Contents

Formaliz. Math. 25 (**3**)

FORMALIZED MATHEMATICS
Vol. 25, No. 3, Pages 171–178, 2017
DOI: 10.1515/forma-2017-0016

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

Isomorphism Theorem on Vector Spaces over a Ring[1]

Yuichi Futa
Tokyo University of Technology
Tokyo, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize in the Mizar system [1, 4] some properties of vector spaces over a ring. We formally prove the first isomorphism theorem of vector spaces over a ring. We also formalize the product space of vector spaces. $\mathbb{Z}$-modules are useful for lattice problems such as LLL (Lenstra, Lenstra and Lovász) [5] base reduction algorithm and cryptographic systems [6, 2].

MSC: 15A03 15A04 03B35

Keywords: isomorphism theorem; vector space

MML identifier: VECTSP12, version: 8.1.06 5.44.1305

1. Bijective Linear Transformation

From now on K, F denote rings, V, W denote vector spaces over K, l denotes a linear combination of V, and T denotes a linear transformation from V to W.

Now we state the propositions:

(1) Let us consider a field K, finite dimensional vector spaces V, W over K, a subset A of V, a basis B of V, a linear transformation T from V to W, and a linear combination l of $B \setminus A$. Suppose A is a basis of $\ker T$ and $A \subseteq B$. Then $T(\sum l) = \sum (T \mathbin{@*} l)$.

(2) Let us consider a field F, vector spaces X, Y over F, a linear transformation T from X to Y, and a subset A of X. Suppose T is bijective. Then A is a basis of X if and only if $T^\circ A$ is a basis of Y.

[1]This work was supported by JSPS KAKENHI grant number JP15K00183.

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

(3) Let us consider a field F, vector spaces X, Y over F, and a linear transformation T from X to Y. Suppose T is bijective. Then X is finite dimensional if and only if Y is finite dimensional.

(4) Let us consider a field F, a finite dimensional vector space X over F, a vector space Y over F, and a linear transformation T from X to Y. Suppose T is bijective. Then

(i) Y is finite dimensional, and

(ii) $\dim(X) = \dim(Y)$.

PROOF: For every basis I of X, $\dim(Y) = \overline{\overline{I}}$. □

(5) Let us consider a field F, vector spaces X, Y over F, a linear combination l of X, and a linear transformation T from X to Y. If T is one-to-one, then $T\,^{@}\,l = T\,@{*}\,l$.

PROOF: For every element y of Y, $(T\,^{@}\,l)(y) = \sum \mathrm{CFS}(l, T, y)$. □

2. Properties of Linear Combinations of Modules over a Ring

Now we state the proposition:

(6) Let us consider a field K, a vector space V over K, subspaces W_1, W_2 of V, a basis I_1 of W_1, and a basis I_2 of W_2. If V is the direct sum of W_1 and W_2, then $I_1 \cap I_2 = \emptyset$.

Let us consider a field K, a vector space V over K, subspaces W_1, W_2 of V, a basis I_1 of W_1, a basis I_2 of W_2, and a subset I of V. Now we state the propositions:

(7) Suppose V is the direct sum of W_1 and W_2 and $I = I_1 \cup I_2$. Then $\mathrm{Lin}(I) =$ the vector space structure of V.

PROOF: Reconsider $I_3 = I_1$ as a subset of V. Reconsider $I_4 = I_2$ as a subset of V. For every vector x of V, $x \in W_1 + W_2$ iff $x \in \mathrm{Lin}(I_3) + \mathrm{Lin}(I_4)$. □

(8) If V is the direct sum of W_1 and W_2 and $I = I_1 \cup I_2$, then I is linearly independent.

PROOF: Consider l being a linear combination of I such that $\sum l = 0_V$ and the support of $l \neq \emptyset$. $I_1 \cap I_2 = \emptyset$. I_1 misses I_2. Reconsider $I_3 = I_1$, $I_4 = I_2$ as a subset of V. Consider l_1 being a linear combination of I_3, l_2 being a linear combination of I_4 such that $l = l_1 + l_2$. Reconsider $l_3 = l_1$ as a linear combination of I. Set $v_1 = \sum l_3$. $v_1 \neq 0_V$ by [3, (25)]. □

(9) Let us consider a field K, a vector space V over K, subspaces W_1, W_2 of V, a basis I_1 of W_1, and a basis I_2 of W_2. If $W_1 \cap W_2 = \mathbf{0}_V$, then $I_1 \cup I_2$ is a basis of $W_1 + W_2$.

Proof: Set $I = I_1 \cup I_2$. Reconsider $W = W_1 + W_2$ as a strict subspace of V. Reconsider $W_3 = W_1$, $W_4 = W_2$ as a subspace of W. Reconsider $I_0 = I$ as a subset of W. For every object x, $x \in W_3 \cap W_4$ iff $x \in \mathbf{0}_V$. For every object x, $x \in W$ iff $x \in W_3 + W_4$. I_0 is base. □

3. First Isomophism Theorem

Let us consider a field K, a finite dimensional vector space V over K, and a subspace W of V. Now we state the propositions:

(10) There exists a linear complement S of W and there exists a linear transformation T from S to ${}^{V}/_{W}$ such that T is bijective and for every vector v of V such that $v \in S$ holds $T(v) = v + W$.

Proof: Set $S =$ the linear complement of W. Set $V_1 = {}^{V}/_{W}$. Define $\mathcal{P}[\text{vector of } V, \text{vector of } V_1] \equiv \$_2 = \$_1 + W$. Consider f_1 being a function from the carrier of V into the carrier of V_1 such that for every vector v of V, $\mathcal{P}[v, f_1(v)]$. Set $T = f_1 \restriction$(the carrier of S). For every vector v of V such that $v \in S$ holds $T(v) = v + W$. The carrier of $V_1 \subseteq \operatorname{rng} T$. For every objects x_1, x_2 such that x_1, $x_2 \in$ the carrier of S and $T(x_1) = T(x_2)$ holds $x_1 = x_2$. □

(11) (i) ${}^{V}/_{W}$ is finite dimensional, and

(ii) $\dim({}^{V}/_{W}) + \dim(W) = \dim(V)$.

The theorem is a consequence of (10) and (4).

Let K be a ring, V, U be vector spaces over K, W be a subspace of V, and f be a linear transformation from V to U. Assume the carrier of $W \subseteq$ the carrier of $\ker f$. The functor ${}^{f}/_{W}$ yielding a linear transformation from ${}^{V}/_{W}$ to U is defined by

(Def. 1) for every vector A of ${}^{V}/_{W}$ and for every vector a of V such that $A = a + W$ holds $it(A) = f(a)$.

The functor CQFunctional f yielding a linear transformation from ${}^{V}/_{\ker f}$ to U is defined by the term

(Def. 2) ${}^{f}/_{\ker f}$.

Observe that CQFunctional f is one-to-one.

Now we state the proposition:

(12) Let us consider a ring K, vector spaces V, U over K, and a linear transformation f from V to U. Then there exists a linear transformation T from ${}^{V}/_{\ker f}$ to $\operatorname{im} f$ such that

(i) $T =$ CQFunctional f, and

(ii) T is bijective.

PROOF: Set $T = \mathrm{CQFunctional}\, f$. For every object x, $x \in \mathrm{rng}\, T$ iff $x \in \mathrm{rng}\, f$. $\square$

Let K be a ring, V, U, W be vector spaces over K, f be a linear transformation from V to U, and g be a linear transformation from U to W. One can verify that the functor $g \cdot f$ yields a linear transformation from V to W.

4. The Product Space of Vector Spaces

Let K be a ring.

A sequence of vector spaces over K is a non empty finite sequence and is defined by

(Def. 3) for every set S such that $S \in \mathrm{rng}\, it$ holds S is a vector space over K.

Note that every sequence of vector spaces over K is Abelian group yielding.

Let G be a sequence of vector spaces over K and j be an element of $\mathrm{dom}\, G$. One can check that the functor $G(j)$ yields a vector space over K. Let j be an element of $\mathrm{dom}\, \overline{G}$. One can verify that the functor $G(j)$ yields a vector space over K. The functor $\mathrm{multop}\, G$ yielding a multi-operation of the carrier of K and $\overline{G}$ is defined by

(Def. 4) $\mathrm{len}\, it = \mathrm{len}\, \overline{G}$ and for every element j of $\mathrm{dom}\, \overline{G}$, $it(j) =$ the left multiplication of $G(j)$.

The functor $\prod G$ yielding a strict, non empty vector space structure over K is defined by the term

(Def. 5) $\langle \prod \overline{G}, \prod^{\circ} \langle +_{G_i} \rangle_i, \langle 0_{G_i} \rangle_i, \prod^{\circ} \mathrm{multop}\, G \rangle$.

Let us note that $\prod G$ is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

5. Cartesian Product of Vector Spaces

From now on K denotes a ring.

Let K be a ring and G, F be non empty vector space structures over K. The functor $\mathrm{prodmlt}(G, F)$ yielding a function from (the carrier of K) $\times$ ((the carrier of G) $\times$ (the carrier of F)) into (the carrier of G) $\times$ (the carrier of F) is defined by

(Def. 6) for every element r of K and for every vector g of G and for every vector f of F, $it(r, \langle g, f \rangle) = \langle r \cdot g, r \cdot f \rangle$.

The functor $G \times F$ yielding a strict, non empty vector space structure over K is defined by the term

(Def. 7) $\langle$(the carrier of G) $\times$ (the carrier of F), prodadd(G, F), prodzero(G, F), prodmlt$(G, F)\rangle$.

Let G, F be Abelian, non empty vector space structures over K. Note that $G \times F$ is Abelian.

Let G, F be add-associative, non empty vector space structures over K. One can verify that $G \times F$ is add-associative.

Let G, F be right zeroed, non empty vector space structures over K. One can verify that $G \times F$ is right zeroed.

Let G, F be right complementable, non empty vector space structures over K. One can check that $G \times F$ is right complementable.

Now we state the propositions:

(13) Let us consider non empty vector space structures G, F over K. Then

(i) for every set x, x is a vector of $G \times F$ iff there exists a vector x_1 of G and there exists a vector x_2 of F such that $x = \langle x_1, x_2 \rangle$, and

(ii) for every vectors x, y of $G \times F$ and for every vectors x_1, y_1 of G and for every vectors x_2, y_2 of F such that $x = \langle x_1, x_2 \rangle$ and $y = \langle y_1, y_2 \rangle$ holds $x + y = \langle x_1 + y_1, x_2 + y_2 \rangle$, and

(iii) $0_{G \times F} = \langle 0_G, 0_F \rangle$, and

(iv) for every vector x of $G \times F$ and for every vector x_1 of G and for every vector x_2 of F and for every element a of K such that $x = \langle x_1, x_2 \rangle$ holds $a \cdot x = \langle a \cdot x_1, a \cdot x_2 \rangle$.

(14) Let us consider add-associative, right zeroed, right complementable, non empty vector space structures G, F over K, a vector x of $G \times F$, a vector x_1 of G, and a vector x_2 of F. Suppose $x = \langle x_1, x_2 \rangle$. Then $-x = \langle -x_1, -x_2 \rangle$.

Let K be a ring and G, F be vector distributive, non empty vector space structures over K. Let us note that $G \times F$ is vector distributive.

Let G, F be scalar distributive, non empty vector space structures over K. One can check that $G \times F$ is scalar distributive.

Let G, F be scalar associative, non empty vector space structures over K. Let us note that $G \times F$ is scalar associative.

Let G, F be scalar unital, non empty vector space structures over K. Let us observe that $G \times F$ is scalar unital.

Let G be a vector space over K. One can check that the functor $\langle G \rangle$ yields a sequence of vector spaces over K. Let G, F be vector spaces over K. Let us note that the functor $\langle G, F \rangle$ yields a sequence of vector spaces over K. Now we state the proposition:

(15) Let us consider a vector space X over K. Then there exists a function I from X into $\prod\langle X\rangle$ such that

(i) I is one-to-one and onto, and

(ii) for every vector x of X, $I(x) = \langle x\rangle$, and

(iii) for every vectors v, w of X, $I(v + w) = I(v) + I(w)$, and

(iv) for every vector v of X and for every element r of the carrier of K, $I(r \cdot v) = r \cdot I(v)$, and

(v) $I(0_X) = 0_{\prod\langle X\rangle}$.

Proof: Set C_3 = the carrier of X. Consider I being a function from C_3 into $\prod\langle C_3\rangle$ such that I is one-to-one and onto and for every object x such that $x \in C_3$ holds $I(x) = \langle x\rangle$. For every vectors v, w of X, $I(v + w) = I(v) + I(w)$. For every vector v of X and for every element r of the carrier of K, $I(r \cdot v) = r \cdot I(v)$. □

Let K be a ring and G, F be sequences of vector spaces over K. One can verify that the functor $G \frown F$ yields a sequence of vector spaces over K. Now we state the propositions:

(16) Let us consider vector spaces X, Y over K. Then there exists a function I from $X \times Y$ into $\prod\langle X, Y\rangle$ such that

(i) I is one-to-one and onto, and

(ii) for every vector x of X and for every vector y of Y, $I(x, y) = \langle x, y\rangle$, and

(iii) for every vectors v, w of $X \times Y$, $I(v + w) = I(v) + I(w)$, and

(iv) for every vector v of $X \times Y$ and for every element r of K, $I(r \cdot v) = r \cdot I(v)$, and

(v) $I(0_{X\times Y}) = 0_{\prod\langle X,Y\rangle}$.

Proof: Set C_3 = the carrier of X. Set C_4 = the carrier of Y. Consider I being a function from $C_3 \times C_4$ into $\prod\langle C_3, C_4\rangle$ such that I is one-to-one and onto and for every objects x, y such that $x \in C_3$ and $y \in C_4$ holds $I(x, y) = \langle x, y\rangle$. For every vectors v, w of $X \times Y$, $I(v + w) = I(v) + I(w)$. For every vector v of $X \times Y$ and for every element r of K, $I(r \cdot v) = r \cdot I(v)$. □

(17) Let us consider sequences of vector spaces X, Y over K. Then there exists a function I from $\prod X \times \prod Y$ into $\prod(X \frown Y)$ such that

(i) I is one-to-one and onto, and

(ii) for every vector x of $\prod X$ and for every vector y of $\prod Y$, there exist finite sequences x_1, y_1 such that $x = x_1$ and $y = y_1$ and $I(x, y) = x_1 \frown y_1$, and

(iii) for every vectors v, w of $\prod X \times \prod Y$, $I(v + w) = I(v) + I(w)$, and

(iv) for every vector v of $\prod X \times \prod Y$ and for every element r of the carrier of K, $I(r \cdot v) = r \cdot I(v)$, and

(v) $I(0_{\prod X \times \prod Y}) = 0_{\prod(X \frown Y)}$.

PROOF: Reconsider $C_1 = \overline{X}$, $C_2 = \overline{Y}$ as a non-empty, non empty finite sequence. Consider I being a function from $\prod C_1 \times \prod C_2$ into $\prod(C_1 \frown C_2)$ such that I is one-to-one and onto and for every finite sequences x, y such that $x \in \prod C_1$ and $y \in \prod C_2$ holds $I(x, y) = x \frown y$. Set $P_1 = \prod X$. Set $P_2 = \prod Y$. For every natural number k such that $k \in \operatorname{dom} \overline{X \frown Y}$ holds $\overline{X \frown Y}(k) = (C_1 \frown C_2)(k)$. For every vector x of $\prod X$ and for every vector y of $\prod Y$, there exist finite sequences x_1, y_1 such that $x = x_1$ and $y = y_1$ and $I(x, y) = x_1 \frown y_1$. For every vectors v, w of $P_1 \times P_2$, $I(v+w) = I(v)+I(w)$. For every vector v of $P_1 \times P_2$ and for every element r of the carrier of K, $I(r \cdot v) = r \cdot I(v)$ by [7, (9)]. □

(18) Let us consider vector spaces G, F over K. Then

(i) for every set x, x is a vector of $\prod\langle G, F\rangle$ iff there exists a vector x_1 of G and there exists a vector x_2 of F such that $x = \langle x_1, x_2\rangle$, and

(ii) for every vectors x, y of $\prod\langle G, F\rangle$ and for every vectors x_1, y_1 of G and for every vectors x_2, y_2 of F such that $x = \langle x_1, x_2\rangle$ and $y = \langle y_1, y_2\rangle$ holds $x + y = \langle x_1 + y_1, x_2 + y_2\rangle$, and

(iii) $0_{\prod\langle G,F\rangle} = \langle 0_G, 0_F\rangle$, and

(iv) for every vector x of $\prod\langle G, F\rangle$ and for every vector x_1 of G and for every vector x_2 of F such that $x = \langle x_1, x_2\rangle$ holds $-x = \langle -x_1, -x_2\rangle$, and

(v) for every vector x of $\prod\langle G, F\rangle$ and for every vector x_1 of G and for every vector x_2 of F and for every element a of K such that $x = \langle x_1, x_2\rangle$ holds $a \cdot x = \langle a \cdot x_1, a \cdot x_2\rangle$.

PROOF: Consider I being a function from $G \times F$ into $\prod\langle G, F\rangle$ such that I is one-to-one and onto and for every vector x of G and for every vector y of F, $I(x, y) = \langle x, y\rangle$ and for every vectors v, w of $G \times F$, $I(v+w) = I(v)+I(w)$ and for every vector v of $G \times F$ and for every element r of K, $I(r \cdot v) = r \cdot I(v)$ and $0_{\prod\langle G,F\rangle} = I(0_{G \times F})$. For every set x, x is a vector of $\prod\langle G, F\rangle$ iff there exists a vector x_1 of G and there exists a vector x_2 of F such that $x = \langle x_1, x_2\rangle$. For every vectors x, y of $\prod\langle G, F\rangle$ and for every vectors x_1, y_1 of G and for every vectors x_2, y_2 of F such that $x = \langle x_1, x_2\rangle$ and $y = \langle y_1, y_2\rangle$ holds $x + y = \langle x_1 + y_1, x_2 + y_2\rangle$. $0_{\prod\langle G,F\rangle} = \langle 0_G, 0_F\rangle$. For every vector x of $\prod\langle G, F\rangle$ and for every vector x_1 of G and for every vector x_2 of F such that $x = \langle x_1, x_2 \rangle$ holds $-x = \langle -x_1, -x_2 \rangle$. For every vector x of $\prod\langle G, F\rangle$ and for every vector x_1 of G and for every vector x_2 of F and for every element a of K such that $x = \langle x_1, x_2 \rangle$ holds $a \cdot x = \langle a \cdot x_1, a \cdot x_2 \rangle$. $\square$

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] Wolfgang Ebeling. *Lattices and Codes*. Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.

[3] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Submodule of free ℤ-module. *Formalized Mathematics*, 21(**4**):273–282, 2013. doi:10.2478/forma-2013-0029.

[4] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[5] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982. doi:10.1007/BF01457454.

[6] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: a cryptographic perspective. *The International Series in Engineering and Computer Science*, 2002.

[7] Yasunari Shidama. Differentiable functions on normed linear spaces. *Formalized Mathematics*, 20(**1**):31–40, 2012. doi:10.2478/v10037-012-0005-1.

Received August 30, 2017

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 25, No. 3, Pages 179–184, 2017
DOI: 10.1515/forma-2017-0017

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

F. Riesz Theorem

Keiko Narita
Hirosaki-city
Aomori, Japan

Kazuhisa Nakasho
Akita Prefectural University
Akita, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize in the Mizar system [1, 4] the F. Riesz theorem. In the first section, we defined Mizar functor `ClstoCmp`, compact topological spaces as closed interval subset of real numbers. Then using the former definition and referring to the article [10] and the article [5], we defined the normed spaces of continuous functions on closed interval subset of real numbers, and defined the normed spaces of bounded functions on closed interval subset of real numbers. We also proved some related properties.

In Sec.2, we proved some lemmas for the proof of F. Riesz theorem. In Sec.3, we proved F. Riesz theorem, about the dual space of the space of continuous functions on closed interval subset of real numbers, finally. We applied Hahn-Banach theorem (36) in [7], to the proof of the last theorem. For the description of theorems of this section, we also referred to the article [8] and the article [6]. These formalizations are based on [2], [3], [9], and [11].

MSC: 46E15 46B10 03B35

Keywords: F. Riesz theorem; dual spaces; continuous functions

MML identifier: `DUALSP05`, version: `8.1.06 5.44.1305`

1. The Normed Space of Continuous Functions on Closed Interval

Now we state the propositions:

(1) Let us consider a real number d. Then $|\operatorname{sgn} d| \leqslant 1$.

(2) Let us consider a real number x. Then $|x| = \operatorname{sgn} x \cdot x$.

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

Let A be a non empty, closed interval subset of $\mathbb{R}$. The functor Cls2Cmp(A) yielding a strict, compact, non empty topological space is defined by

(Def. 1) there exist real numbers a, b such that $a \leqslant b$ and $[a, b] = A$ and $it = [a, b]_{\mathrm{T}}$.

