of $\mathfrak{T}$ such that $p, u \frown v \Rightarrow^{*}_{\mathfrak{T}} q$ there exists an element r of $\mathfrak{T}$ such that $p, u \Rightarrow^{*}_{\mathfrak{T}} r$ and $r, v \Rightarrow^{*}_{\mathfrak{T}} q$.

(30) $w \frown v\text{-succ}_{\mathfrak{T}}(X) = v\text{-succ}_{\mathfrak{T}}(w\text{-succ}_{\mathfrak{T}}(X))$.

(31) bool $\mathfrak{T}$ is a non empty transition-system over Lex $E \cup \{\langle\rangle_E\}$.

(32) $w\text{-succ}_{\text{bool}\,\mathfrak{T}}(\{v\text{-succ}_{\mathfrak{T}}(X)\}) = \{v \frown w\text{-succ}_{\mathfrak{T}}(X)\}$.

In the sequel $\mathfrak{S}$ denotes a non empty semiautomaton over Lex $E \cup \{\langle\rangle_E\}$.

One can prove the following proposition

(33) $w\text{-succ}_{\text{bool}\,\mathfrak{S}}(\{\langle\rangle_E\text{-succ}_{\mathfrak{S}}(X)\}) = \{w\text{-succ}_{\mathfrak{S}}(X)\}$.

In the sequel $\mathfrak{A}$ denotes a non empty automaton over Lex $E \cup \{\langle\rangle_E\}$ and P denotes a subset of $\mathfrak{A}$.

Next we state several propositions:

(34) If $x \in$ the final states of $\mathfrak{A}$ and $x \in P$, then $P \in$ the final states of bool $\mathfrak{A}$.

(35) If $X \in$ the final states of bool $\mathfrak{A}$, then X meets the final states of $\mathfrak{A}$.

(36) The initial state of bool $\mathfrak{A} = \{\langle\rangle_E\text{-succ}_{\mathfrak{A}}(\text{the initial state of } \mathfrak{A})\}$.

(37) $w\text{-succ}_{\text{bool}\,\mathfrak{A}}(\{\langle\rangle_E\text{-succ}_{\mathfrak{A}}(X)\}) = \{w\text{-succ}_{\mathfrak{A}}(X)\}$.

(38) $w\text{-succ}_{\text{bool}\,\mathfrak{A}}(\text{the initial state of bool}\,\mathfrak{A}) = \{w\text{-succ}_{\mathfrak{A}}(\text{the initial state of } \mathfrak{A})\}$.

(39) The language generated by $\mathfrak{A} =$ the language generated by bool $\mathfrak{A}$.

(40) Let $\mathfrak{A}$ be a non empty automaton over Lex $E \cup \{\langle\rangle_E\}$. Then there exists a non empty deterministic automaton $\mathfrak{A}_1$ over Lex E such that the language generated by $\mathfrak{A} =$ the language generated by $\mathfrak{A}_1$.

(41) Let $\mathfrak{F}$ be a non empty finite automaton over Lex $E \cup \{\langle\rangle_E\}$. Then there exists a non empty deterministic finite automaton $\mathfrak{A}_2$ over Lex E such that the language generated by $\mathfrak{F} =$ the language generated by $\mathfrak{A}_2$.

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. Reduction relations. *Formalized Mathematics*, 5(**4**):469–478, 1996.

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

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

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

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

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

[10] Karol Pąk. The Catalan numbers. Part II. *Formalized Mathematics*, 14(**4**):153–159, 2006, doi:10.2478/v10037-006-0019-7.

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

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

[13] Michał Trybulec. Formal languages – concatenation and closure. *Formalized Mathematics*, 15(**1**):11–15, 2007, doi:10.2478/v10037-007-0002-y.

[14] Michał Trybulec. Labelled state transition systems. *Formalized Mathematics*, 17(**2**):163–171, 2009, doi: 10.2478/v10037-009-0019-5.

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

[16] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.

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

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

Received May 25, 2009