Now we state the propositions:

(3) Let us consider a strict, non empty subspace X of $\mathbb{R}^{\mathbf{1}}$, a real map f of X, a partial function g from $\mathbb{R}$ to $\mathbb{R}$, a point x of X, and a real number x_0. Suppose $g = f$ and $x = x_0$. Then for every subset V of $\mathbb{R}$ such that $f(x) \in V$ and V is open there exists a subset W of X such that $x \in W$ and W is open and $f^{\circ}W \subseteq V$ if and only if g is continuous in x_0.

(4) Let us consider a strict, non empty subspace X of $\mathbb{R}^{\mathbf{1}}$, a real map f of X, and a partial function g from $\mathbb{R}$ to $\mathbb{R}$. If $g = f$, then f is continuous iff g is continuous. The theorem is a consequence of (3).

(5) Let us consider a non empty, closed interval subset A of $\mathbb{R}$. Then the carrier of Cls2Cmp(A) $= A$.

(6) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, and a function u. Then u is a point of C(Cls2Cmp(A); $\mathbb{R}$) if and only if $\operatorname{dom} u = A$ and u is a continuous partial function from $\mathbb{R}$ to $\mathbb{R}$. The theorem is a consequence of (5) and (4).

(7) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, and a point v of C(Cls2Cmp(A); $\mathbb{R}$). Then $v \in$ BoundedFunctions(the carrier of Cls2Cmp(A)).

2. Preliminaries

Now we state the proposition:

(8) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, and real numbers a, b. Suppose $A = [a, b]$. Then there exists a function x from A into BoundedFunctions A such that for every real number s such that $s \in [a, b]$ holds if $s = a$, then $x(s) = [a, b] \longmapsto 0$ and if $s \neq a$, then $x(s) = ([a, s] \longmapsto 1) + \cdot (]s, b] \longmapsto 0)$.

Proof: Define $\mathcal{C}[\text{object}] \equiv \$_1 = a$. Define $\mathcal{F}(\text{object}) = [a, b] \longmapsto 0$. Define $\mathcal{G}(\text{object}) = ([a, \$_1(\in \mathbb{R})] \longmapsto 1) + \cdot (]\$_1(\in \mathbb{R}), b] \longmapsto 0)$. Set $B =$ BoundedFunctions A. For every object s such that $s \in [a, b]$ holds if $\mathcal{C}[s]$, then $\mathcal{F}(s) \in B$ and if $\mathcal{C}[s]$, then $\mathcal{G}(s) \in B$. Consider x being a function from $[a, b]$ into B such that for every object s such that $s \in [a, b]$ holds if $\mathcal{C}[s]$, then $x(s) = \mathcal{F}(s)$ and if $\mathcal{C}[s]$, then $x(s) = \mathcal{G}(s)$. For every real number s such that $s \in [a, b]$ holds if $s = a$, then $x(s) = [a, b] \longmapsto 0$ and if $s \neq a$, then $x(s) = ([a, s] \longmapsto 1) + \cdot (]s, b] \longmapsto 0)$. $\square$

Let A be a non empty, closed interval subset of $\mathbb{R}$, D be a partition of A, m be a function from A into BoundedFunctions A, and i be a natural number. Assume $i \in \mathrm{Seg}(\mathrm{len}\, D + 1)$. The functor $\mathrm{Dp1}(m, D, i)$ yielding a point of the $\mathbb{R}$-normed algebra of bounded functions on the carrier of Cls2Cmp(A) is defined by the term

(Def. 2) $\begin{cases} m(\inf A), & \textbf{if } i = 1, \\ m(D(i-1)), & \textbf{otherwise}. \end{cases}$

Let ϱ be a function from A into $\mathbb{R}$. The functor $\mathrm{Dp2}(\varrho, D, i)$ yielding a real number is defined by the term

(Def. 3) $\begin{cases} \varrho(\inf A), & \textbf{if } i = 1, \\ \varrho(D(i-1)), & \textbf{otherwise}. \end{cases}$

Now we state the propositions:

(9) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, a partition D of A, a function m from A into BoundedFunctions A, and a function ϱ from A into $\mathbb{R}$. Then there exists a finite sequence s of elements of the $\mathbb{R}$-normed algebra of bounded functions on the carrier of Cls2Cmp(A) such that

(i) $\mathrm{len}\, s = \mathrm{len}\, D$, and

(ii) for every natural number i such that $i \in \mathrm{dom}\, s$ holds $s(i) = \mathrm{sgn}(\mathrm{Dp2}(\varrho, D, i+1) - \mathrm{Dp2}(\varrho, D, i)) \cdot (\mathrm{Dp1}(m, D, i+1) - \mathrm{Dp1}(m, D, i))$.

Proof: Set $V =$ the $\mathbb{R}$-normed algebra of bounded functions on the carrier of Cls2Cmp(A). Define $\mathcal{P}[\text{natural number}, \text{set}] \equiv \$_2 = \mathrm{sgn}(\mathrm{Dp2}(\varrho, D, \$_1 + 1) - \mathrm{Dp2}(\varrho, D, \$_1)) \cdot (\mathrm{Dp1}(m, D, \$_1 + 1) - \mathrm{Dp1}(m, D, \$_1))$. Consider s being a finite sequence of elements of V such that $\mathrm{dom}\, s = \mathrm{Seg}\,\mathrm{len}\, D$ and for every natural number i such that $i \in \mathrm{Seg}\,\mathrm{len}\, D$ holds $\mathcal{P}[i, s(i)]$. $\square$

(10) Let us consider a real linear space V, a functional f in V, and a finite sequence s of elements of V. If f is additive, then $f(\sum s) = \sum (f \cdot s)$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every real linear space V for every functional f in V for every finite sequence s of elements of V such that $\mathrm{len}\, s = \$_1$ and f is additive holds $f(\sum s) = \sum (f \cdot s)$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. $\square$

(11) Let us consider a non empty set A. Then every element of the $\mathbb{R}$-normed algebra of bounded functions on A is a function from A into $\mathbb{R}$.

(12) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, a finite sequence s of elements of the $\mathbb{R}$-normed algebra of bounded functions on the carrier of Cls2Cmp(A), a finite sequence z of elements of $\mathbb{R}$, a function g from A into $\mathbb{R}$, and an element t of A. Suppose $\mathrm{len}\, s = \mathrm{len}\, z$ and $g = \sum s$

and for every natural number k such that $k \in \operatorname{dom} z$ there exists a function s_1 from A into $\mathbb{R}$ such that $s_1 = s(k)$ and $z(k) = s_1(t)$. Then $g(t) = \sum z$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non empty, closed interval subset A of $\mathbb{R}$ for every finite sequence s of elements of the $\mathbb{R}$-normed algebra of bounded functions on the carrier of Cls2Cmp(A) for every finite sequence z of elements of $\mathbb{R}$ for every function g from A into $\mathbb{R}$ for every element t of A such that $\operatorname{len} s = \$_1$ and $\operatorname{len} s = \operatorname{len} z$ and $g = \sum s$ and for every natural number k such that $k \in \operatorname{dom} z$ there exists a function s_1 from A into $\mathbb{R}$ such that $s_1 = s(k)$ and $z(k) = s_1(t)$ holds $g(t) = \sum z$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(13) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, a partition D of A, and an element t of A. Suppose $\inf A < D(1)$. Then there exists an element i of $\mathbb{N}$ such that

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

(ii) $t \in \operatorname{divset}(D, i)$, and

(iii) $i = 1$ or $\inf \operatorname{divset}(D, i) < t \leqslant \sup \operatorname{divset}(D, i)$.

(14) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, a function ϱ from A into $\mathbb{R}$, and a real number B. Suppose $0 < \operatorname{vol}(A)$. Suppose for every partition D of A and for every var-volume K of ϱ and D such that $\inf A < D(1)$ holds $\sum K \leqslant B$. Let us consider a partition D of A, and a var-volume K of ϱ and D. Then $\sum K \leqslant B$.

3. F. Riesz Theorem

Now we state the propositions:

(15) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, a function ϱ from A into $\mathbb{R}$, and a point f of DualSp C(Cls2Cmp(A); $\mathbb{R}$). Suppose ϱ is bounded-variation and for every continuous partial function u from $\mathbb{R}$ to $\mathbb{R}$ such that $\operatorname{dom} u = A$ holds $f(u) = \int\limits_{\varrho} u(x)dx$. Then $\|f\| \leqslant \operatorname{TotalVD}(\varrho)$.

PROOF: Set $X = \mathrm{C}(\mathrm{Cls2Cmp(A)}; \mathbb{R})$. For every continuous partial function u from $\mathbb{R}$ to $\mathbb{R}$ such that $u \in$ the carrier of X holds $f(u) = \int\limits_{\varrho} u(x)dx$. For every continuous partial function u from $\mathbb{R}$ to $\mathbb{R}$ and for every point v of X such that $\operatorname{dom} u = A$ and $u = v$ holds $|\int\limits_{\varrho} u(x)dx| \leqslant \|v\| \cdot \operatorname{TotalVD}(\varrho)$.

□

(16) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, and a point x of $\mathrm{DualSp}\,\mathrm{C}(\mathrm{Cls2Cmp(A)};\mathbb{R})$. Suppose $0 < \mathrm{vol}(A)$. Then there exists a function ϱ from A into $\mathbb{R}$ such that

(i) ϱ is bounded-variation, and

(ii) for every continuous partial function u from $\mathbb{R}$ to $\mathbb{R}$ such that $\mathrm{dom}\,u = A$ holds $x(u) = \int\limits_{\varrho} u(x)dx$, and

(iii) $\|x\| = \mathrm{TotalVD}(\varrho)$.

Proof: Set $X = \mathrm{C}(\mathrm{Cls2Cmp(A)};\mathbb{R})$. Set $V =$ the $\mathbb{R}$-normed algebra of bounded functions on the carrier of $\mathrm{Cls2Cmp}(A)$. Set $A_1 =$ the carrier of $\mathrm{Cls2Cmp}(A)$. $A_1 = A$. Reconsider $h = x$ as a Lipschitzian linear functional in X. Consider f being a Lipschitzian linear functional in V, F being a point of $\mathrm{DualSp}\,V$ such that $f = F$ and $f\restriction$(the carrier of X) $= h$ and $\|F\| = \|x\|$. Consider a, b being real numbers such that $a \leqslant b$ and $[a, b] = A$ and $\mathrm{Cls2Cmp}(A) = [a, b]_{\mathrm{T}}$. Consider m being a function from A into BoundedFunctions A such that for every real number s such that $s \in [a, b]$ holds if $s = a$, then $m(s) = [a, b] \longmapsto 0$ and if $s \neq a$, then $m(s) = ([a, s] \longmapsto 1) + \cdot (]s, b] \longmapsto 0)$. The carrier of $V =$ BoundedFunctions A. Reconsider $\varrho = f \cdot m$ as a function from A into $\mathbb{R}$. For every partition D of A and for every var-volume K of ϱ and D such that $a < D(1)$ holds $\sum K \leqslant \|x\|$. For every partition D of A and for every var-volume K of ϱ and D, $\sum K \leqslant \|x\|$. Consider V_1 being a non empty subset of $\mathbb{R}$ such that V_1 is upper bounded and $V_1 = \{r$, where r is a real number : there exists a partition t of A and there exists a var-volume F_0 of ϱ and t such that $r = \sum F_0\}$ and $\mathrm{TotalVD}(\varrho) = \sup V_1$. For every continuous partial function u from $\mathbb{R}$ to $\mathbb{R}$ such that $\mathrm{dom}\,u = A$ holds $x(u) = \int\limits_{\varrho} u(x)dx$. $\|x\| \leqslant \mathrm{TotalVD}(\varrho)$. $\square$

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] Haim Brezis. *Functional Analysis, Sobolev Spaces and Partial Differential Equations.* Springer, 2011.

[3] Peter D. Dax. *Functional Analysis.* Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley Interscience, 2002.

[4] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[5] Katuhiko Kanazashi, Noboru Endou, and Yasunari Shidama. Banach algebra of continuous functionals and the space of real-valued continuous functionals with bounded support. *Formalized Mathematics*, 18(**1**):11–16, 2010. doi:10.2478/v10037-010-0002-1.

[6] Kazuhisa Nakasho, Keiko Narita, and Yasunari Shidama. The basic existence theorem of Riemann-Stieltjes integral. *Formalized Mathematics*, 24(**4**):253–259, 2016. doi:10.1515/forma-2016-0021.

[7] Keiko Narita, Noboru Endou, and Yasunari Shidama. Dual spaces and Hahn-Banach theorem. *Formalized Mathematics*, 22(**1**):69–77, 2014. doi:10.2478/forma-2014-0007.

[8] Keiko Narita, Kazuhisa Nakasho, and Yasunari Shidama. Riemann-Stieltjes integral. *Formalized Mathematics*, 24(**3**):199–204, 2016. doi:10.1515/forma-2016-0016.

[9] Walter Rudin. *Functional Analysis*. New York, McGraw-Hill, 2nd edition, 1991.

[10] Yasunari Shidama, Hikofumi Suzuki, and Noboru Endou. Banach algebra of bounded functionals. *Formalized Mathematics*, 16(**2**):115–122, 2008. doi:10.2478/v10037-008-0017-z.

[11] Kosaku Yoshida. *Functional Analysis*. Springer, 1980.

Received August 30, 2017

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 25, No. 3, Pages 185–195, 2017
DOI: 10.1515/forma-2017-0018

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

On Roots of Polynomials and Algebraically Closed Fields

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. In this article we further extend the algebraic theory of polynomial rings in Mizar [1, 2, 3]. We deal with roots and multiple roots of polynomials and show that both the real numbers and finite domains are not algebraically closed [5, 7]. We also prove the identity theorem for polynomials and that the number of multiple roots is bounded by the polynomial's degree [4, 6].

MSC: 13A05 13B25 03B35

Keywords: commutative algebra; polynomials; algebraic closed fields

MML identifier: RING_5, version: 8.1.06 5.44.1305

1. Preliminaries

From now on n denotes a natural number.

Note that there exists a natural number which is non trivial and non prime.

Now we state the proposition:

(1) Let us consider an even natural number n, and an element x of $\mathbb{R}_{\mathrm{F}}$. Then $x^n \geqslant 0_{\mathbb{R}_{\mathrm{F}}}$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv x^{2 \cdot \$_1} \geqslant 0_{\mathbb{R}_{\mathrm{F}}}$. For every element x of $\mathbb{R}_{\mathrm{F}}$, $x^2 \geqslant 0_{\mathbb{R}_{\mathrm{F}}}$. For every natural number k, $\mathcal{P}[k]$. □

Let us consider a ring R and an element a of R. Now we state the propositions:

(2) $2 \star a = a + a$.

(3) $a^2 = a \cdot a$.

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

Let F be a field and a be an element of F. Note that $\frac{a}{1_F}$ reduces to a.

One can check that $\mathbb{Z}/2$ is non trivial and almost left invertible.

Let n be a non trivial, non prime natural number. Note that $\mathbb{Z}/n$ is non integral domain-like and $\mathbb{Z}/6$ is non degenerated.

2. Some More Properties of Polynomials

Let R be a non degenerated ring. Observe that every non zero polynomial over R is non-zero and every polynomial over R which is monic is also non zero.

Let p be a non zero polynomial over R. One can check that $\deg p$ is natural.

Let R be a ring, p be a zero polynomial over R, and q be a polynomial over R. Let us observe that $p * q$ is zero and $q * p$ is zero.

Let us observe that $p + q$ reduces to q and $q + p$ reduces to q.

Let p be a polynomial over R. One can check that $p * \mathbf{0}.R$ reduces to $\mathbf{0}.R$ and $p * \mathbf{1}.R$ reduces to p and $\mathbf{0}.R * p$ reduces to $\mathbf{0}.R$ and $\mathbf{1}.R * p$ reduces to p.

One can check that $1_R \cdot p$ reduces to p.

Now we state the propositions:

(4) Let us consider an integral domain R, a polynomial p over R, and a non zero element a of R. Then $\deg(a \cdot p) = \deg p$.

(5) Let us consider an integral domain R, a polynomial p over R, and an element a of R. Then $\mathrm{LC}(a \cdot p) = a \cdot \mathrm{LC}\, p$.

(6) Let us consider an integral domain R, and an element a of R. Then $\mathrm{LC}(a \restriction R) = a$. The theorem is a consequence of (5).

(7) Let us consider an integral domain R, a polynomial p over R, and elements v, x of R. Then $\mathrm{eval}(v \cdot p, x) = v \cdot \mathrm{eval}(p, x)$. The theorem is a consequence of (4).

(8) Let us consider a ring R, and elements a, b of R. Then $\mathrm{eval}(a \restriction R, b) = a$.

Let R be an integral domain and p, q be monic polynomials over R. Let us note that $p * q$ is monic.

Let a be an element of R and k be a natural number. One can check that $(\mathrm{rpoly}(1, a))^k$ is non zero and monic.

Now we state the propositions:

(9) Let us consider a non degenerated ring R, an element a of R, and a non zero element k of $\mathbb{N}$. Then $\mathrm{LC}\,\mathrm{rpoly}(k, a) = 1_R$.

(10) Let us consider a non degenerated, well unital, non empty double loop structure R, and an element a of R. Then $\langle -a, 1_R \rangle = \mathrm{rpoly}(1, a)$.

(11) Let us consider an integral domain R, a polynomial p over R, and an element x of R. Then $\mathrm{eval}(p, x) = 0_R$ if and only if $\mathrm{rpoly}(1, x) \mid p$.

(12) Let us consider an integral domain F, polynomials p, q over F, and an element a of F. Suppose $\mathrm{rpoly}(1, a) \mid p * q$. Then

(i) $\mathrm{rpoly}(1, a) \mid p$, or

(ii) $\mathrm{rpoly}(1, a) \mid q$.

The theorem is a consequence of (11).

(13) Let us consider an integral domain R, a polynomial p over R, and a non zero polynomial q over R. If $p \mid q$, then $\deg p \leqslant \deg q$.

(14) Let us consider a non degenerated commutative ring R, a polynomial q over R, a non zero polynomial p over R, and a non zero element b of R. If $q \mid p$, then $q \mid b \cdot p$.

(15) Let us consider a field F, a polynomial q over F, a non zero polynomial p over F, and a non zero element b of F. Then $q \mid p$ if and only if $q \mid b \cdot p$. The theorem is a consequence of (14).

Let us consider an integral domain R, a non zero polynomial p over R, an element a of R, and a non zero element b of R. Now we state the propositions:

(16) $\mathrm{rpoly}(1, a) \mid p$ if and only if $\mathrm{rpoly}(1, a) \mid b \cdot p$. The theorem is a consequence of (11), (7), and (14).

(17) $(\mathrm{rpoly}(1, a))^n \mid p$ if and only if $(\mathrm{rpoly}(1, a))^n \mid b \cdot p$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ if $(\mathrm{rpoly}(1, a))^{\$_1} \mid b \cdot p$, then $(\mathrm{rpoly}(1, a))^{\$_1} \mid p$. For every natural number k, $\mathcal{P}[k]$. □

Let R be an integral domain, p be a non zero polynomial over R, and b be a non zero element of R. Let us note that $b \cdot p$ is non zero.

3. On Roots of Polynomials

Let R be a non degenerated ring. One can check that $\mathbf{1}.R$ and has not roots.

Let a be a non zero element of R. One can verify that $a \restriction R$ and has not roots and every polynomial over R which is non zero and has roots is also non constant and every polynomial over R which and has not roots is also non zero.

Let a be an element of R. One can check that $\mathrm{rpoly}(1, a)$ is non zero and has roots and there exists a polynomial over R which is non zero and has not roots and there exists a polynomial over R which is non zero and has roots.

Let R be an integral domain, p be a polynomial over R with non roots, and a be a non zero element of R. Let us note that $a \cdot p$ and has not roots.

Let p be a polynomial over R with roots and a be an element of R. Note that $a \cdot p$ has roots.

Let R be a non degenerated commutative ring and q be a polynomial over R. One can verify that $p * q$ has roots.

Let R be an integral domain and p, q be polynomials over R with non roots. One can check that $p * q$ and has not roots.

Let R be a non degenerated commutative ring, a be an element of R, and k be a non zero element of $\mathbb{N}$. Let us note that $\mathrm{rpoly}(k, a)$ is non constant and monic and has roots.

Let R be a non degenerated ring. Let us observe that there exists a polynomial over R which is non constant and monic.

Let R be an integral domain, a be an element of R, k be a non zero natural number, and n be a non zero element of $\mathbb{N}$. Note that $(\mathrm{rpoly}(n, a))^k$ is non constant and monic and has roots.

Let R be a ring and p be a polynomial over R with roots. Note that $\mathrm{Roots}(p)$ is non empty.

Let R be a non degenerated ring and p be a polynomial over R with non roots. Let us observe that $\mathrm{Roots}(p)$ is empty.

Let R be an integral domain. One can check that there exists a polynomial over R which is monic and has roots and there exists a polynomial over R which is monic and has not roots.

Now we state the propositions:

(18) Let us consider a non degenerated ring R, and an element a of R. Then $\mathrm{Roots}(\mathrm{rpoly}(1, a)) = \{a\}$.

(19) Let us consider an integral domain F, a polynomial p over F, and a non zero element b of F. Then $\mathrm{Roots}(b \cdot p) = \mathrm{Roots}(p)$. The theorem is a consequence of (7).

(20) There exist polynomials p, q over $\mathbb{Z}/6$ such that $\mathrm{Roots}(p*q) \not\subseteq \mathrm{Roots}(p) \cup \mathrm{Roots}(q)$.

(21) Let us consider an integral domain R, and elements a, b of R. Then $\mathrm{rpoly}(1, a) \mid \mathrm{rpoly}(1, b)$ if and only if $a = b$. The theorem is a consequence of (18).

(22) Let us consider an integral domain R, and a non zero polynomial p over R. Then $\overline{\overline{\mathrm{Roots}(p)}} \leqslant \deg p$.

4. More about Bags

Let X be a non empty set and B be a bag of X. We introduce the notation $\overline{\overline{B}}$ as a synonym of $\sum B$.

Observe that there exists a bag of X which is zero and there exists a bag of X which is non zero.

Let b_1 be a bag of X and b_2 be a bag of X. One can check that $b_1 + b_2$ is X-defined and $b_1 + b_2$ is total.

Let us consider a non empty set X and a bag b of X. Now we state the propositions:

(23) $\overline{\overline{b}} = 0$ if and only if support $b = \emptyset$.

(24) b is zero if and only if support $b = \emptyset$.

(25) b is zero if and only if rng $b = \{0\}$.

Let X be a non empty set, b_1 be a non zero bag of X, and b_2 be a bag of X. One can check that $b_1 + b_2$ is non zero.

(26) Let us consider a non empty set X, a bag b of X, and an element x of X. Suppose support $b = \{x\}$. Then $b = (\{x\}, b(x))$-bag.

(27) Let us consider a non empty set X, a non empty bag b of X, and an element x of X. Then support $b = \{x\}$ if and only if $b = (\{x\}, b(x))$-bag and $b(x) \neq 0$. The theorem is a consequence of (26).

Let X be a set and S be a finite subset of X. The functor $\mathrm{Bag}(S)$ yielding a bag of X is defined by the term

(Def. 1) $(S, 1)$-bag.

Let X be a non empty set and S be a non empty, finite subset of X. Observe that $\mathrm{Bag}(S)$ is non zero.

Let b be a bag of X and a be an element of X. The functor $b \setminus a$ yielding a bag of X is defined by the term

(Def. 2) $b +\cdot (a, 0)$.

Let us consider a non empty set X, a bag b of X, and an element a of X. Now we state the propositions:

(28) $b \setminus a = b$ if and only if $a \notin$ support b.

(29) support$(b \setminus a) =$ support $b \setminus \{a\}$.

(30) $(b \setminus a) + (\{a\}, b(a))$-bag $= b$.

(31) Let us consider a non empty set X, an element a of X, and an element n of $\mathbb{N}$. Then $\overline{\overline{(\{a\}, n)\text{-bag}}} = n$. The theorem is a consequence of (23).

5. On Multiple Roots of Polynomials

Let R be an integral domain and p be a non zero polynomial over R with roots. One can verify that $\mathrm{BRoots}(p)$ is non zero.

Now we state the propositions:

(32) Let us consider a non degenerated commutative ring R, a non zero polynomial p over R, and an element a of R. Then multiplicity$(p, a) = 0$ if and only if $\mathrm{rpoly}(1, a) \nmid p$.

(33) Let us consider an integral domain R, a non zero polynomial p over R, and an element a of R. Then $\mathrm{multiplicity}(p, a) = n$ if and only if $(\mathrm{rpoly}(1, a))^n \mid p$ and $(\mathrm{rpoly}(1, a))^{n+1} \nmid p$. The theorem is a consequence of (10).

(34) Let us consider an integral domain R, and an element a of R. Then $\mathrm{multiplicity}(\mathrm{rpoly}(1, a), a) = 1$. The theorem is a consequence of (13) and (33).

(35) Let us consider an integral domain R, and elements a, b of R. If $b \neq a$, then $\mathrm{multiplicity}(\mathrm{rpoly}(1, a), b) = 0$. The theorem is a consequence of (21) and (32).

(36) Let us consider an integral domain R, a non zero polynomial p over R, a non zero element b of R, and an element a of R. Then $\mathrm{multiplicity}(p, a) = \mathrm{multiplicity}(b \cdot p, a)$. The theorem is a consequence of (33), (14), and (17).

(37) Let us consider an integral domain R, a non zero polynomial p over R, and a non zero element b of R. Then $\mathrm{BRoots}(b \cdot p) = \mathrm{BRoots}(p)$. The theorem is a consequence of (36).

(38) Let us consider an integral domain R, and a non zero polynomial p over R without roots. Then $\mathrm{BRoots}(p) = \mathrm{EmptyBag}(\text{the carrier of } R)$.

(39) Let us consider an integral domain R, and a non zero element a of R. Then $\overline{\overline{\mathrm{BRoots}(a \restriction R)}} = 0$. The theorem is a consequence of (23).

(40) Let us consider an integral domain R, and an element a of R. Then $\overline{\overline{\mathrm{BRoots}(\mathrm{rpoly}(1, a))}} = 1$. The theorem is a consequence of (10).

(41) Let us consider an integral domain R, and non zero polynomials p, q over R. Then $\overline{\overline{\mathrm{BRoots}(p * q)}} = \overline{\overline{\mathrm{BRoots}(p)}} + \overline{\overline{\mathrm{BRoots}(q)}}$.

(42) Let us consider an integral domain R, and a non zero polynomial p over R. Then $\overline{\overline{\mathrm{BRoots}(p)}} \leqslant \deg p$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non zero polynomial p over R such that $\deg p = \$_1$ holds $\overline{\overline{\mathrm{BRoots}(p)}} \leqslant \deg p$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. □

6. The Polynomial $X^n + 1$

Let R be a unital, non empty double loop structure and n be a natural number. The functor npoly(R, n) yielding a sequence of R is defined by the term

(Def. 3) $\mathbf{0}.R{+}{\cdot}[0 \longmapsto 1_R, n \longmapsto 1_R]$.

One can check that npoly(R, n) is finite-Support and npoly(R, n) is non zero.

Let us consider a unital, non degenerated double loop structure R. Now we state the propositions:

(43) $\deg \operatorname{npoly}(R, n) = n$.

(44) $\operatorname{LC} \operatorname{npoly}(R, n) = 1_R$.

(45) Let us consider a non degenerated ring R, and an element x of R. Then $\operatorname{eval}(\operatorname{npoly}(R, 0), x) = 1_R$.

(46) Let us consider a non degenerated ring R, a non zero natural number n, and an element x of R. Then $\operatorname{eval}(\operatorname{npoly}(R, n), x) = x^n + 1_R$.

PROOF: Set $q = \operatorname{npoly}(R, n)$. Consider F being a finite sequence of elements of R such that $\operatorname{eval}(q, x) = \sum F$ and $\operatorname{len} F = \operatorname{len} q$ and for every element j of $\mathbb{N}$ such that $j \in \operatorname{dom} F$ holds $F(j) = q(j -' 1) \cdot \operatorname{power}_R(x, j -' 1)$. Consider f_1 being a sequence of the carrier of R such that $\sum F = f_1(\operatorname{len} F)$ and $f_1(0) = 0_R$ and for every natural number j and for every element v of R such that $j < \operatorname{len} F$ and $v = F(j + 1)$ holds $f_1(j + 1) = f_1(j) + v$. Define $\mathcal{P}[\text{element of } \mathbb{N}] \equiv \$_1 = 0$ and $f_1(\$_1) = 0_R$ or $0 < \$_1 < \operatorname{len} F$ and $f_1(\$_1) = 1_R$ or $\$_1 = \operatorname{len} F$ and $f_1(\$_1) = x^n + 1_R$. For every element j of $\mathbb{N}$ such that $0 \leqslant j \leqslant \operatorname{len} F$ holds $\mathcal{P}[j]$. $\square$

(47) Let us consider an even natural number n, and an element x of $\mathbb{R}_{\mathrm{F}}$. Then $\operatorname{eval}(\operatorname{npoly}(\mathbb{R}_{\mathrm{F}}, n), x) > 0_{\mathbb{R}_{\mathrm{F}}}$. The theorem is a consequence of (45), (1), and (46).

(48) Let us consider an odd natural number n. Then $\operatorname{eval}(\operatorname{npoly}(\mathbb{R}_{\mathrm{F}}, n), -1_{\mathbb{R}_{\mathrm{F}}}) = 0_{\mathbb{R}_{\mathrm{F}}}$. The theorem is a consequence of (46).

(49) $\operatorname{eval}(\operatorname{npoly}(\mathbb{Z}/2, 2), 1_{\mathbb{Z}/2}) = 0_{\mathbb{Z}/2}$. The theorem is a consequence of (46) and (2).

Let n be an even natural number. Let us note that npoly$(\mathbb{R}_{\mathrm{F}}, n)$ and has not roots.

Let n be an odd natural number. Observe that npoly$(\mathbb{R}_{\mathrm{F}}, n)$ has roots and npoly$(\mathbb{Z}/2, 2)$ has roots.

7. The Polynomials $(x - a_1) * (x - a_2) * \ldots * (x - a_n)$

Let R be a ring.

A product of linear polynomials of R is a polynomial over R and is defined by

(Def. 4) there exists a non empty finite sequence F of elements of PolyRing(R) such that $it = \prod F$ and for every natural number i such that $i \in \operatorname{dom} F$ there exists an element a of R such that $F(i) = \operatorname{rpoly}(1, a)$.

Let R be an integral domain. One can verify that every product of linear polynomials of R is non constant and monic and has roots.

Now we state the propositions:

(50) Let us consider an integral domain R, and a product of linear polynomials p of R. Then $\operatorname{LC} p = 1_R$.

(51) Let us consider an integral domain R, and an element a of R. Then $\operatorname{rpoly}(1, a)$ is a product of linear polynomials of R.

(52) Let us consider an integral domain R, and products of linear polynomials p, q of R. Then $p * q$ is a product of linear polynomials of R.

Let R be an integral domain and B be a non zero bag of the carrier of R.

A product of linear polynomials of R and B is a product of linear polynomials of R and is defined by

(Def. 5) $\deg it = \overline{\overline{B}}$ and for every element a of R, $\operatorname{multiplicity}(it, a) = B(a)$.

Let us consider an integral domain R, a non zero bag B of the carrier of R, a product of linear polynomials p of R and B, and an element a of R. Now we state the propositions:

(53) If $a \in \operatorname{support} B$, then $\operatorname{eval}(p, a) = 0_R$. The theorem is a consequence of (11).

(54) (i) $(\operatorname{rpoly}(1, a))^{B(a)} \mid p$, and

(ii) $(\operatorname{rpoly}(1, a))^{B(a)+1} \nmid p$.

The theorem is a consequence of (33).

Let us consider an integral domain R, a non zero bag B of the carrier of R, and a product of linear polynomials p of R and B. Now we state the propositions:

(55) $\operatorname{BRoots}(p) = B$.

(56) $\deg p = \overline{\overline{\operatorname{BRoots}(p)}}$. The theorem is a consequence of (55).

(57) Let us consider an integral domain R, and an element a of R. Then $\operatorname{rpoly}(1, a)$ is a product of linear polynomials of R and $\operatorname{Bag}(\{a\})$. The theorem is a consequence of (51), (34), and (35).

(58) Let us consider an integral domain R, non zero bags B_1, B_2 of the carrier of R, a product of linear polynomials p of R and B_1, and a product of linear

polynomials q of R and B_2. Then $p * q$ is a product of linear polynomials of R and $B_1 + B_2$. The theorem is a consequence of (52), (56), and (55).

(59) Let us consider an integral domain R. Then every product of linear polynomials of R is a product of linear polynomials of R and BRoots(p).
Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every product of linear polynomials p of R such that $\deg p = \$_1$ holds p is a product of linear polynomials of R and BRoots(p). $\mathcal{P}[1]$. For every natural number k such that $k \geqslant 1$ holds $\mathcal{P}[k]$. □

Let R be an integral domain and S be a non empty, finite subset of R.

A product of linear polynomials of R and S is a product of linear polynomials of R and Bag(S). Now we state the proposition:

(60) Let us consider an integral domain R, a non empty, finite subset S of R, and a product of linear polynomials p of R and S. Then $\deg p = \overline{\overline{S}}$.

Let us consider an integral domain R, a non empty, finite subset S of R, a product of linear polynomials p of R and S, and an element a of R. Now we state the propositions:

(61) If $a \in S$, then $\mathrm{rpoly}(1, a) \mid p$ and $(\mathrm{rpoly}(1, a))^2 \nmid p$. The theorem is a consequence of (54).

(62) If $a \in S$, then $\mathrm{eval}(p, a) = 0_R$. The theorem is a consequence of (61).

(63) Let us consider an integral domain R, a non empty, finite subset S of R, and a product of linear polynomials p of R and S. Then Roots(p) $= S$. The theorem is a consequence of (62), (22), and (60).

8. Main Theorems

Now we state the proposition:

(64) Let us consider an integral domain R, and a non zero polynomial p over R with roots. Then there exists a product of linear polynomials q of R and BRoots(p) and there exists a polynomial r over R with non roots such that $p = q * r$ and Roots(q) = Roots(p).
Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every non zero polynomial p over R with roots such that $\deg p = \$_1$ there exists a product of linear polynomials q of R and BRoots(p) and there exists a polynomial r over R with non roots such that $p = q * r$ and Roots(q) = Roots(p). $\mathcal{P}[1]$ by (11), [9, (1)], (51), [8, (23), (27), (24)]. For every natural number k such that $1 \leqslant k$ holds $\mathcal{P}[k]$. Consider d being a natural number such that $\deg p = d$. □

Let us consider an integral domain R and a non zero polynomial p over R.

(65) $\overline{\overline{\mathrm{Roots}(p)}} \leqslant \overline{\overline{\mathrm{BRoots}(p)}}$. The theorem is a consequence of (64), (56), (55), (22), and (38).

(66) $\overline{\overline{\mathrm{BRoots}(p)}} = \deg p$ if and only if there exists an element a of R and there exists a product of linear polynomials q of R such that $p = a \cdot q$. The theorem is a consequence of (64), (56), (55), (59), (4), (37), and (38).

Now we state the proposition:

(67) Let us consider an integral domain R, and polynomials p, q over R. Suppose there exists a subset S of R such that $\overline{\overline{S}} = \max(\deg p, \deg q) + 1$ and for every element a of R such that $a \in S$ holds $\mathrm{eval}(p, a) = \mathrm{eval}(q, a)$. Then $p = q$. The theorem is a consequence of (22).

Let F be an algebraic closed field. Note that every non constant polynomial over F has roots and $\mathbb{R}_{\mathrm{F}}$ is non algebraic closed and every finite integral domain is non algebraic closed and every ring which is algebraic closed is also almost right invertible.

Now we state the propositions:

(68) Let us consider an algebraic closed field F, and a non constant polynomial p over F. Then there exists an element a of F and there exists a product of linear polynomials q of F and $\mathrm{BRoots}(p)$ such that $a \cdot q = p$. The theorem is a consequence of (64).

(69) Let us consider an algebraic closed field F. Then every non constant, monic polynomial over F is a product of linear polynomials of F and $\mathrm{BRoots}(p)$. The theorem is a consequence of (68).

(70) Let us consider a field F. Then F is algebraic closed if and only if every non constant, monic polynomial over F is a product of linear polynomials of F. The theorem is a consequence of (69).

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[3] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. On algebraic hierarchies in mathematical repository of Mizar. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, volume 8 of *Annals of Computer Science and Information Systems*, pages 363–371, 2016. doi:10.15439/2016F520.

[4] H. Heuser. *Lehrbuch der Analysis*. B.G. Teubner Stuttgart, 1990.

[5] Nathan Jacobson. *Basic Algebra I*. 2nd edition. Dover Publications Inc., 2009.

[6] Heinz Lüneburg. *Gruppen, Ringe, Körper: Die grundlegenden Strukturen der Algebra.* Oldenbourg Verlag, 1990.

[7] Knut Radbruch. *Algebra I.* Lecture Notes, University of Kaiserslautern, Germany, 1991.

[8] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Schur's theorem on the stability of networks. *Formalized Mathematics*, 14(**4**):135–142, 2006. doi:10.2478/v10037-006-0017-9.

[9] Christoph Schwarzweller, Artur Korniłowicz, and Agnieszka Rowińska-Schwarzweller. Some algebraic properties of polynomial rings. *Formalized Mathematics*, 24(**3**):227–237, 2016. doi:10.1515/forma-2016-0019.

Received August 30, 2017

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 25, No. 3, Pages 197–204, 2017
DOI: 10.1515/forma-2017-0019

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

Pell's Equation[1]

Marcin Acewicz
Institute of Informatics
University of Białystok
Poland

Karol Pąk
Institute of Informatics
University of Białystok
Poland

Summary. In this article we formalize several basic theorems that correspond to Pell's equation. We focus on two aspects: that the Pell's equation $x^2 - Dy^2 = 1$ has infinitely many solutions in positive integers for a given D not being a perfect square, and that based on the least fundamental solution of the equation when we can simply calculate algebraically each remaining solution.

"Solutions to Pell's Equation" are listed as item `#39` from the "Formalizing 100 Theorems" list maintained by Freek Wiedijk at `http://www.cs.ru.nl/F.Wiedijk/100/` .

MSC: 11D45 03B35

Keywords: Pell's equation; Diophantine equation; Hilbert's 10th problem

MML identifier: `PELLS_EQ`, version: `8.1.06 5.44.1305`

0. Introduction

Pell's equation (alternatively called the Pell-Fermat equation) is a type of a diophantine equation of the form $x^2 - Dy^2 = 1$ for a natural number D. If D is a perfect square, then Pell's equation can be rewritten as $(x - \sqrt{d}y) \cdot (x + \sqrt{d}y) = 1$. Similarly, the trivial solution $(x, y) = (1, 0)$ is not very interesting. Therefore it is often assumed that D is not a square and only nontrivial solutions (non zero pairs of integers) are considered. The first nontrivial solution (x_1, y_1), if the solutions are ordered by their magnitude, is called the *fundamental solution* and determine all other solutions since the n-th solution x_n, y_n can be expressed in terms of the fundamental solution by $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$.

[1]This work has been financed by the resources of the Polish National Science Centre granted by decision no. DEC-2015/19/D/ST6/01473.

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

Pell's equation has an exceptional history, described in detail in [5, 10]. Firstly, John Pell (1611–1685) has nothing to do with the equation, except the fact that Leonhard Euler (1707–1783) mistakenly attributed to Pell a solution method founded by William Brouncker (1620–1684). Solutions of Pell's equation for special cases (e.g., $D = 2$) were even considered in India and Greece around 400 BC. The first description of a method which allowed to construct a nontrivial solution of the equation for an arbitrary D can be found, e.g. in Euler's *Algebra*, but the method was described without any justification guaranteeing that it would find at least one solution. The first proof of correctness was published by Joseph Louis Lagrange [4].

Motivation The solution of Pell's equation has been applied in many branches of mathematics. Most basically, the sequence of fractions $\frac{x_i}{y_i}$ approximates $\sqrt{D}$ arbitrarily closely, where (x_i, y_i) is i-th solution for a given not square natural D. Note also that Stormer's theorem applies Pell's equations to find pairs of consecutive smooth numbers.

From our point of view, the most significant application of Pell's equation was done in the proof of Matiyasevich's theorem [6] that we try to formalize in the Mizar system [1]. That theorem states that every computable enumerable set is diophantine. It implies the undecidability of Hilbert's 10th problem. The proof is based mainly on a particular case

$$x^2 - (a^2 - 1)y^2 = 1, \tag{0.1}$$

where a is a natural number. Note that the pair $(a, 1)$ is the fundamental solution of the equation, so it seems that we do not need to consider a complicated construction of the fundamental solution for an arbitrary non square D to analyze all solutions of (0.1). Such a case of Pell's equation has been already formalized in HOL Light [2] and Metamath [7]. However, in our formalization we consider Pell's equation in the general case. This decision is a consequence of the fact that Matiyasevich to show that the equality $y_n(a) = y$ is diophantine used Pell's equation for $\overline{D} = (a^2 - 1) \cdot (2 \cdot y^2)^2$, where $y_n(a)$ is the n-th solution of (0.1). From Amthor's approach [3] to the cattle problem we can obtain a solution of Pell's equation for $\overline{D}$ based on the fundamental solution of (0.1), since for each solution $(\overline{x}, \overline{y})$ calculated for $\overline{D}$ there exists some n such that

$$\overline{x} + \overline{y} \cdot (2 \cdot y^2) = (a + 1\sqrt{a})^n. \tag{0.2}$$

But this approach is more difficult to formalize than Dirichlet's argumentation to obtain existence of the fundamental solution in the general case, as considered by W. Sierpiński [9].

Contributions We formalize theorems related to the solvability of Pell's equation imitating the approach considered in [9]. We formalize the Dirichlet's approximation theorem as Theorem 9, to show that $|x - y\sqrt{D}|$ can be arbitrarily close to 0. Then we show in Theorem 12 that there exist infinitely many pairs (x, y) where $|x^2 - Dy^2| < 2\sqrt{D} + 1$. Next, using several times the infinite variant of the pigeonhole principle in the justification of Theorem 13, we indicate two pairs of such solutions that fulfill the additional list of congruence, sufficient to construct a nontrivial solution of Pell's equation for a given non square D in the proof of Theorem 14. Since we can give another nontrivial solution $(ac + Dbd, cb + ad)$ based on any two nontrivial solutions $(a, b), (c, d)$ we show in Theorem 17 that there exist infinitely many solutions in positive integers for a given not square D. Then we show in Theorem 19 that such solutions can be ordered and we specify the fundamental solution in Definition 3. Finally, we show in Theorem 21 that each nontrivial solution can easily be calculated algebraically based on the fundamental solution.

1. Preliminaries

From now on n, n_1, n_2, k, D denote natural numbers, r, r_1, r_2 denote real numbers, and x, y denote integers.

Now we state the propositions:

(1) Let us consider integers i, j. If $j < 0$, then $j < i \bmod j \leqslant 0$.

(2) Let us consider integers i, j. If $j \neq 0$, then $|i \bmod j| < |j|$. The theorem is a consequence of (1).

(3) Let us consider a natural number D, and integers a, b, c, d. If $a + (b \cdot \sqrt{D}) = c + (d \cdot \sqrt{D})$, then $a = c$ and $b = d$.

(4) Let us consider natural numbers c, d, n. Then there exist natural numbers a, b such that $a + (b \cdot \sqrt{D}) = (c + (d \cdot \sqrt{D}))^n$.

Proof: Set $c_1 = c + (d \cdot \sqrt{D})$. Define $\mathcal{P}$[natural number] $\equiv$ there exist natural numbers a, b such that $a + (b \cdot \sqrt{D}) = {c_1}^{\$_1}$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n + 1]$. $\mathcal{P}[n]$. □

(5) Let us consider integers c, d, and a natural number n. Then there exist integers a, b such that $a + (b \cdot \sqrt{D}) = (c + (d \cdot \sqrt{D}))^n$.

Proof: Set $c_1 = c + (d \cdot \sqrt{D})$. Define $\mathcal{P}$[natural number] $\equiv$ there exist integers a, b such that $a + (b \cdot \sqrt{D}) = {c_1}^{\$_1}$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n + 1]$. $\mathcal{P}[n]$. □

(6) Let us consider a natural number D, integers a, b, c, d, and a natural number n. Suppose $a + (b \cdot \sqrt{D}) = (c + (d \cdot \sqrt{D}))^n$. Then $a - (b \cdot \sqrt{D}) = (c - (d \cdot \sqrt{D}))^n$.

PROOF: Set $S = \sqrt{D}$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every integers a, b, c, d such that $a + (b \cdot S) = (c + (d \cdot S))^{\$_1}$ holds $a - (b \cdot S) = (c - (d \cdot S))^{\$_1}$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

2. Solutions to Pell's Equation – Construction

Now we state the propositions:

(7) There exists a finite sequence F of elements of $\mathbb{N}$ such that

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

(ii) for every k such that $k \in \operatorname{dom} F$ holds $F(k) = \lfloor k - 1 \cdot \sqrt{D} \rfloor + 1$, and

(iii) if D is not square, then F is one-to-one.

PROOF: Define $\mathcal{F}(\text{natural number}) = \lfloor \$_1 - 1 \cdot \sqrt{D} \rfloor + 1$. Consider p being a finite sequence such that $\operatorname{len} p = n+1$ and for every k such that $k \in \operatorname{dom} p$ holds $p(k) = \mathcal{F}(k)$. $\operatorname{rng} p \subseteq \mathbb{N}$. □

(8) Let us consider real numbers a, b, and a finite sequence F of elements of $\mathbb{R}$. Suppose $n > 1$ and $\operatorname{len} F = n + 1$ and for every k such that $k \in \operatorname{dom} F$ holds $a < F(k) \leqslant b$. Then there exist natural numbers i, j such that

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

(ii) $i \neq j$, and

(iii) $F(i) \leqslant F(j)$, and

(iv) $F(j) - F(i) < \frac{b-a}{n}$.

PROOF: Define $\mathcal{P}(\text{natural number}) =]a + \frac{\$_1 - 1 \cdot (b-a)}{n}, a + \frac{\$_1 \cdot (b-a)}{n}]$. Define $\mathcal{H}[\text{object}, \text{object}] \equiv$ for every natural number k such that $\$_1 \in \mathcal{P}(k)$ holds $k = \$_2$. For every object x such that $x \in]a, b]$ there exists a natural number k such that $x \in \mathcal{P}(k)$ and $k \in \operatorname{Seg} n$. For every object x such that $x \in]a, b]$ there exists an object y such that $\mathcal{H}[x, y]$. Consider f being a function such that $\operatorname{dom} f =]a, b]$ and for every object x such that $x \in]a, b]$ holds $\mathcal{H}[x, f(x)]$. Set $f_1 = f \cdot F$. $\operatorname{rng} F \subseteq \operatorname{dom} f$. $\operatorname{rng} f_1 \subseteq \operatorname{Seg} n$. f_1 is one-to-one. □

(9) If D is not square and $n > 1$, then there exist integers x, y such that $y \neq 0$ and $|y| \leqslant n$ and $0 < x - (y \cdot \sqrt{D}) < \frac{1}{n}$.

PROOF: Consider x being a finite sequence of elements of $\mathbb{N}$ such that $\operatorname{len} x = n + 1$ and for every k such that $k \in \operatorname{dom} x$ holds $x(k) = \lfloor k - 1 \cdot \sqrt{D} \rfloor + 1$ and if D is not square, then x is one-to-one. Define $\mathcal{U}(\text{natural number}) = x(\$_1) - (\$_1 - 1 \cdot \sqrt{D})$. Consider u being a finite sequence such that $\operatorname{len} u = n+1$ and for every k such that $k \in \operatorname{dom} u$ holds $u(k) = \mathcal{U}(k)$. $\operatorname{rng} u \subseteq \mathbb{R}$. For every k such that $k \in \operatorname{dom} u$ holds $0 < u(k) \leqslant 1$. Consider

n_1, n_2 being natural numbers such that n_1, $n_2 \in \operatorname{dom} u$ and $n_1 \neq n_2$ and $u(n_1) \leqslant u(n_2)$ and $u(n_2) - u(n_1) < \frac{1-0}{n}$. $u(n_1) \neq u(n_2)$. □

(10) Suppose D is not square and $n \neq 0$ and $|y| \leqslant n$ and $0 < x-(y \cdot \sqrt{D}) < \frac{1}{n}$. Then $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| \leqslant 2 \cdot \sqrt{D} + \frac{1}{n^{\mathbf{2}}}$.

(11) If D is not square, then there exist integers x, y such that $y \neq 0$ and $0 < x - (y \cdot \sqrt{D})$ and $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| < 2 \cdot \sqrt{D} + 1$. The theorem is a consequence of (9) and (10).

(12) Suppose D is not square. Then $\{\langle x, y\rangle$, where x, y are integers : $y \neq 0$ and $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| < 2 \cdot \sqrt{D} + 1$ and $0 < x - (y \cdot \sqrt{D})\}$ is infinite.
Proof: Set $S = \{\langle x, y\rangle$, where x, y are integers : $y \neq 0$ and $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| < 2 \cdot \sqrt{D} + 1$ and $0 < x - (y \cdot \sqrt{D})\}$. There exists a function f from S into $\mathbb{R}$ such that for every integers x, y such that $\langle x, y\rangle \in S$ holds $f(\langle x, y\rangle) = x - (y \cdot \sqrt{D})$. Consider f being a function from S into $\mathbb{R}$ such that for every integers x, y such that $\langle x, y\rangle \in S$ holds $f(\langle x, y\rangle) = x-(y \cdot \sqrt{D})$. S is not empty. Reconsider $R = \operatorname{rng} f$ as a finite, non empty subset of $\mathbb{R}$. $\inf R > 0$. Consider n being a natural number such that $\frac{1}{n} < \inf R$ and $n > 1$. Consider x, y being integers such that $y \neq 0$ and $|y| \leqslant n$ and $0 < x-(y \cdot \sqrt{D}) < \frac{1}{n}$. $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| \leqslant 2 \cdot \sqrt{D} + \frac{1}{n^{\mathbf{2}}}$. $2 \cdot \sqrt{D} + \frac{1}{n^{\mathbf{2}}} < 2 \cdot \sqrt{D} + 1$. □

(13) Suppose D is not square. Then there exist integers k, a, b, c, d such that

(i) $0 \neq k$, and

(ii) $a^{\mathbf{2}} - (D \cdot b^{\mathbf{2}}) = k = c^{\mathbf{2}} - (D \cdot d^{\mathbf{2}})$, and

(iii) $a \equiv c \pmod{k}$, and

(iv) $b \equiv d \pmod{k}$, and

(v) $|a| \neq |c|$ or $|b| \neq |d|$.

Proof: Set $S = \{\langle x, y\rangle$, where x is an integer, y is an integer : $y \neq 0$ and $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| < 2 \cdot \sqrt{D} + 1$ and $0 < x - (y \cdot \sqrt{D})\}$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ for every integers x, y such that $\langle x, y\rangle = \$_1$ holds $\$_2 = x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})$. For every object x_1 such that $x_1 \in S$ there exists an object u such that $\mathcal{P}[x_1, u]$. Consider f being a function such that $\operatorname{dom} f = S$ and for every object x_1 such that $x_1 \in S$ holds $\mathcal{P}[x_1, f(x_1)]$. Reconsider $M = \lceil 2 \cdot \sqrt{D} + 1 \rceil$ as an element of $\mathbb{N}$. Define $\mathcal{P}[\text{integer}] \equiv \$_1 \neq 0$. Define $\mathcal{F}(\text{set}) = \$_1$. Set $S_1 = \{\mathcal{F}(i)$, where i is an element of $\mathbb{Z}$: $-M \leqslant i \leqslant M$ and $\mathcal{P}[i]\}$. S_1 is finite. $\operatorname{rng} f \subseteq S_1$. Consider k_1 being an object such that $k_1 \in \operatorname{rng} f$ and $f^{-1}(\{k_1\})$ is infinite. Consider k being an element of $\mathbb{Z}$ such that $k = k_1$ and $-M \leqslant k \leqslant M$ and $\mathcal{P}[k]$. Set $Z = f^{-1}(\{k\})$. Define $\mathcal{R}[\text{object}, \text{object}] \equiv$ for every integers x, y such that $\langle x, y\rangle = \$_1$ holds $\$_2 = \langle x \bmod k$, $y \bmod k\rangle$. For every object x_1 such that $x_1 \in Z$ there exists an object u

such that $\mathcal{R}[x_1, u]$. Consider g being a function such that $\operatorname{dom} g = Z$ and for every object x_1 such that $x_1 \in Z$ holds $\mathcal{R}[x_1, g(x_1)]$. Define $\mathcal{R}[\text{object}] \equiv$ not contradiction. Set $K = \{\mathcal{F}(i)$, where i is an element of $\mathbb{Z} : -|k| \leqslant i \leqslant |k|$ and $\mathcal{R}[i]\}$. K is finite. $\operatorname{rng} g \subseteq K \times K$. Consider a_1 being an object such that $a_1 \in \operatorname{rng} g$ and $g^{-1}(\{a_1\})$ is infinite. Consider X being an object such that $X \in g^{-1}(\{a_1\})$. Consider x, y being integers such that $X = \langle x, y \rangle$ and $y \neq 0$ and $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| < 2 \cdot \sqrt{D} + 1$ and $0 < x - (y \cdot \sqrt{D})$. There exist integers a, b, c, d such that $a^{\mathbf{2}} - (D \cdot b^{\mathbf{2}}) = k = c^{\mathbf{2}} - (D \cdot d^{\mathbf{2}})$ and $a \equiv c \pmod{k}$ and $b \equiv d \pmod{k}$ and $(|a| \neq |c|$ or $|b| \neq |d|)$. □

3. Pell's Equation

Now we state the proposition:

(14) #39: Solutions to Pell's Equation:
If D is not square, then there exist natural numbers x, y such that $x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}}) = 1$ and $y \neq 0$. The theorem is a consequence of (13).

Let D be a natural number.

A Pell's solution of D is an element of $\mathbb{Z} \times \mathbb{Z}$ and is defined by

(Def. 1) $((it)_{\mathbf{1}})^{\mathbf{2}} - (D \cdot ((it)_{\mathbf{2}})^{\mathbf{2}}) = 1$.

Let D_1, D_2 be real-membered, non empty sets and p be an element of $D_1 \times D_2$. We say that p is positive if and only if

(Def. 2) $(p)_{\mathbf{1}}$ is positive and $(p)_{\mathbf{2}}$ is positive.

One can check that there exists an element of $\mathbb{Z} \times \mathbb{Z}$ which is positive.

Let p be a positive element of $\mathbb{Z} \times \mathbb{Z}$. Observe that $(p)_{\mathbf{1}}$ is positive as an integer and $(p)_{\mathbf{2}}$ is positive as an integer.

Now we state the propositions:

(15) Let us consider square natural number D, and a positive element p of $\mathbb{Z} \times \mathbb{Z}$. If $D > 0$, then p is not a Pell's solution of D.

(16) If D is not square, then there exists a Pell's solution p of D such that p is positive. The theorem is a consequence of (14).

Let D be a natural number. One can verify that there exists a Pell's solution of D which is positive.

(17) The Cardinality of the Pell's Solutions:
Let us consider a natural number D. Then the set of all a_1 where a_1 is a positive Pell's solution of D is infinite.
Proof: Set $P =$ the set of all a_1 where a_1 is a positive Pell's solution of D. Set $a_1 =$ the positive Pell's solution of D. $\pi_2(P) \subseteq \mathbb{N}$. Reconsider $P_2 = \pi_2(P)$ as a finite, non empty subset of $\mathbb{N}$. Set $b = \max P_2$. Consider

a being an object such that $\langle a, b\rangle \in P$. Consider a_1 being a positive Pell's solution of D such that $\langle a, b\rangle = a_1$. $\square$

4. Solutions to Pell's Equation – Shape

In the sequel p, p_1, p_2 denote Pell's solutions of D.

Now we state the propositions:

(18) If D is not square, then p is positive iff $(p)_{\mathbf{1}} + ((p)_{\mathbf{2}} \cdot \sqrt{D}) > 1$.
Proof: If p is positive, then $(p)_{\mathbf{1}} + ((p)_{\mathbf{2}} \cdot \sqrt{D}) > 1$. $\square$

(19) Suppose $1 < (p_1)_{\mathbf{1}} + ((p_1)_{\mathbf{2}} \cdot \sqrt{D}) < (p_2)_{\mathbf{1}} + ((p_2)_{\mathbf{2}} \cdot \sqrt{D})$ and D is not square. Then

(i) $(p_1)_{\mathbf{1}} < (p_2)_{\mathbf{1}}$, and

(ii) $(p_1)_{\mathbf{2}} < (p_2)_{\mathbf{2}}$.

The theorem is a consequence of (18).

(20) Let us consider a natural number D, a positive Pell's solution p of D, integers a, b, and a natural number n. Suppose $n > 0$ and $a + (b \cdot \sqrt{D}) = ((p)_{\mathbf{1}} + ((p)_{\mathbf{2}} \cdot \sqrt{D}))^n$. Then $\langle a, b\rangle$ is a positive Pell's solution of D. The theorem is a consequence of (6) and (18).

Let D be a natural number. The minimal Pell's solution of D yielding a positive Pell's solution of D is defined by

(Def. 3) for every positive Pell's solution p of D, $(it)_{\mathbf{1}} \leqslant (p)_{\mathbf{1}}$ and $(it)_{\mathbf{2}} \leqslant (p)_{\mathbf{2}}$.

Now we state the proposition:

(21) Let us consider a natural number D, and an element p of $\mathbb{Z} \times \mathbb{Z}$. Then p is a positive Pell's solution of D if and only if there exists a positive natural number n such that $(p)_{\mathbf{1}} + ((p)_{\mathbf{2}} \cdot \sqrt{D}) = ((\text{the minimal Pell's solution of } D)_{\mathbf{1}} + ((\text{the minimal Pell's solution of } D)_{\mathbf{2}} \cdot \sqrt{D}))^n$.
Proof: Set $m =$ the minimal Pell's solution of D. Set $t = (m)_{\mathbf{1}}$. Set $u = (m)_{\mathbf{2}}$. Set $S = \sqrt{D}$. Set $x = (p)_{\mathbf{1}}$. Set $y = (p)_{\mathbf{2}}$. If p is a positive Pell's solution of D, then there exists a positive natural number n such that $x + (y \cdot S) = (t + (u \cdot S))^n$ by (18), (19), [8, (51), (57)]. $\langle x, y\rangle$ is a positive Pell's solution of D. $\square$

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] John Harrison. The HOL Light system REFERENCE. 2014. `http://www.cl.cam.ac.uk/~jrh13/hol-light/reference.pdf`.

[3] B. Krumbiegel and A. Amthor. Das Problema Bovinum des Archimedes. *Historisch-literarische Abteilung der Zeitschrift fur Mathematik und Physik*, 25:121–136, 153–171, 1880.

[4] Joseph L. Lagrange. Solution d'un probleème d'arithmétique. *Mélanges de philosophie et de math. de la Société Royale de Turin*, (44–97), 1773.

[5] Hendrik W. Lenstra. Solving the Pell equation. *Algorithmic Number Theory*, 44:1–24, 2008.

[6] Yuri Matiyasevich. Martin Davis and Hilbert's Tenth Problem. *Martin Davis on Computability, Computational Logic and Mathematical Foundations*, pages 35–54, 2017.

[7] Norman D. Megill. Metamath: A Computer Language for Pure Mathematics. 2007. `http://us.metamath.org/downloads/metamath.pdf`.

[8] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.

[9] Wacław Sierpiński. *Elementary Theory of Numbers*. PWN, Warsaw, 1964.

[10] André Weil. *Number Theory. An Approach through History from Hammurapi to Legendre*. Birkhäuser, Boston, Mass., 1983.

Received August 30, 2017

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 25, No. 3, Pages 205–216, 2017
DOI: 10.1515/forma-2017-0020

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

Simple-Named Complex-Valued Nominative Data – Definition and Basic Operations

Ievgen Ivanov
Taras Shevchenko National University
Kyiv, Ukraine

Mykola Nikitchenko
Taras Shevchenko National University
Kyiv, Ukraine

Andrii Kryvolap
Taras Shevchenko National University
Kyiv, Ukraine

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Summary. In this paper we give a formal definition of the notion of nominative data with simple names and complex values [15, 16, 19] and formal definitions of the basic operations on such data, including naming, denaming and overlapping, following the work [19].

The notion of nominative data plays an important role in the composition-nominative approach to program formalization [15, 16] which is a development of composition programming [18]. Both approaches are compared in [14].

The composition-nominative approach considers mathematical models of computer software and data on various levels of abstraction and generality and provides mathematical tools for reasoning about their properties. In particular, nominative data are mathematical models of data which are stored and processed in computer systems. The composition-nominative approach considers different types [14, 19] of nominative data, but all of them are based on the name-value relation. One powerful type of nominative data, which is suitable for representing many kinds of data commonly used in programming like lists, multidimensional arrays, trees, tables, etc. is the type of nominative data with simple (abstract) names and complex (structured) values. The set of nominative data of given type together with a number of basic operations on them like naming, denaming and overlapping [19] form an algebra which is called *data algebra*.

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

In the composition-nominative approach computer programs which process data are modeled as partial functions which map nominative data from the carrier of a given data algebra (input data) to nominative data (output data). Such functions are also called *binominative functions*. Programs which evaluate conditions are modeled as partial predicates on nominative data (nominative predicates). Programming language constructs like sequential execution, branching, cycle, etc. which construct programs from the existing programs are modeled as operations which take binominative functions and predicates and produce binominative functions. Such operations are called *compositions*. A set of binominative functions and a set of predicates together with appropriate compositions form an algebra which is called *program algebra*. This algebra serves as a semantic model of a programming language.

For functions over nominative data a special computability called abstract computability is introduces and complete classes of computable functions are specified [16].

For reasoning about properties of programs modeled as binominative functions a Floyd-Hoare style logic [1, 2] is introduced and applied [12, 13, 8, 11, 9, 10]. One advantage of this approach to reasoning about programs is that it naturally handles programs which process complex data structures (which can be quite straightforwardly represented as nominative data). Also, unlike classical Floyd-Hoare logic, the mentioned logic allows reasoning about assertions which include partial pre- and post-conditions [11].

Besides modeling data processed by programs, nominative data can be also applied to modeling data processed by signal processing systems in the context of the mathematical systems theory [4, 6, 7, 5, 3].

MSC: 68Q60 03B70 03B35

Keywords: program semantics; software verification; nominative data

MML identifier: `NOMIN_1`, version: `8.1.06 5.44.1305`

1. Preliminaries

From now on a, a_1, a_2, v, v_1, v_2, x denote objects, V, A denote sets, m, n denote natural numbers, and S, S_1, S_2 denote finite sequences.

Now we state the propositions:

(1) Let us consider a finite sequence f. If $n \in \operatorname{dom} f$, then $(\langle x \rangle ^\frown f)(n+1) = f(n)$.

(2) Let us consider a function f. Suppose $\operatorname{dom} f = \mathbb{N}$. Then $f \restriction \operatorname{Seg} n$ is a finite sequence.

(3) Let us consider finite sequences f, g. Then

(i) $\operatorname{dom} f \subseteq \operatorname{dom} g$, or

(ii) $\operatorname{dom} g \subseteq \operatorname{dom} f$.

Let f, g be finite sequences. One can check that $f{+}{\cdot}g$ is finite sequence-like.

Let f_1, f_2 be functions. Note that $f_2 \cup f_1 \restriction (\operatorname{dom} f_1 \setminus \operatorname{dom} f_2)$ is function-like.

Let f, g be functions and x, y be objects. We say that $f(x) \cong g(y)$ if and only if

(Def. 1) ($x \in \operatorname{dom} f$ iff $y \in \operatorname{dom} g$) and if $x \in \operatorname{dom} f$, then $f(x) = g(y)$.

2. Definition of Simple-Named Complex-Valued Nominative Data

Let us consider V and A.

A nominative set of V and A is a partial function from V to A. Let us note that there exists a nominative set of V and A which is finite.

A nominative data with simple names from V and simple values from A is a finite nominative set of V and A. The functor $\mathrm{ND}_{\mathrm{SS}}(V, A)$ yielding a set is defined by the term

(Def. 2) the set of all d where d is a nominative data with simple names from V and simple values from A.

Let us note that $\mathrm{ND}_{\mathrm{SS}}(V, A)$ is non empty.

Now we state the propositions:

(4) If $x \in \mathrm{ND}_{\mathrm{SS}}(V, A)$, then x is a nominative data with simple names from V and simple values from A.

(5) $\mathrm{ND}_{\mathrm{SS}}(V, A) \subseteq V \dot{\to} A$.

(6) $\emptyset \in \mathrm{ND}_{\mathrm{SS}}(V, A)$.

(7) Let us consider sets A, B. If $A \subseteq B$, then $\mathrm{ND}_{\mathrm{SS}}(V, A) \subseteq \mathrm{ND}_{\mathrm{SS}}(V, B)$.

(8) Let us consider finite functions f, g. Suppose $f \approx g$ and $f, g \in \mathrm{ND}_{\mathrm{SS}}(V, A)$. Then $f \cup g \in \mathrm{ND}_{\mathrm{SS}}(V, A)$. The theorem is a consequence of (4).

Let us consider V and A. The functor $\mathrm{FND}_{\mathrm{SC}}(V, A)$ yielding a function is defined by

(Def. 3) $\operatorname{dom} \mathit{it} = \mathbb{N}$ and $\mathit{it}(0) = A$ and for every natural number n, $\mathit{it}(n+1) = \mathrm{ND}_{\mathrm{SS}}(V, A \cup \mathit{it}(n))$.

Now we state the propositions:

(9) $(\mathrm{FND}_{\mathrm{SC}}(V, A))(1) = \mathrm{ND}_{\mathrm{SS}}(V, A)$.

(10) $(\mathrm{FND}_{\mathrm{SC}}(V, A))(2) = \mathrm{ND}_{\mathrm{SS}}(V, A \cup \mathrm{ND}_{\mathrm{SS}}(V, A))$. The theorem is a consequence of (9).

(11) $A \subseteq \bigcup \mathrm{FND}_{\mathrm{SC}}(V, A)$.

(12) If $1 \leqslant n$, then $\emptyset \in (\mathrm{FND}_{\mathrm{SC}}(V, A))(n)$. The theorem is a consequence of (6).

Let us consider V, A, and n. One can check that $\mathrm{FND}_{\mathrm{SC}}(V, A) \restriction \mathrm{Seg}\, n$ is finite sequence-like.

Now we state the proposition:

(13) If $m \neq 0$ and $m \leqslant n$, then $(\mathrm{FND}_{\mathrm{SC}}(V, A))(m) \subseteq (\mathrm{FND}_{\mathrm{SC}}(V, A))(n)$.
PROOF: Set $S = \mathrm{FND}_{\mathrm{SC}}(V, A)$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $m \leqslant \$_1$, then $S(m) \subseteq S(\$_1)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

Let us consider V and A. Let S be a finite sequence. We say that S is a rank sequence if and only if

(Def. 4) $S(1) = \mathrm{ND}_{\mathrm{SS}}(V, A)$ and for every natural number n such that $n, n+1 \in \mathrm{dom}\, S$ holds $S(n+1) = \mathrm{ND}_{\mathrm{SS}}(V, A \cup S(n))$.

Now we state the propositions:

(14) If S is a rank sequence, then $S \neq \emptyset$.

(15) If S is a rank sequence and $S_1 \subseteq S$ and $S_1 \neq \emptyset$, then S_1 is a rank sequence.

(16) If S is a rank sequence and $n \in \mathrm{dom}\, S$, then $S \restriction n$ is a rank sequence. The theorem is a consequence of (15).

(17) If S is a rank sequence, then $S \frown \langle \mathrm{ND}_{\mathrm{SS}}(V, A \cup S(\mathrm{len}\, S)) \rangle$ is a rank sequence.

(18) If $1 \leqslant n$, then $\mathrm{FND}_{\mathrm{SC}}(V, A) \restriction \mathrm{Seg}\, n$ is a rank sequence. The theorem is a consequence of (9).

(19) If S is a rank sequence and $n \in \mathrm{dom}\, S$, then $S(n) = (\mathrm{FND}_{\mathrm{SC}}(V, A))(n)$.
PROOF: Set $F = \mathrm{FND}_{\mathrm{SC}}(V, A)$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \in \mathrm{dom}\, S$, then $S(\$_1) = F(\$_1)$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every n, $\mathcal{P}[n]$. □

(20) If S is a rank sequence, then $S = \mathrm{FND}_{\mathrm{SC}}(V, A) \restriction \mathrm{dom}\, S$. The theorem is a consequence of (19).

(21) If S_1 is a rank sequence and S_2 is a rank sequence, then $S_1 \approx S_2$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \in \mathrm{dom}\, S_1 \cap \mathrm{dom}\, S_2$, then $S_1(\$_1) = S_2(\$_1)$. $\mathcal{P}[0]$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every n, $\mathcal{P}[n]$. □

(22) If S_1 is a rank sequence and S_2 is a rank sequence, then $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$. The theorem is a consequence of (20) and (3).

(23) If S_1 is a rank sequence and S_2 is a rank sequence, then $S_1 {+}\!\cdot S_2 = S_1$ or $S_1 {+}\!\cdot S_2 = S_2$. The theorem is a consequence of (21) and (3).

(24) If S_1 is a rank sequence and S_2 is a rank sequence, then $S_1 {+}\!\cdot S_2$ is a rank sequence.

(25) If S is a rank sequence and $m \leqslant n$ and $n \in \operatorname{dom} S$, then $S(m) \subseteq S(n)$. The theorem is a consequence of (19) and (13).

(26) Let us consider a finite sequence F. Suppose F is a rank sequence. Then there exists a finite sequence S such that

(i) $\operatorname{len} S = 1 + \operatorname{len} F$, and

(ii) S is a rank sequence, and

(iii) for every natural number n such that $n \in \operatorname{dom} S$ holds $S(n) = \mathrm{ND}_{\mathrm{SS}}(V, A \cup (\langle A \rangle \frown F)(n))$.

PROOF: Set $G = \langle A \rangle ^\frown F$. Define $\mathcal{F}(\text{object}) = \mathrm{ND}_{\mathrm{SS}}(V, A \cup G(\$_1))$. Consider S being a finite sequence such that $\operatorname{len} S = \operatorname{len} G$ and for every natural number n such that $n \in \operatorname{dom} S$ holds $S(n) = \mathcal{F}(n)$. For every natural number n such that $n \in \operatorname{dom} F$ holds $G(n + 1) = F(n)$. S is a rank sequence by (1), [17, (20)]. □

(27) $\langle \mathrm{ND}_{\mathrm{SS}}(V, A) \rangle$ is a rank sequence.

(28) $\langle \mathrm{ND}_{\mathrm{SS}}(V, A), \mathrm{ND}_{\mathrm{SS}}(V, A \cup \mathrm{ND}_{\mathrm{SS}}(V, A)) \rangle$ is a rank sequence. The theorem is a consequence of (27) and (17).

(29) $\langle \mathrm{ND}_{\mathrm{SS}}(V, A), \mathrm{ND}_{\mathrm{SS}}(V, A \cup \mathrm{ND}_{\mathrm{SS}}(V, A)), \mathrm{ND}_{\mathrm{SS}}(V, A \cup \mathrm{ND}_{\mathrm{SS}}(V, A \cup \mathrm{ND}_{\mathrm{SS}}(V, A))) \rangle$ is a rank sequence. The theorem is a consequence of (17) and (28).

Let us consider V and A.

A non-atomic nominative data of V and A is a function and is defined by

(Def. 5) there exists a finite sequence S such that S is a rank sequence and $\mathit{it} \in \bigcup S$.

From now on D, D_1, D_2 denote non-atomic nominative data of V and A.

Now we state the propositions:

(30) $\emptyset$ is a non-atomic nominative data of V and A. The theorem is a consequence of (27).

(31) $D \in \bigcup \mathrm{FND}_{\mathrm{SC}}(V, A)$.

(32) Let us consider a set d. If $d \subseteq D$, then d is a non-atomic nominative data of V and A. The theorem is a consequence of (4).

(33) There exists a natural number n such that D is a nominative data with simple names from V and simple values from $A \cup (\mathrm{FND}_{\mathrm{SC}}(V, A))(n)$. The theorem is a consequence of (19) and (4).

Let us consider V and A. Note that every non-atomic nominative data of V and A is finite.

Now we state the propositions:

(34) If $D_1 \approx D_2$ and S is a rank sequence and $D_1, D_2 \in S(m)$, then $D_1 \cup D_2 \in S(m)$. The theorem is a consequence of (4) and (8).

(35) If $D_1 \approx D_2$ and S_2 is a rank sequence and $S_1 \subseteq S_2$ and $D_1 \in \bigcup S_1$ and $D_2 \in \bigcup S_2$, then $D_1 \cup D_2 \in \bigcup S_2$. The theorem is a consequence of (25) and (34).

(36) If $D_1 \approx D_2$, then $D_1 \cup D_2$ is a non-atomic nominative data of V and A. The theorem is a consequence of (22) and (35).

(37) If $D_1 \approx D_2$, then $D_1 {+\cdot} D_2$ is a non-atomic nominative data of V and A. The theorem is a consequence of (36).

Let us consider V and A. A nominative data with simple names from V and complex values from A is a set and is defined by

(Def. 6) *it* $\in A$ or *it* is a non-atomic nominative data of V and A.

The functor $\mathrm{ND}_{\mathrm{SC}}(V, A)$ yielding a set is defined by the term

(Def. 7) the set of all D where D is a nominative data with simple names from V and complex values from A.

Let us observe that $\mathrm{ND}_{\mathrm{SC}}(V, A)$ is non empty. Now we state the propositions:

(38) $\emptyset \in \mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (30).

(39) If $x \in \mathrm{ND}_{\mathrm{SC}}(V, A)$, then x is a nominative data with simple names from V and complex values from A.

(40) $\mathrm{ND}_{\mathrm{SC}}(V, A) = \bigcup \mathrm{FND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (39), (11), (31), (4), and (18).

(41) $D \in \mathrm{ND}_{\mathrm{SC}}(V, A)$.

(42) If $D \notin A$, then $D \in \mathrm{ND}_{\mathrm{SC}}(V, A) \setminus A$. The theorem is a consequence of (41).

(43) If $x \in \mathrm{ND}_{\mathrm{SC}}(V, A) \setminus A$, then x is a non-atomic nominative data of V and A.

(44) Let us consider a nominative data D with simple names from V and complex values from A. Then $D \in \bigcup \mathrm{FND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (11) and (31).

3. Examples of Simple-Named Complex-Valued Nominative Data

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

(Def. 8) $v \dot{\longmapsto} a$.

Observe that $\mathrm{ND}(v, a)$ is function-like and relation-like.

Now we state the propositions:

(45) If $v \in V$ and $a \in A$, then $\mathrm{ND}(v, a) \in \mathrm{ND}_{\mathrm{SS}}(V, A)$.

(46) If $v \in V$ and $a \in A$, then $\mathrm{ND}(v, a)$ is a non-atomic nominative data of V and A. The theorem is a consequence of (27) and (45).

Let V, A be non empty sets, v be an element of V, and a be an element of A. Observe that the functor $\mathrm{ND}(v, a)$ yields a non-atomic nominative data of V and A. Now we state the proposition:

(47) If $v \in V$ and $a \in A$, then $\mathrm{ND}(v, a)$ is a nominative data with simple names from V and complex values from A. The theorem is a consequence of (46).

Let us consider v, v_1, and a_1. The functor $\mathrm{ND}(v, v_1, a_1)$ yielding a set is defined by the term

(Def. 9) $v \dot{\longmapsto} (v_1 \dot{\longmapsto} a_1)$.

Note that $\mathrm{ND}(v, v_1, a_1)$ is function-like and relation-like.

Now we state the propositions:

(48) If $\{v, v_1\} \subseteq V$ and $a_1 \in A$, then $\mathrm{ND}(v, v_1, a_1) \in \mathrm{ND}_{\mathrm{SS}}(V, A \cup \mathrm{ND}_{\mathrm{SS}}(V, A))$.

(49) If $\{v, v_1\} \subseteq V$ and $a_1 \in A$, then $\mathrm{ND}(v, v_1, a_1)$ is a non-atomic nominative data of V and A. The theorem is a consequence of (28) and (48).

Let V, A be non empty sets, v, v_1 be elements of V, and a be an element of A. Let us note that the functor $\mathrm{ND}(v, v_1, a)$ yields a non-atomic nominative data of V and A. Now we state the proposition:

(50) If $\{v, v_1\} \subseteq V$ and $a_1 \in A$, then $\mathrm{ND}(v, v_1, a_1)$ is a nominative data with simple names from V and complex values from A. The theorem is a consequence of (49).

Let us consider v, v_1, a, and a_1. The functor $\mathrm{ND}(v, v_1, a, a_1)$ yielding a set is defined by the term

(Def. 10) $[v \longmapsto a, v_1 \longmapsto a_1]$.

Let us note that $\mathrm{ND}(v, v_1, a, a_1)$ is function-like and relation-like.

Now we state the propositions:

(51) If $\{v, v_1\} \subseteq V$ and $\{a, a_1\} \subseteq A$, then $\mathrm{ND}(v, v_1, a, a_1) \in \mathrm{ND}_{\mathrm{SS}}(V, A)$. The theorem is a consequence of (45) and (8).

(52) If $\{v, v_1\} \subseteq V$ and $\{a, a_1\} \subseteq A$, then $\mathrm{ND}(v, v_1, a, a_1)$ is a non-atomic nominative data of V and A. The theorem is a consequence of (27) and (51).

Let V, A be non empty sets, v, v_1 be elements of V, and a, a_1 be elements of A. Let us observe that the functor $\mathrm{ND}(v, v_1, a, a_1)$ yields a non-atomic nominative data of V and A. Now we state the proposition:

(53) Suppose $\{v, v_1\} \subseteq V$ and $\{a, a_1\} \subseteq A$. Then $\mathrm{ND}(v, v_1, a, a_1)$ is a nominative data with simple names from V and complex values from A. The theorem is a consequence of (52).

Let us consider v, v_1, v_2, a, and a_1. The functor $\mathrm{ND}(v, v_1, v_2, a, a_1)$ yielding a set is defined by the term

(Def. 11) $[v \longmapsto a, v_1 \longmapsto v_2 \dot{\longmapsto} a_1]$.

Let us note that $\mathrm{ND}(v, v_1, v_2, a, a_1)$ is function-like and relation-like.

Now we state the propositions:

(54) Suppose $\{v, v_1, v_2\} \subseteq V$ and $\{a, a_1\} \subseteq A$. Then $\mathrm{ND}(v, v_1, v_2, a, a_1) \in \mathrm{ND}_{\mathrm{SS}}(V, A \cup \mathrm{ND}_{\mathrm{SS}}(V, A))$.

PROOF: Set $g = \mathrm{ND}(v, v_1, v_2, a, a_1)$. $\mathrm{rng}\, g \subseteq A \cup \mathrm{ND}_{\mathrm{SS}}(V, A)$. □

(55) If $\{v, v_1, v_2\} \subseteq V$ and $\{a, a_1\} \subseteq A$, then $\mathrm{ND}(v, v_1, v_2, a, a_1)$ is a non-atomic nominative data of V and A. The theorem is a consequence of (54) and (28).

Let V, A be non empty sets, v, v_1, v_2 be elements of V, and a, a_1 be elements of A. One can check that the functor $\mathrm{ND}(v, v_1, v_2, a, a_1)$ yields a non-atomic nominative data of V and A. Now we state the propositions:

(56) Suppose $\{v, v_1, v_2\} \subseteq V$ and $\{a, a_1\} \subseteq A$. Then $\mathrm{ND}(v, v_1, v_2, a, a_1)$ is a nominative data with simple names from V and complex values from A. The theorem is a consequence of (55).

(57) $\langle x \rangle$ is a non-atomic nominative data of $\{1\}$ and $\{x\}$.

PROOF: $\langle x \rangle \in \mathrm{ND}_{\mathrm{SS}}(\{1\}, \{x\})$. □

4. Operations on Simple-Named Complex-Valued Nominative Data

Let us consider V, A, v, and D. Assume $v \in \mathrm{dom}\, D$. The functor $v \Rightarrow_a D$ yielding a nominative data with simple names from V and complex values from A is defined by the term

(Def. 12) $D(v)$.

Let v, D be objects. Assume D is a nominative data with simple names from V and complex values from A. Assume $v \in V$. The functor $\Rightarrow v(D)$ yielding a non-atomic nominative data of V and A is defined by the term

(Def. 13) $v \dot{\longmapsto} D$.

Let a be an object and f be a V-valued finite sequence. Assume $\mathrm{len}\, f > 0$. The functor $\Rightarrow(V, A, f, a)$ yielding a finite sequence is defined by

(Def. 14) $\mathrm{len}\, it = \mathrm{len}\, f$ and $it(1) = \Rightarrow(f(\mathrm{len}\, f))(a)$ and for every natural number n such that $1 \leqslant n < \mathrm{len}\, it$ holds $it(n+1) = \Rightarrow(f(\mathrm{len}\, f - n))(it(n))$.

Now we state the proposition:

(58) Let us consider a V-valued finite sequence f. Suppose $1 \leqslant n \leqslant \mathrm{len}\, f$. Then $(\Rightarrow(V, A, f, a))(n)$ is a non-atomic nominative data of V and A.

Let us consider V and A. Let f be a V-valued finite sequence and a be an object. The functor $\Rightarrow f(a)$ yielding a set is defined by the term

(Def. 15) $(\Rightarrow(V, A, f, a))(\operatorname{len} \Rightarrow(V, A, f, a))$.

Now we state the propositions:

(59) Let us consider a V-valued finite sequence f. Suppose $\operatorname{len} f > 0$. Then $\Rightarrow f(a)$ is a non-atomic nominative data of V and A. The theorem is a consequence of (58).

(60) Let us consider a non empty set V, and an element v of V. Then $\Rightarrow\langle v\rangle(a) = \Rightarrow v(a)$.

(61) Let us consider a non empty set V, and elements v_1, v_2 of V. Suppose a is a nominative data with simple names from V and complex values from A. Then $\Rightarrow\langle v_1, v_2\rangle(a) = v_1 \dot{\longmapsto} (v_2 \dot{\longmapsto} a)$. The theorem is a consequence of (58).

(62) Let us consider a nominative data D with simple names from V and complex values from A. If $v \in V$, then $v \Rightarrow_a \Rightarrow v(D) = D$.

(63) If $v \in \operatorname{dom} D$, then $\Rightarrow v(v \Rightarrow_a D) = v \dot{\longmapsto} D(v)$. The theorem is a consequence of (33).

Let us consider V and A. Let d_1, d_2 be objects. Assume d_1 is a nominative data with simple names from V and complex values from A and d_2 is a nominative data with simple names from V and complex values from A.

The functor $d_1 \nabla_a d_2$ yielding a nominative data with simple names from V and complex values from A is defined by

(Def. 16) (i) there exist functions f_1, f_2 such that $f_1 = d_1$ and $f_2 = d_2$ and $it = f_2 \cup f_1 \restriction (\operatorname{dom} f_1 \setminus \operatorname{dom} f_2)$, **if** $d_1 \notin A$ and $d_2 \notin A$,

(ii) $it = d_2$, **otherwise**.

Let d_1, d_2, v be objects.

The functor $d_1 \nabla_a^v d_2$ yielding a nominative data with simple names from V and complex values from A is defined by the term

(Def. 17) $d_1 \nabla_a (\Rightarrow v(d_2))$.

Now we state the propositions:

(64) If $D_1 \notin A$ and $D_2 \notin A$, then $D_1 \nabla_a D_2 = D_2 \cup D_1 \restriction (\operatorname{dom} D_1 \setminus \operatorname{dom} D_2)$.

(65) If $D_1 \notin A$ and $D_2 \notin A$ and $\operatorname{dom} D_1 \subseteq \operatorname{dom} D_2$, then $D_1 \nabla_a D_2 = D_2$. The theorem is a consequence of (64).

(66) If $D \notin A$, then $D \nabla_a D = D$. The theorem is a consequence of (65).

(67) Suppose $v \in V$ and $v \dot{\longmapsto} a_1 \notin A$ and $v \dot{\longmapsto} a_2 \notin A$ and a_1 is a nominative data with simple names from V and complex values from A and a_2 is a nominative data with simple names from V and complex values from A. Then $(v \dot{\longmapsto} a_1) \nabla_a (v \dot{\longmapsto} a_2) = v \dot{\longmapsto} a_2$. The theorem is a consequence of (65).

(68) Suppose $\{v_1, v_2\} \subseteq V$ and $v_1 \neq v_2$ and $v_1 \dot{\longmapsto} a_1 \notin A$ and $v_2 \dot{\longmapsto} a_2 \notin A$ and a_1 is a nominative data with simple names from V and complex values from A and a_2 is a nominative data with simple names from V and complex values from A. Then $(v_1 \dot{\longmapsto} a_1) \nabla_a (v_2 \dot{\longmapsto} a_2) = [v_2 \longmapsto a_2, v_1 \longmapsto a_1]$. The theorem is a consequence of (64).

(69) Suppose $\{v, v_1, v_2\} \subseteq V$ and $v \neq v_1$ and $a_2 \in A$ and $v_1 \dot{\longmapsto} a_1 \notin A$ and $v \dot{\longmapsto} (v_2 \dot{\longmapsto} a_2) \notin A$ and a_1 is a nominative data with simple names from V and complex values from A. Then $(v_1 \dot{\longmapsto} a_1) \nabla_a^v (v_2 \dot{\longmapsto} a_2) = [v \longmapsto v_2 \dot{\longmapsto} a_2, v_1 \longmapsto a_1]$. The theorem is a consequence of (47) and (68).

Let us consider V, A, and v. The functor $v \Rightarrow_a$ yielding a partial function from $\mathrm{ND_{SC}}(V, A)$ to $\mathrm{ND_{SC}}(V, A)$ is defined by

(Def. 18) $\mathrm{dom}\, it = \{d$, where d is a non-atomic nominative data of V and $A : v \in \mathrm{dom}\, d\}$ and for every non-atomic nominative data D of V and A such that $D \in \mathrm{dom}\, it$ holds $it(D) = v \Rightarrow_a D$.

The functor $\Rightarrow v$ yielding a function from $\mathrm{ND_{SC}}(V, A)$ into $\mathrm{ND_{SC}}(V, A)$ is defined by

(Def. 19) for every nominative data D with simple names from V and complex values from A, $it(D) = \Rightarrow v(D)$.

The functor ∇_a^v yielding a partial function from $\mathrm{ND_{SC}}(V, A) \times \mathrm{ND_{SC}}(V, A)$ to $\mathrm{ND_{SC}}(V, A)$ is defined by

(Def. 20) $\mathrm{dom}\, it = (\mathrm{ND_{SC}}(V, A) \setminus A) \times \mathrm{ND_{SC}}(V, A)$ and for every non-atomic nominative data d_1 of V and A and for every object d_2 such that $d_1 \notin A$ and $d_2 \in \mathrm{ND_{SC}}(V, A)$ holds $it(\langle d_1, d_2 \rangle) = d_1 \nabla_a^v d_2$.

References

[1] R.W. Floyd. Assigning meanings to programs. *Mathematical aspects of computer science*, 19(19–32), 1967.

[2] C.A.R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10): 576–580, 1969.

[3] Ievgen Ivanov. On the underapproximation of reach sets of abstract continuous-time systems. In Erika Ábrahám and Sergiy Bogomolov, editors, *Proceedings 3rd International Workshop on Symbolic and Numerical Methods for Reachability Analysis, SNR@ETAPS 2017, Uppsala, Sweden, 22nd April 2017*, volume 247 of *EPTCS*, pages 46–51, 2017. doi:10.4204/EPTCS.247.4.

[4] Ievgen Ivanov. On representations of abstract systems with partial inputs and outputs. In T. V. Gopal, Manindra Agrawal, Angsheng Li, and S. Barry Cooper, editors, *Theory and Applications of Models of Computation – 11th Annual Conference, TAMC 2014, Chennai, India, April 11–13, 2014. Proceedings*, volume 8402 of *Lecture Notes in Computer Science*, pages 104–123. Springer, 2014. ISBN 978-3-319-06088-0. doi:10.1007/978-3-319-06089-7_8.

[5] Ievgen Ivanov. On local characterization of global timed bisimulation for abstract continuous-time systems. In Ichiro Hasuo, editor, *Coalgebraic Methods in Computer Science – 13th IFIP WG 1.3 International Workshop, CMCS 2016, Colocated with ETAPS 2016, Eindhoven, The Netherlands, April 2–3, 2016, Revised Selected Papers*, volume

9608 of *Lecture Notes in Computer Science*, pages 216–234. Springer, 2016. ISBN 978-3-319-40369-4. doi:10.1007/978-3-319-40370-0_13.

[6] Ievgen Ivanov, Mykola Nikitchenko, and Uri Abraham. On a decidable formal theory for abstract continuous-time dynamical systems. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications*, volume 469 of *Communications in Computer and Information Science*, pages 78–99. Springer International Publishing, 2014. ISBN 978-3-319-13205-1. doi:10.1007/978-3-319-13206-8_4.

[7] Ievgen Ivanov, Mykola Nikitchenko, and Uri Abraham. Event-based proof of the mutual exclusion property of Peterson's algorithm. *Formalized Mathematics*, 23(4):325–331, 2015. doi:10.1515/forma-2015-0026.

[8] Ievgen Ivanov, Mykola Nikitchenko, and Volodymyr G. Skobelev. Proving properties of programs on hierarchical nominative data. *The Computer Science Journal of Moldova*, 24(3):371–398, 2016.

[9] Artur Kornilowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the algebra of nominative data in Mizar. In Maria Ganzha, Leszek A. Maciaszek, and Marcin Paprzycki, editors, *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, FedCSIS 2017, Prague, Czech Republic, September 3–6, 2017.*, pages 237–244, 2017. ISBN 978-83-946253-7-5. doi:10.15439/2017F301.

[10] Artur Kornilowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the nominative algorithmic algebra in Mizar. In Leszek Borzemski, Jerzy Świątek, and Zofia Wilimowska, editors, *Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017 – Part II, Szklarska Poręba, Poland, September 17–19, 2017*, volume 656 of *Advances in Intelligent Systems and Computing*, pages 176–186. Springer, 2017. ISBN 978-3-319-67228-1. doi:10.1007/978-3-319-67229-8_16.

[11] Artur Korniłowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. An approach to formalization of an extension of Floyd-Hoare logic. In Vadim Ermolayev, Nick Bassiliades, Hans-Georg Fill, Vitaliy Yakovyna, Heinrich C. Mayr, Vyacheslav Kharchenko, Vladimir Peschanenko, Mariya Shyshkina, Mykola Nikitchenko, and Aleksander Spivakovsky, editors, *Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, Kyiv, Ukraine, May 15–18, 2017*, volume 1844 of *CEUR Workshop Proceedings*, pages 504–523. CEUR-WS.org, 2017.

[12] Andrii Kryvolap, Mykola Nikitchenko, and Wolfgang Schreiner. *Extending Floyd-Hoare Logic for Partial Pre- and Postconditions*, pages 355–378. Springer International Publishing, 2013. ISBN 978-3-319-03998-5. doi:10.1007/978-3-319-03998-5_18.

[13] Mykola Nikitchenko and Andrii Kryvolap. Properties of inference systems for Floyd-Hoare logic with partial predicates. *Acta Electrotechnica et Informatica*, 13(4):70–78, 2013. doi:10.15546/aeei-2013-0052.

[14] Mykola S. Nikitchenko. Composition-nominative aspects of address programming. *Cybernetics and Systems Analysis*, 45(864), 2009. doi:10.1007/s10559-009-9159-4. (Translated from Kibernetika i Sistemnyi Analiz, No. 6, pp. 24–35, November–December 2009).

[15] Nikolaj S. Nikitchenko. A composition nominative approach to program semantics. Technical Report IT-TR 1998-020, Department of Information Technology, Technical University of Denmark, 1998.

[16] N.S. Nikitchenko. Abstract computability of non-deterministic programs over various data structures. In Zamulin A.V. Bjorner D., Broy M., editor, *Perspectives of System Informatics: 4th International Andrei Ershov Memorial Conference, PSI 2001*, volume 2244 of *Lecture Notes in Computer Science*, pages 468–481. Springer, Berlin, Heidelberg, 2001. doi:10.1007/3-540-45575-2_45.

[17] Robin Nittka. Conway's games and some of their basic properties. *Formalized Mathematics*, 19(**2**):73–81, 2011. doi:10.2478/v10037-011-0013-6.

[18] V.N. Red'ko. Backgrounds of compositional programming. *Programming [in Russian]*, (3):3–13, 1979.

[19] Volodymyr G. Skobelev, Mykola Nikitchenko, and Ievgen Ivanov. On algebraic properties of nominative data and functions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and*

Communication Technologies in Education, Research, and Industrial Applications – 10th International Conference, ICTERI 2014, Kherson, Ukraine, June 9–12, 2014, Revised Selected Papers, volume 469 of *Communications in Computer and Information Science*, pages 117–138. Springer, 2014. ISBN 978-3-319-13205-1. doi:10.1007/978-3-319-13206-8_6.

Received August 30, 2017

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 25, No. 3, Pages 217–225, 2017
DOI: 10.1515/forma-2017-0021

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

Gauge Integral

Roland Coghetto
Rue de la Brasserie 5
7100 La Louvière, Belgium

Summary. Some authors have formalized the integral in the Mizar Mathematical Library (MML). The first article in a series on the Darboux/Riemann integral was written by Noboru Endou and Artur Korniłowicz: [6]. The Lebesgue integral was formalized a little later [13] and recently the integral of Riemann-Stieltjes was introduced in the MML by Keiko Narita, Kazuhisa Nakasho and Yasunari Shidama [12].

A presentation of definitions of integrals in other proof assistants or proof checkers (ACL2, COQ, Isabelle/HOL, HOL4, HOL Light, PVS, ProofPower) may be found in [10] and [4].

Using the Mizar system [1], we define the Gauge integral (Henstock-Kurzweil) of a real-valued function on a real interval $[a, b]$ (see [2], [3], [15], [14], [11]). In the next section we formalize that the Henstock-Kurzweil integral is linear.

In the last section, we verified that a real-valued bounded integrable (in sense Darboux/Riemann [6, 7, 8]) function over a interval a, b is Gauge integrable.

Note that, in accordance with the possibilities of the MML [9], we reuse a large part of demonstrations already present in another article. Instead of rewriting the proof already contained in [7] (MML Version: 5.42.1290), we slightly modified this article in order to use directly the expected results.

MSC: 26A39 26A42 03B35

Keywords: Gauge integral; Henstock-Kurzweil integral; generalized Riemann integral

MML identifier: `COUSIN2`, version: `8.1.06 5.44.1305`

1. Preliminaries

From now on a, b, c, d, e denote real numbers.

Now we state the propositions:

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

(1) If $a - b \leqslant c$ and $b \leqslant a$, then $|b - a| \leqslant c$.

(2) If $b - a \leqslant c$ and $a \leqslant b$, then $|b - a| \leqslant c$.

(3) If $a \leqslant b \leqslant c$ and $|a - d| \leqslant e$ and $|c - d| \leqslant e$, then $|b - d| \leqslant e$.

(4) If for every c such that $0 < c$ holds $|a - b| \leqslant c$, then $a = b$.

(5) Let us consider non negative real numbers b, c, d. Suppose $d < \frac{e}{2 \cdot b \cdot |c|}$. Then

(i) b is positive, and

(ii) c is positive.

(6) If $a \neq 0$, then $a \cdot \frac{b}{2 \cdot a} = \frac{b}{2}$.

(7) Let us consider non negative real numbers b, c, d. Suppose $a \leqslant b \cdot c \cdot d$ and $d < \frac{e}{2 \cdot b \cdot |c|}$. Then $a \leqslant \frac{e}{2}$. The theorem is a consequence of (5) and (6).

2. Vector Lattice / Riesz Space

Let X be a non empty set and f, g be functions from X into $\mathbb{R}$. The functor $\min(f, g)$ yielding a function from X into $\mathbb{R}$ is defined by

(Def. 1) for every element x of X, $it(x) = \min(f(x), g(x))$.

One can verify that the functor is commutative. The functor $\max(f, g)$ yielding a function from X into $\mathbb{R}$ is defined by

(Def. 2) for every element x of X, $it(x) = \max(f(x), g(x))$.

Note that the functor is commutative.

Let f, g be positive yielding functions from X into $\mathbb{R}$. One can check that $\min(f, g)$ is positive yielding and $\max(f, g)$ is positive yielding.

Let f, g be functions from X into $\mathbb{R}$. We say that $f \leqslant g$ if and only if

(Def. 3) for every element x of X, $f(x) \leqslant g(x)$.

Now we state the proposition:

(8) Let us consider a non empty set X, and functions f, g from X into $\mathbb{R}$. Then $\min(f, g) \leqslant f$.

Let us consider a non empty, real-membered set X. Now we state the propositions:

(9) If for every real number r such that $r \in X$ holds $\sup X = r$, then there exists a real number r such that $X = \{r\}$.

(10) If for every real number r such that $r \in X$ holds $\inf X = r$, then there exists a real number r such that $X = \{r\}$.

(11) Let us consider a non empty, lower bounded, upper bounded, real-membered set X. Suppose $\sup X = \inf X$. Then there exists a real number r such that $X = \{r\}$. The theorem is a consequence of (9).

3. Some Properties of the χ Function

In the sequel X, Y denote sets, Z denotes a non empty set, r denotes a real number, s denotes an extended real, A denotes a subset of $\mathbb{R}$, and f denotes a real-valued function.

Now we state the propositions:

(12) $\chi_{X,Y}$ is a function from Y into $\mathbb{R}$.

(13) If $A \subseteq]r, s[$, then A is lower bounded.

(14) If $A \subseteq]s, r[$, then A is upper bounded.

(15) If $\operatorname{rng} f \subseteq [a, b]$, then f is bounded.

(16) If $a \leqslant b$, then $\{a, b\} \subseteq [a, b]$.

(17) $\chi_{X,Y}$ is bounded. The theorem is a consequence of (16) and (15).

(18) If X misses Y, then for every element x of X, $\chi_{Y,X}(x) = 0$.

(19) Let us consider a function f from Z into $\mathbb{R}$. Then f is constant if and only if there exists a real number r such that $f = r \cdot \chi_{Z,Z}$.

(20) $\chi_{X,X}$ is positive yielding.

4. Refinement of Tagged Partition

In the sequel I denotes a non empty, closed interval subset of $\mathbb{R}$, T_1 denotes a tagged partition of I, D denotes a partition of I, T denotes an element of the set of tagged partitions of D, and f denotes a partial function from I to $\mathbb{R}$.

Now we state the propositions:

(21) If f is lower integrable, then $\text{lower\_sum}(f, D) \leqslant \text{lower\_integral}\, f$.

(22) If f is upper integrable, then $\text{upper\_integral}\, f \leqslant \text{upper\_sum}(f, D)$.

Let A be a non empty, closed interval subset of $\mathbb{R}$. The functor tagged-divs(A) yielding a set is defined by

(Def. 4) for every set x, $x \in \mathit{it}$ iff x is a tagged partition of A.

One can check that tagged-divs(A) is non empty.

Let T_1 be a tagged partition of A. The functor T_1-tags yielding a non empty, non-decreasing finite sequence of elements of $\mathbb{R}$ is defined by

(Def. 5) there exists a partition D of A and there exists an element T of the set of tagged partitions of D such that $\mathit{it} = T$ and $T_1 = \langle D, T \rangle$.

Now we state the propositions:

(23) If $T_1 = \langle D, T \rangle$, then $T = T_1$-tags and $D = T_1$-partition.

(24) $\text{len}(T_1\text{-tags}) = \text{len}(T_1\text{-partition})$. The theorem is a consequence of (23).

Let A be a non empty, closed interval subset of $\mathbb{R}$ and T_1 be a tagged partition of A. The functor $\operatorname{len} T_1$ yielding an element of $\mathbb{N}$ is defined by the term

(Def. 6) $\operatorname{len}(T_1\text{-partition})$.

The functor $\operatorname{dom} T_1$ yielding a set is defined by the term

(Def. 7) $\operatorname{dom}(T_1\text{-partition})$.

Now we state the propositions:

(25) Let us consider a non empty, closed interval subset I of $\mathbb{R}$, a partition D of I, and an element T of the set of tagged partitions of D. Then $\operatorname{rng} T \subseteq I$.

(26) Let us consider a non empty, closed interval subset I of $\mathbb{R}$, positive yielding functions j_1, j_2 from I into $\mathbb{R}$, and a j_1-fine tagged partition T_1 of I. If $j_1 \leqslant j_2$, then T_1 is a j_2-fine tagged partition of I. The theorem is a consequence of (23), (24), and (25).

5. Definition of the Gauge Integral on a Real Bounded Interval

Let I be a non empty, closed interval subset of $\mathbb{R}$, f be a partial function from I to $\mathbb{R}$, and T_1 be a tagged partition of I. The functor tagged-volume(f, T_1) yielding a finite sequence of elements of $\mathbb{R}$ is defined by

(Def. 8) $\operatorname{len} it = \operatorname{len} T_1$ and for every natural number i such that $i \in \operatorname{dom} T_1$ holds $it(i) = f((T_1\text{-tags})(i)) \cdot \operatorname{vol}(\operatorname{divset}(T_1\text{-partition}, i))$.

The functor tagged-sum(f, T_1) yielding a real number is defined by the term

(Def. 9) $\sum(\text{tagged-volume}(f, T_1))$.

Now we state the proposition:

(27) If $Y \subseteq X$, then $\chi_{X,Y} = \chi_{Y,Y}$.

From now on f denotes a function from I into $\mathbb{R}$.

Now we state the propositions:

(28) If I is non empty and trivial, then $\operatorname{vol}(I) = 0$.

(29) Let us consider a real number r. If $I = \{r\}$, then for every partition D of I, $D = \langle r \rangle$.

Let I be a non empty, closed interval subset of $\mathbb{R}$ and f be a function from I into $\mathbb{R}$. We say that f is HK-integrable if and only if

(Def. 10) there exists a real number J such that for every real number ε such that $\varepsilon > 0$ there exists a positive yielding function j from I into $\mathbb{R}$ such that for every tagged partition T_1 of I such that T_1 is j-fine holds $|\text{tagged-sum}(f, T_1) - J| \leqslant \varepsilon$.

Assume f is HK-integrable. The functor HK-integral(f) yielding a real number is defined by

(Def. 11) for every real number ε such that $\varepsilon > 0$ there exists a positive yielding function j from I into $\mathbb{R}$ such that for every tagged partition T_1 of I such that T_1 is j-fine holds $|\text{tagged-sum}(f, T_1) - it| \leqslant \varepsilon$.

Now we state the propositions:

(30) Let us consider a function f from I into $\mathbb{R}$. Suppose I is trivial. Then

(i) f is HK-integrable, and

(ii) HK-integral$(f) = 0$.

The theorem is a consequence of (20), (12), and (29).

(31) If A misses I and $f = \chi_{A,I}$, then tagged-sum$(f, T_1) = 0$.
Proof: For every natural number i such that $i \in \operatorname{dom} T_1$ holds (tagged-volume$(f, T_1))(i) = 0$. □

(32) If A misses I and $f = \chi_{A,I}$, then f is HK-integrable and HK-integral$(f) = 0$. The theorem is a consequence of (12) and (31).

(33) If $I \subseteq A$ and $f = \chi_{A,I}$, then f is HK-integrable and HK-integral(f) $=$ vol(I). The theorem is a consequence of (12) and (27).

Let I be a non empty, closed interval subset of $\mathbb{R}$. One can check that there exists a function from I into $\mathbb{R}$ which is HK-integrable.

6. The Linearity Property of the Gauge Integral

In the sequel f, g denote HK-integrable functions from I into $\mathbb{R}$ and r denotes a real number.

Now we state the propositions:

(34) Let us consider a natural number i. Suppose $i \in \operatorname{dom} T_1$. Then (tagged-volume$(r \cdot f, T_1))(i) =$ $r \cdot f((T_1\text{-tags})(i)) \cdot \text{vol}(\text{divset}(T_1\text{-partition}, i))$.

(35) tagged-volume$(r \cdot f, T_1) = r \cdot (\text{tagged-volume}(f, T_1))$.
Proof: For every natural number i such that $i \in \operatorname{dom}(\text{tagged-volume}(r \cdot f, T_1))$ holds (tagged-volume$(r \cdot f, T_1))(i) =$ $(r \cdot (\text{tagged-volume}(f, T_1)))(i)$. □

(36) Let us consider a natural number i. Suppose $i \in \operatorname{dom} T_1$. Then (tagged-volume$(f + g, T_1))(i) = f((T_1\text{-tags})(i)) \cdot \text{vol}(\text{divset}(T_1\text{-partition}, i)) + (g((T_1\text{-tags})(i)) \cdot \text{vol}(\text{divset}(T_1\text{-partition}, i)))$. The theorem is a consequence of (23), (24), and (25).

(37) tagged-volume$(f + g, T_1) =$ (tagged-volume$(f, T_1)) +$ (tagged-volume$(g, T_1))$.
Proof: For every natural number i such that $i \in$ dom(tagged-volume

$(f+g, T_1))$ holds $(\text{tagged-volume}(f+g, T_1))(i) = ((\text{tagged-volume}(f, T_1)) + (\text{tagged-volume}(g, T_1)))(i)$. □

(38) Suppose f is HK-integrable. Then

(i) $r \cdot f$ is an HK-integrable function from I into $\mathbb{R}$, and

(ii) $\text{HK-integral}(r \cdot f) = r \cdot \text{HK-integral}(f)$.

PROOF: Consider J being a real number such that for every real number ε such that $\varepsilon > 0$ there exists a positive yielding function j from I into $\mathbb{R}$ such that for every tagged partition T_1 of I such that T_1 is j-fine holds $|\text{tagged-sum}(f, T_1) - J| \leqslant \varepsilon$. For every real number ε such that $\varepsilon > 0$ there exists a positive yielding function j from I into $\mathbb{R}$ such that for every tagged partition T_1 of I such that T_1 is j-fine holds $|\text{tagged-sum}(r \cdot f, T_1) - (r \cdot J)| \leqslant \varepsilon$. □

(39) (i) $f+g$ is an HK-integrable function from I into $\mathbb{R}$, and

(ii) $\text{HK-integral}(f+g) = \text{HK-integral}(f) + \text{HK-integral}(g)$.

PROOF: Consider J_1 being a real number such that for every real number ε such that $\varepsilon > 0$ there exists a positive yielding function j from I into $\mathbb{R}$ such that for every tagged partition T_1 of I such that T_1 is j-fine holds $|\text{tagged-sum}(f, T_1) - J_1| \leqslant \varepsilon$. Consider J_2 being a real number such that for every real number ε such that $\varepsilon > 0$ there exists a positive yielding function j from I into $\mathbb{R}$ such that for every tagged partition T_1 of I such that T_1 is j-fine holds $|\text{tagged-sum}(g, T_1) - J_2| \leqslant \varepsilon$. For every real number ε such that $\varepsilon > 0$ there exists a positive yielding function j from I into $\mathbb{R}$ such that for every tagged partition T_1 of I such that T_1 is j-fine holds $|\text{tagged-sum}(f+g, T_1) - (J_1 + J_2)| \leqslant \varepsilon$. □

(40) Let us consider a function f from I into $\mathbb{R}$. Suppose f is constant. Then

(i) f is HK-integrable, and

(ii) there exists a real number r such that $f = r \cdot \chi_{I,I}$ and $\text{HK-integral}(f) = r \cdot \text{vol}(I)$.

The theorem is a consequence of (19), (12), (33), and (38).

7. Riemann Integrability and Gauge Integrability

Let I be a non empty, closed interval subset of $\mathbb{R}$. Note that there exists a function from I into $\mathbb{R}$ which is integrable.

Let X be a non empty set. Observe that there exists a function from X into $\mathbb{R}$ which is bounded.

Now we state the proposition:

(41) Let us consider a bounded function f from I into $\mathbb{R}$.
Then $|\sup \operatorname{rng} f - \inf \operatorname{rng} f| = 0$ if and only if f is constant. The theorem is a consequence of (11).

Let I be a non empty, closed interval subset of $\mathbb{R}$. Observe that there exists an integrable function from I into $\mathbb{R}$ which is bounded.

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

(42) If f is upper integrable, then there exists a real number r such that for every partition D of I, $r <$ upper_sum(f, D).

(43) If f is lower integrable, then there exists a real number r such that for every partition D of I, lower_sum$(f, D) < r$.

(44) Let us consider a function f from I into $\mathbb{R}$, and partitions D, D_1 of I. Suppose $D(1) = \inf I$ and $D_1 = D_{\lfloor 1}$. Then

(i) upper_sum(f, D_1) = upper_sum(f, D), and

(ii) lower_sum(f, D_1) = lower_sum(f, D).

Proof: (upper_volume(f, D))$(1) = 0$ by [5, (50)]. (lower_volume(f, D))$(1) = 0$ by [5, (50)]. □

In the sequel f denotes a bounded, integrable function from I into $\mathbb{R}$.

Now we state the propositions:

(45) Let us consider a natural number i. Suppose $i \in \operatorname{dom} T_1$. Then (lower_volume$(f, T_1$-partition$)$)$(i) \leqslant$ (tagged-volume(f, T_1))$(i) \leqslant$ (upper_volume$(f, T_1$-partition$)$)(i). The theorem is a consequence of (23).

(46) $\sum$ lower_volume$(f, T_1$-partition$) \leqslant \sum$(tagged-volume(f, T_1)) $\leqslant$ $\sum$ upper_volume$(f, T_1$-partition$)$. The theorem is a consequence of (45).

(47) Let us consider a real number ε. Suppose I is not trivial and $0 < \varepsilon$. Then there exists a partition D of I such that

(i) $D(1) \neq \inf I$, and

(ii) upper_sum$(f, D) <$ integral $f + \frac{\varepsilon}{2}$, and

(iii) integral $f - \frac{\varepsilon}{2} <$ lower_sum(f, D), and

(iv) upper_sum(f, D) − lower_sum$(f, D) < \varepsilon$.

The theorem is a consequence of (44).

From now on j denotes a positive yielding function from I into $\mathbb{R}$.

(48) If $j = r \cdot \chi_{I,I}$, then $0 < r$.

In the sequel D denotes a tagged partition of I. Now we state the proposition:

(49) If $j = r \cdot \chi_{I,I}$ and D is j-fine, then $\delta_{D\text{-partition}} \leqslant r$.

PROOF: Reconsider $g = \chi_{I,I}$ as a function from I into $\mathbb{R}$. For every natural number i such that $i \in \mathrm{dom}(D\text{-partition})$ holds $(\mathrm{upper\_volume}(g, D\text{-partition}))(i) \leqslant r$. $\delta_{D\text{-partition}} \leqslant r$. □

From now on r_1, r_2, s denote real numbers, D, D_1 denote partitions of I, and f_1 denotes a function from I into $\mathbb{R}$. Now we state the propositions:

(50) There exists a natural number i such that

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

(ii) $\min \mathrm{rng}\, \mathrm{upper\_volume}(f_1, D) = (\mathrm{upper\_volume}(f_1, D))(i)$.

(51) Let us consider a function f from I into $\mathbb{R}$, and a real number ε. Suppose $f_1 = \chi_{I,I}$ and $r_1 = \min \mathrm{rng}\, \mathrm{upper\_volume}(f_1, D_1)$ and $r_2 = \frac{\varepsilon}{2 \cdot \mathrm{len}\, D_1 \cdot |\sup \mathrm{rng}\, f - \inf \mathrm{rng}\, f|}$ and $0 < r_1$ and $0 < r_2$ and $s = \frac{\min(r_1, r_2)}{2}$ and $j = s \cdot f_1$ and T_1 is j-fine. Then

(i) $\delta_{T_1\text{-partition}} < \min \mathrm{rng}\, \mathrm{upper\_volume}(f_1, D_1)$, and

(ii) $\delta_{T_1\text{-partition}} < \frac{\varepsilon}{2 \cdot \mathrm{len}\, D_1 \cdot |\sup \mathrm{rng}\, f - \inf \mathrm{rng}\, f|}$.

The theorem is a consequence of (49).

(52) Let us consider a finite sequence p of elements of $\mathbb{R}$. Suppose for every natural number i such that $i \in \mathrm{dom}\, p$ holds $r \leqslant p(i)$ and there exists a natural number i_0 such that $i_0 \in \mathrm{dom}\, p$ and $p(i_0) = r$. Then $r = \inf \mathrm{rng}\, p$.

(53) Suppose $f_1 = \chi_{I,I}$. Then

(i) $0 \leqslant \min \mathrm{rng}\, \mathrm{upper\_volume}(f_1, D)$, and

(ii) $0 = \min \mathrm{rng}\, \mathrm{upper\_volume}(f_1, D)$ iff $\mathrm{divset}(D, 1) = [D(1), D(1)]$.

PROOF: Consider i_0 being a natural number such that $i_0 \in \mathrm{dom}\, D$ and $\min \mathrm{rng}\, \mathrm{upper\_volume}(f_1, D) = (\mathrm{upper\_volume}(f_1, D))(i_0)$. $0 = \min \mathrm{rng}\, \mathrm{upper\_volume}(f_1, D)$ iff $\mathrm{divset}(D, 1) = [D(1), D(1)]$. □

(54) If $\mathrm{divset}(D, 1) = [D(1), D(1)]$, then $D(1) = \inf I$.

(55) Let us consider a bounded, integrable function f from I into $\mathbb{R}$. Then

(i) f is HK-integrable, and

(ii) $\mathrm{HK\text{-}integral}(f) = \mathrm{integral}\, f$.

The theorem is a consequence of (40), (12), (17), (28), (30), (47), (53), (54), (41), (20), (46), (51), (21), (22), (7), (1), (2), and (3).

Let I be a non empty, closed interval subset of $\mathbb{R}$. Note that every function from I into $\mathbb{R}$ which is bounded and integrable is also HK-integrable.

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] Robert G. Bartle. Return to the Riemann integral. *American Mathematical Monthly*, pages 625–632, 1996.

[3] Robert G. Bartle. *A modern theory of integration*, volume 32. American Mathematical Society Providence, 2001.

[4] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Formalization of real analysis: A survey of proof assistants and libraries. *Mathematical Structures in Computer Science*, 26(7):1196–1233, 2016.

[5] Roland Coghetto. Cousin's lemma. *Formalized Mathematics*, 24(**2**):107–119, 2016. doi:10.1515/forma-2016-0009.

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

[7] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Darboux's theorem. *Formalized Mathematics*, 9(**1**):197–200, 2001.

[8] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Integrability of bounded total functions. *Formalized Mathematics*, 9(**2**):271–274, 2001.

[9] Adam Grabowski and Christoph Schwarzweller. Revisions as an essential tool to maintain mathematical repositories. In M. Kauers, M. Kerber, R. Miner, and W. Windsteiger, editors, *Towards Mechanized Mathematical Assistants. Lecture Notes in Computer Science*, volume 4573, pages 235–249. Springer: Berlin, Heidelberg, 2007.

[10] John Harrison. Formalizing basic complex analysis. *Studies in Logic, Grammar and Rhetoric*, 23(10):151–165, 2007.

[11] Jean Mawhin. L'éternel retour des sommes de Riemann-Stieltjes dans l'évolution du calcul intégral. *Bulletin de la Société Royale des Sciences de Liège*, 70(4–6):345–364, 2001.

[12] Keiko Narita, Kazuhisa Nakasho, and Yasunari Shidama. Riemann-Stieltjes integral. *Formalized Mathematics*, 24(**3**):199–204, 2016. doi:10.1515/forma-2016-0016.

[13] Yasunari Shidama, Noburu Endou, and Pauline N. Kawamoto. On the formalization of Lebesgue integrals. *Studies in Logic, Grammar and Rhetoric*, 10(23):167–177, 2007.

[14] Lee Peng Yee. The integral à la Henstock. *Scientiae Mathematicae Japonicae*, 67(1): 13–21, 2008.

[15] Lee Peng Yee and Rudolf Vyborny. *Integral: an easy approach after Kurzweil and Henstock*, volume 14. Cambridge University Press, 2000.

Received September 3, 2017

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 25, No. 3, Pages 227–240, 2017
DOI: 10.1515/forma-2017-0022

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

Integral of Non Positive Functions

Noboru Endou
National Institute of Technology, Gifu College
2236-2 Kamimakuwa, Motosu, Gifu, Japan

Summary. In this article, we formalize in the Mizar system [1, 7] the Lebesgue type integral and convergence theorems for non positive functions [8],[2]. Many theorems are based on our previous results [5], [6].

MSC: 28A25 03B35

Keywords: integration of non positive function

MML identifier: `MESFUN11`, version: `8.1.06 5.44.1305`

1. Preliminaries

Let X be a non empty set and f be a non-negative partial function from X to $\overline{\mathbb{R}}$. Observe that $-f$ is non-positive.

Let f be a non-positive partial function from X to $\overline{\mathbb{R}}$. One can check that $-f$ is non-negative.

Now we state the propositions:

(1) Let us consider a non empty set X, a non-positive partial function f from X to $\overline{\mathbb{R}}$, and a set E. Then $f \restriction E$ is non-positive.

(2) Let us consider a non empty set X, a set A, a real number r, and a partial function f from X to $\overline{\mathbb{R}}$. Then $(r \cdot f) \restriction A = r \cdot (f \restriction A)$.

(3) Let us consider a non empty set X, a set A, and a partial function f from X to $\overline{\mathbb{R}}$. Then $-f \restriction A = (-f) \restriction A$. The theorem is a consequence of (2).

(4) Let us consider a non empty set X, a partial function f from X to $\overline{\mathbb{R}}$, and a real number c. Suppose f is non-positive. Then

(i) if $0 \leqslant c$, then $c \cdot f$ is non-positive, and

(ii) if $c \leqslant 0$, then $c \cdot f$ is non-negative.

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

(5) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, and a partial function f from X to $\overline{\mathbb{R}}$. Then

(i) $\max_{+}(f)$ is non-negative, and

(ii) $\max_{-}(f)$ is non-negative, and

(iii) $|f|$ is non-negative.

(6) Let us consider a non empty set X, a partial function f from X to $\overline{\mathbb{R}}$, and an object x. Then

(i) $f(x) \leqslant (\max_{+}(f))(x)$, and

(ii) $f(x) \geqslant -(\max_{-}(f))(x)$.

(7) Let us consider a non empty set X, a partial function f from X to $\overline{\mathbb{R}}$, and a positive real number r. Then $\text{LE-dom}(f, r) = \text{LE-dom}(\max_{+}(f), r)$.

(8) Let us consider a non empty set X, a partial function f from X to $\overline{\mathbb{R}}$, and a non positive real number r. Then $\text{LE-dom}(f, r) = \text{GT-dom}(\max_{-}(f), -r)$.

(9) Let us consider a non empty set X, partial functions f, g from X to $\overline{\mathbb{R}}$, an extended real a, and a real number r. Suppose $r \neq 0$ and $g = r \cdot f$. Then $\text{EQ-dom}(f, a) = \text{EQ-dom}(g, a \cdot r)$.

(10) Let us consider a non empty set X, a σ-field S of subsets of X, a partial function f from X to $\overline{\mathbb{R}}$, and an element A of S. Suppose $A \subseteq \text{dom} f$. Then f is measurable on A if and only if $\max_{+}(f)$ is measurable on A and $\max_{-}(f)$ is measurable on A.

Let X be a non empty set, f be a function from X into $\overline{\mathbb{R}}$, and r be a real number. Note that the functor $r \cdot f$ yields a function from X into $\overline{\mathbb{R}}$. Now we state the proposition:

(11) Let us consider a non empty set X, a real number r, and a without $+\infty$ function f from X into $\overline{\mathbb{R}}$. If $r \geqslant 0$, then $r \cdot f$ is without $+\infty$.

Let X be a non empty set, f be a without $+\infty$ function from X into $\overline{\mathbb{R}}$, and r be a non negative real number. Let us note that $r \cdot f$ is without $+\infty$ as a function from X into $\overline{\mathbb{R}}$.

Now we state the proposition:

(12) Let us consider a non empty set X, a real number r, and a without $+\infty$ function f from X into $\overline{\mathbb{R}}$. If $r \leqslant 0$, then $r \cdot f$ is without $-\infty$.

Let X be a non empty set, f be a without $+\infty$ function from X into $\overline{\mathbb{R}}$, and r be a non positive real number. One can check that $r \cdot f$ is without $-\infty$.

Now we state the proposition:

(13) Let us consider a non empty set X, a real number r, and a without $-\infty$ function f from X into $\overline{\mathbb{R}}$. If $r \geqslant 0$, then $r \cdot f$ is without $-\infty$.

Let X be a non empty set, f be a without $-\infty$ function from X into $\overline{\mathbb{R}}$, and r be a non negative real number. One can check that $r \cdot f$ is without $-\infty$.

Now we state the proposition:

(14) Let us consider a non empty set X, a real number r, and a without $-\infty$ function f from X into $\overline{\mathbb{R}}$. If $r \leqslant 0$, then $r \cdot f$ is without $+\infty$.

Let X be a non empty set, f be a without $-\infty$ function from X into $\overline{\mathbb{R}}$, and r be a non positive real number. One can check that $r \cdot f$ is without $+\infty$.

Now we state the proposition:

(15) Let us consider a non empty set X, a real number r, and a without $-\infty$, without $+\infty$ function f from X into $\overline{\mathbb{R}}$. Then $r \cdot f$ is without $-\infty$ and without $+\infty$.

Let X be a non empty set, f be a without $-\infty$, without $+\infty$ function from X into $\overline{\mathbb{R}}$, and r be a real number. Note that $r \cdot f$ is without $-\infty$ and without $+\infty$.

Now we state the propositions:

(16) Let us consider a non empty set X, a positive real number r, and a function f from X into $\overline{\mathbb{R}}$. Then f is without $+\infty$ if and only if $r \cdot f$ is without $+\infty$.

(17) Let us consider a non empty set X, a negative real number r, and a function f from X into $\overline{\mathbb{R}}$. Then f is without $+\infty$ if and only if $r \cdot f$ is without $-\infty$.

(18) Let us consider a non empty set X, a positive real number r, and a function f from X into $\overline{\mathbb{R}}$. Then f is without $-\infty$ if and only if $r \cdot f$ is without $-\infty$.

(19) Let us consider a non empty set X, a negative real number r, and a function f from X into $\overline{\mathbb{R}}$. Then f is without $-\infty$ if and only if $r \cdot f$ is without $+\infty$.

(20) Let us consider a non empty set X, a non zero real number r, and a function f from X into $\overline{\mathbb{R}}$. Then f is without $-\infty$ and without $+\infty$ if and only if $r \cdot f$ is without $-\infty$ and without $+\infty$. The theorem is a consequence of (16), (18), (17), and (19).

(21) Let us consider non empty sets X, Y, a partial function f from X to $\overline{\mathbb{R}}$, and a real number r. Suppose $f = Y \longmapsto r$. Then f is without $-\infty$ and without $+\infty$.

(22) Let us consider a non empty set X, and a function f from X into $\overline{\mathbb{R}}$. Then

(i) $0 \cdot f = X \longmapsto 0$, and

(ii) $0 \cdot f$ is without $-\infty$ and without $+\infty$.

Proof: For every element x of X, $(0 \cdot f)(x) = (X \longmapsto 0)(x)$. □

(23) Let us consider a non empty set X, and partial functions f, g from X to $\overline{\mathbb{R}}$. Suppose f is without $-\infty$ and without $+\infty$. Then

(i) $\operatorname{dom}(f + g) = \operatorname{dom} f \cap \operatorname{dom} g$, and

(ii) $\operatorname{dom}(f - g) = \operatorname{dom} f \cap \operatorname{dom} g$, and

(iii) $\operatorname{dom}(g - f) = \operatorname{dom} f \cap \operatorname{dom} g$.

Let us consider a non empty set X and functions f_1, f_2 from X into $\overline{\mathbb{R}}$. Now we state the propositions:

(24) Suppose f_2 is without $-\infty$ and without $+\infty$. Then

(i) $f_1 + f_2$ is a function from X into $\overline{\mathbb{R}}$, and

(ii) for every element x of X, $(f_1 + f_2)(x) = f_1(x) + f_2(x)$.

The theorem is a consequence of (23).

(25) Suppose f_1 is without $-\infty$ and without $+\infty$. Then

(i) $f_1 - f_2$ is a function from X into $\overline{\mathbb{R}}$, and

(ii) for every element x of X, $(f_1 - f_2)(x) = f_1(x) - f_2(x)$.

The theorem is a consequence of (23).

(26) Suppose f_2 is without $-\infty$ and without $+\infty$. Then

(i) $f_1 - f_2$ is a function from X into $\overline{\mathbb{R}}$, and

(ii) for every element x of X, $(f_1 - f_2)(x) = f_1(x) - f_2(x)$.

The theorem is a consequence of (23).

(27) Let us consider non empty sets X, Y, and partial functions f_1, f_2 from X to $\overline{\mathbb{R}}$. Suppose $\operatorname{dom} f_1 \subseteq Y$ and $f_2 = Y \longmapsto 0$. Then

(i) $f_1 + f_2 = f_1$, and

(ii) $f_1 - f_2 = f_1$, and

(iii) $f_2 - f_1 = -f_1$.

The theorem is a consequence of (21) and (23).

Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, and partial functions f, g from X to $\overline{\mathbb{R}}$. Now we state the propositions:

(28) If f is simple function in S and g is simple function in S, then $f + g$ is simple function in S.

Proof: Consider F being a finite sequence of separated subsets of S, a being a finite sequence of elements of $\overline{\mathbb{R}}$ such that F and a are representation of f. Consider G being a finite sequence of separated subsets of S, b being a finite sequence of elements of $\overline{\mathbb{R}}$ such that G and b are representation of g. Set $l_1 = \operatorname{len} a$. Set $l_2 = \operatorname{len} b$. Define $\mathcal{H}(\text{natural number}) =$

$F((\$_1 -' 1 \operatorname{div} l_2) + 1) \cap G((\$_1 -' 1 \bmod l_2) + 1)$. Consider F_1 being a finite sequence such that $\operatorname{len} F_1 = l_1 \cdot l_2$ and for every natural number k such that $k \in \operatorname{dom} F_1$ holds $F_1(k) = \mathcal{H}(k)$. For every natural numbers k, l such that k, $l \in \operatorname{dom} F_1$ and $k \neq l$ holds $F_1(k)$ misses $F_1(l)$. $\operatorname{dom}(f+g) = \bigcup \operatorname{rng} F_1$. For every natural number k and for every elements x, y of X such that $k \in \operatorname{dom} F_1$ and x, $y \in F_1(k)$ holds $(f+g)(x) = (f+g)(y)$. □

(29) If f is simple function in S and g is simple function in S, then $f - g$ is simple function in S. The theorem is a consequence of (28).

(30) Let us consider a non empty set X, a σ-field S of subsets of X, and a partial function f from X to $\overline{\mathbb{R}}$. If f is simple function in S, then $-f$ is simple function in S.

(31) Let us consider a non empty set X, and a non-negative partial function f from X to $\overline{\mathbb{R}}$. Then $f = \max_+(f)$.
PROOF: For every element x of X such that $x \in \operatorname{dom} f$ holds $f(x) = (\max_+(f))(x)$. □

(32) Let us consider a non empty set X, and a non-positive partial function f from X to $\overline{\mathbb{R}}$. Then $f = -\max_-(f)$.
PROOF: For every element x of X such that $x \in \operatorname{dom} f$ holds $f(x) = (-\max_-(f))(x)$. □

(33) Let us consider a non empty set C, a partial function f from C to $\overline{\mathbb{R}}$, and a real number c. Suppose $c \leqslant 0$. Then

   (i) $\max_+(c \cdot f) = (-c) \cdot \max_-(f)$, and

   (ii) $\max_-(c \cdot f) = (-c) \cdot \max_+(f)$.

PROOF: For every element x of C such that $x \in \operatorname{dom} \max_+(c \cdot f)$ holds $(\max_+(c \cdot f))(x) = ((-c) \cdot \max_-(f))(x)$. For every element x of C such that $x \in \operatorname{dom} \max_-(c \cdot f)$ holds $(\max_-(c \cdot f))(x) = ((-c) \cdot \max_+(f))(x)$. □

(34) Let us consider a non empty set X, and a partial function f from X to $\overline{\mathbb{R}}$. Then $\max_+(f) = \max_-(-f)$. The theorem is a consequence of (33).

(35) Let us consider a non empty set X, a partial function f from X to $\overline{\mathbb{R}}$, and real numbers r_1, r_2. Then $r_1 \cdot (r_2 \cdot f) = (r_1 \cdot r_2) \cdot f$.

(36) Let us consider a non empty set X, and partial functions f, g from X to $\overline{\mathbb{R}}$. If $f = -g$, then $g = -f$. The theorem is a consequence of (35).

Let X be a non empty set, F be a sequence of partial functions from X into $\overline{\mathbb{R}}$, and r be a real number. The functor $r \cdot F$ yielding a sequence of partial functions from X into $\overline{\mathbb{R}}$ is defined by

(Def. 1) for every natural number n, $it(n) = r \cdot F(n)$.

The functor $-F$ yielding a sequence of partial functions from X into $\overline{\mathbb{R}}$ is defined by the term

(Def. 2) $(-1) \cdot F$.

Now we state the proposition:

(37) Let us consider a non empty set X, a sequence F of partial functions from X into $\overline{\mathbb{R}}$, and a natural number n. Then $(-F)(n) = -F(n)$.

Let us consider a non empty set X, a sequence F of partial functions from X into $\overline{\mathbb{R}}$, and an element x of X. Now we state the propositions:

(38) $(-F)\#x = -F\#x$. The theorem is a consequence of (37).

(39) (i) $F\#x$ is convergent to $+\infty$ iff $(-F)\#x$ is convergent to $-\infty$, and

(ii) $F\#x$ is convergent to $-\infty$ iff $(-F)\#x$ is convergent to $+\infty$, and

(iii) $F\#x$ is convergent to a finite limit iff $(-F)\#x$ is convergent to a finite limit, and

(iv) $F\#x$ is convergent iff $(-F)\#x$ is convergent, and

(v) if $F\#x$ is convergent, then $\lim((-F)\#x) = -\lim(F\#x)$.

The theorem is a consequence of (38).

Let us consider a non empty set X and a sequence F of partial functions from X into $\overline{\mathbb{R}}$. Now we state the propositions:

(40) If F has the same dom, then $-F$ has the same dom. The theorem is a consequence of (37).

(41) If F is additive, then $-F$ is additive. The theorem is a consequence of (37).

(42) Let us consider a non empty set X, a sequence F of partial functions from X into $\overline{\mathbb{R}}$, and a natural number n. Then $(\sum_{\alpha=0}^{\kappa}(-F)(\alpha))_{\kappa\in\mathbb{N}}(n) = (-(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}})(n)$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (\sum_{\alpha=0}^{\kappa}(-F)(\alpha))_{\kappa\in\mathbb{N}}(\$_1) = (-(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}})(\$_1)$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(43) Let us consider a sequence s of extended reals, and a natural number n. Then $(\sum_{\alpha=0}^{\kappa}(-s)(\alpha))_{\kappa\in\mathbb{N}}(n) = -(\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}(n)$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (\sum_{\alpha=0}^{\kappa}(-s)(\alpha))_{\kappa\in\mathbb{N}}(\$_1) = -(\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}(\$_1)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

Let us consider a sequence s of extended reals. Now we state the propositions:

(44) $(\sum_{\alpha=0}^{\kappa}(-s)(\alpha))_{\kappa\in\mathbb{N}} = -(\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}$. The theorem is a consequence of (43).

(45) If s is summable, then $-s$ is summable. The theorem is a consequence of (44).

Let us consider a non empty set X and a sequence F of partial functions from X into $\overline{\mathbb{R}}$. Now we state the propositions:

(46) If for every natural number n, $F(n)$ is without $+\infty$, then F is additive.

(47) If for every natural number n, $F(n)$ is without $-\infty$, then F is additive.

(48) Let us consider a non empty set X, a sequence F of partial functions from X into $\overline{\mathbb{R}}$, and an element x of X. Suppose $F\#x$ is summable. Then

(i) $(-F)\#x$ is summable, and

(ii) $\sum((-F)\#x) = -\sum(F\#x)$.

The theorem is a consequence of (45), (38), and (44).

(49) Let us consider a non empty set X, a σ-field S of subsets of X, and a sequence F of partial functions from X into $\overline{\mathbb{R}}$. Suppose F is additive and has the same dom and for every element x of X such that $x \in \mathrm{dom}(F(0))$ holds $F\#x$ is summable. Then $\lim(\sum_{\alpha=0}^{\kappa}(-F)(\alpha))_{\kappa\in\mathbb{N}} = -\lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}$.
Proof: Set $G = -F$. For every element n of $\mathbb{N}$, $(\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}}(n) = (-(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}})(n)$. For every element x of X such that $x \in \mathrm{dom}\lim (\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}}$ holds $(\lim(\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}})(x) = (-\lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}})(x)$. □

(50) Let us consider a non empty set X, a σ-field S of subsets of X, sequences F, G of partial functions from X into $\overline{\mathbb{R}}$, and an element E of S. Suppose $E \subseteq \mathrm{dom}(F(0))$ and F is additive and has the same dom and for every natural number n, $G(n) = F(n)\restriction E$. Then $\lim(\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}} = \lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\restriction E$.
Proof: For every element x of X such that $x \in E$ holds $F\#x = G\#x$. Set $P_1 = (\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}$. Set $P_2 = (\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}}$. For every element x of X such that $x \in \mathrm{dom}\lim P_2$ holds $(\lim P_2)(x) = (\lim P_1)(x)$. For every element x of X such that $x \in \mathrm{dom}(\lim P_2\restriction E)$ holds $(\lim P_2\restriction E)(x) = (\lim P_1\restriction E)(x)$. □

2. Integral of Non Positive Measurable Functions

Now we state the propositions:

(51) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, and a non-negative partial function f from X to $\overline{\mathbb{R}}$. Then $\int' \max_{-}(-f)\,\mathrm{d}M = \int' f\,\mathrm{d}M$. The theorem is a consequence of (32), (36), and (35).

(52) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a partial function f from X to $\overline{\mathbb{R}}$, and an element A of S.

Suppose $A = \mathrm{dom}\, f$ and f is measurable on A. Then $\int -f \,\mathrm{d}M = -\int f \,\mathrm{d}M$. The theorem is a consequence of (36), (10), (5), and (34).

(53) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a non-negative partial function f from X to $\overline{\mathbb{R}}$, and an element E of S. Suppose $E = \mathrm{dom}\, f$ and f is measurable on E. Then

(i) $\int \max_-(f) \,\mathrm{d}M = 0$, and

(ii) $\int^+ \max_-(f) \,\mathrm{d}M = 0$.

Proof: $\max_-(f)$ is measurable on E. For every object x such that $x \in \mathrm{dom}\max_-(f)$ holds $(\max_-(f))(x) = 0$. $\square$

Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a partial function f from X to $\overline{\mathbb{R}}$, and an element E of S. Now we state the propositions:

(54) If $E = \mathrm{dom}\, f$ and f is measurable on E, then $\int f \,\mathrm{d}M = \int \max_+(f) \,\mathrm{d}M - \int \max_-(f) \,\mathrm{d}M$. The theorem is a consequence of (10) and (5).

(55) If $E \subseteq \mathrm{dom}\, f$ and f is measurable on E, then $\int (-f)\restriction E \,\mathrm{d}M = -\int f\restriction E \,\mathrm{d}M$. The theorem is a consequence of (3) and (52).

(56) Let us consider a non empty set X, a σ-field S of subsets of X, and a partial function f from X to $\overline{\mathbb{R}}$. Suppose there exists an element A of S such that $A = \mathrm{dom}\, f$ and f is measurable on A and (f **qua** extended real-valued function) is non-positive. Then there exists a sequence F of partial functions from X into $\overline{\mathbb{R}}$ such that

(i) for every natural number n, $F(n)$ is simple function in S and $\mathrm{dom}(F(n)) = \mathrm{dom}\, f$, and

(ii) for every natural number n, $F(n)$ is non-positive, and

(iii) for every natural numbers n, m such that $n \leqslant m$ for every element x of X such that $x \in \mathrm{dom}\, f$ holds $F(n)(x) \geqslant F(m)(x)$, and

(iv) for every element x of X such that $x \in \mathrm{dom}\, f$ holds $F\#x$ is convergent and $\lim(F\#x) = f(x)$.

The theorem is a consequence of (37), (30), and (39).

(57) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, an element E of S, and a non-positive partial function f from X to $\overline{\mathbb{R}}$. Suppose there exists an element A of S such that $A = \mathrm{dom}\, f$ and f is measurable on A. Then

(i) $\int f \,\mathrm{d}M = -\int^+ \max_-(f) \,\mathrm{d}M$, and

(ii) $\int f \,\mathrm{d}M = -\int^+ -f \,\mathrm{d}M$, and

(iii) $\int f \,\mathrm{d}M = -\int -f \,\mathrm{d}M$.

PROOF: Consider A being an element of S such that $A = \mathrm{dom}\, f$ and f is measurable on A. $f = -\max_-(f)$. $-f = \max_-(f)$. For every element x of X such that $x \in \mathrm{dom}\max_+(f)$ holds $(\max_+(f))(x) = 0$. □

(58) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, and a non-positive partial function f from X to $\overline{\mathbb{R}}$. Suppose f is simple function in S. Then

(i) $\int f \,\mathrm{d}M = -\int' -f \,\mathrm{d}M$, and

(ii) $\int f \,\mathrm{d}M = -\int' \max_-(f) \,\mathrm{d}M$.

The theorem is a consequence of (30), (57), (32), and (36).

Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a partial function f from X to $\overline{\mathbb{R}}$, and a real number c. Now we state the propositions:

(59) If f is simple function in S and f is non-negative, then $\int c \cdot f \,\mathrm{d}M = c \cdot \int' f \,\mathrm{d}M$.

(60) Suppose f is simple function in S and f is non-positive. Then

(i) $\int c \cdot f \,\mathrm{d}M = -c \cdot \int' -f \,\mathrm{d}M$, and

(ii) $\int c \cdot f \,\mathrm{d}M = -(c \cdot \int' -f \,\mathrm{d}M)$.

The theorem is a consequence of (35), (30), and (59).

(61) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, and a partial function f from X to $\overline{\mathbb{R}}$. Suppose there exists an element A of S such that $A = \mathrm{dom}\, f$ and f is measurable on A and f is non-positive. Then $0 \geqslant \int f \,\mathrm{d}M$. The theorem is a consequence of (57).

(62) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a partial function f from X to $\overline{\mathbb{R}}$, and elements A, B, E of S. Suppose $E = \mathrm{dom}\, f$ and f is measurable on E and f is non-positive and A misses B. Then $\int f \restriction (A \cup B) \,\mathrm{d}M = \int f \restriction A \,\mathrm{d}M + \int f \restriction B \,\mathrm{d}M$. The theorem is a consequence of (3) and (52).

(63) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a partial function f from X to $\overline{\mathbb{R}}$, and elements A, E of S. Suppose $E = \mathrm{dom}\, f$ and f is measurable on E and f is non-positive. Then $0 \geqslant \int f \restriction A \,\mathrm{d}M$. The theorem is a consequence of (61) and (1).

(64) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a partial function f from X to $\overline{\mathbb{R}}$, and elements A, B, E of S. Suppose $E = \mathrm{dom}\, f$ and f is measurable on E and f is non-positive and $A \subseteq B$. Then $\int f \restriction A \,\mathrm{d}M \geqslant \int f \restriction B \,\mathrm{d}M$. The theorem is a consequence of (3) and (52).

3. Convergence Theorems for Non Positive Function's Integration

Now we state the propositions:

(65) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, an element E of S, and a partial function f from X to $\overline{\mathbb{R}}$. Suppose $E = \operatorname{dom} f$ and f is measurable on E and f is non-positive and $M(E \cap \text{EQ-dom}(f, -\infty)) \neq 0$. Then $\int f \, \mathrm{d}M = -\infty$. The theorem is a consequence of (9) and (52).

(66) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, an element E of S, and partial functions f, g from X to $\overline{\mathbb{R}}$. Suppose $E \subseteq \operatorname{dom} f$ and $E \subseteq \operatorname{dom} g$ and f is measurable on E and g is measurable on E and f is non-positive and for every element x of X such that $x \in E$ holds $g(x) \leqslant f(x)$. Then $\int g \restriction E \, \mathrm{d}M \leqslant \int f \restriction E \, \mathrm{d}M$. The theorem is a consequence of (3) and (52).

(67) Let us consider a non empty set X, a sequence F of partial functions from X into $\overline{\mathbb{R}}$, a σ-field S of subsets of X, an element E of S, and a natural number m. Suppose F has the same dom and $E = \operatorname{dom}(F(0))$ and for every natural number n, $F(n)$ is measurable on E and $F(n)$ is without $+\infty$. Then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(m)$ is measurable on E. The theorem is a consequence of (37), (42), and (46).

(68) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a sequence F of partial functions from X into $\overline{\mathbb{R}}$, an element E of S, a sequence I of extended reals, and a natural number m. Suppose $E = \operatorname{dom}(F(0))$ and F is additive and has the same dom and for every natural number n, $F(n)$ is measurable on E and $F(n)$ is non-positive and $I(n) = \int F(n) \, \mathrm{d}M$. Then $\int (\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(m) \, \mathrm{d}M = (\sum_{\alpha=0}^{\kappa} I(\alpha))_{\kappa \in \mathbb{N}}(m)$.

Proof: Set $G = -F$. Set $J = -I$. $G(0) = -F(0)$. G has the same dom. For every natural number n, $F(n)$ is measurable on E and $F(n)$ is without $+\infty$. For every natural number n, $G(n)$ is measurable on E and $G(n)$ is non-negative and $J(n) = \int G(n) \, \mathrm{d}M$. $\int (\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa \in \mathbb{N}}(m) \, \mathrm{d}M = (\sum_{\alpha=0}^{\kappa} J(\alpha))_{\kappa \in \mathbb{N}}(m)$. $\int (-(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}})(m) \, \mathrm{d}M = (\sum_{\alpha=0}^{\kappa} J(\alpha))_{\kappa \in \mathbb{N}}(m)$.
$\int (-(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}})(m) \, \mathrm{d}M = -(\sum_{\alpha=0}^{\kappa} I(\alpha))_{\kappa \in \mathbb{N}}(m)$.
$\int -(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(m) \, \mathrm{d}M = -(\sum_{\alpha=0}^{\kappa} I(\alpha))_{\kappa \in \mathbb{N}}(m)$.
$-\int (\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(m) \, \mathrm{d}M = -(\sum_{\alpha=0}^{\kappa} I(\alpha))_{\kappa \in \mathbb{N}}(m)$. □

(69) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a sequence F of partial functions from X into $\overline{\mathbb{R}}$, an element E of S, and a partial function f from X to $\overline{\mathbb{R}}$. Suppose $E \subseteq \operatorname{dom} f$ and f is non-positive and f is measurable on E and for every natural

number n, $F(n)$ is simple function in S and $F(n)$ is non-positive and $E \subseteq \mathrm{dom}(F(n))$ and for every element x of X such that $x \in E$ holds $F\#x$ is summable and $f(x) = \sum(F\#x)$. Then there exists a sequence I of extended reals such that

(i) for every natural number n, $I(n) = \int F(n){\restriction}E \,\mathrm{d}M$, and

(ii) I is summable, and

(iii) $\int f{\restriction}E \,\mathrm{d}M = \sum I$.

PROOF: Set $g = -f$. Set $G = -F$. G is additive. For every natural number n, $G(n)$ is simple function in S and $G(n)$ is non-negative and $E \subseteq \mathrm{dom}(G(n))$. For every element x of X such that $x \in E$ holds $G\#x$ is summable and $g(x) = \sum(G\#x)$. Consider J being a sequence of extended reals such that for every natural number n, $J(n) = \int G(n){\restriction}E \,\mathrm{d}M$ and J is summable and $\int g{\restriction}E \,\mathrm{d}M = \sum J$. For every natural number n, $I(n) = \int F(n){\restriction}E \,\mathrm{d}M$. $\int g{\restriction}E \,\mathrm{d}M = -\int f{\restriction}E \,\mathrm{d}M$. $\lim(\sum_{\alpha=0}^{\kappa} I(\alpha))_{\kappa\in\mathbb{N}} = -\int g{\restriction}E \,\mathrm{d}M$. □

(70) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, an element E of S, and a partial function f from X to $\overline{\mathbb{R}}$. Suppose $E \subseteq \mathrm{dom}\, f$ and f is non-positive and f is measurable on E. Then there exists a sequence F of partial functions from X into $\overline{\mathbb{R}}$ such that

(i) F is additive, and

(ii) for every natural number n, $F(n)$ is simple function in S and $F(n)$ is non-positive and $F(n)$ is measurable on E, and

(iii) for every element x of X such that $x \in E$ holds $F\#x$ is summable and $f(x) = \sum(F\#x)$, and

(iv) there exists a sequence I of extended reals such that for every natural number n, $I(n) = \int F(n){\restriction}E \,\mathrm{d}M$ and I is summable and $\int f{\restriction}E \,\mathrm{d}M = \sum I$.

PROOF: Set $g = -f$. Consider G being a sequence of partial functions from X into $\overline{\mathbb{R}}$ such that G is additive and for every natural number n, $G(n)$ is simple function in S and $G(n)$ is non-negative and $G(n)$ is measurable on E and for every element x of X such that $x \in E$ holds $G\#x$ is summable and $g(x) = \sum(G\#x)$ and there exists a sequence J of extended reals such that for every natural number n, $J(n) = \int G(n){\restriction}E \,\mathrm{d}M$ and J is summable and $\int g{\restriction}E \,\mathrm{d}M = \sum J$. For every natural number n, $F(n)$ is simple function in S and $F(n)$ is non-positive and $F(n)$ is measurable on E. For every element x of X such that $x \in E$ holds $F\#x$ is summable and $f(x) = \sum(F\#x)$. There exists a sequence I of extended reals such that for every natural number n, $I(n) = \int F(n){\restriction}E\,\mathrm{d}M$ and I is summable and $\int f{\restriction}E\,\mathrm{d}M = \sum I$. □

Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a sequence F of partial functions from X into $\overline{\mathbb{R}}$, and an element E of S. Now we state the propositions:

(71) Suppose $E = \mathrm{dom}(F(0))$ and F has the same dom and for every natural number n, $F(n)$ is non-positive and $F(n)$ is measurable on E. Then there exists a sequence F_1 of $(X \dot{\rightarrow} \overline{\mathbb{R}})^{\mathbb{N}}$ such that for every natural number n, for every natural number m, $F_1(n)(m)$ is simple function in S and $\mathrm{dom}(F_1(n)(m)) = \mathrm{dom}(F(n))$ and for every natural number m, $F_1(n)(m)$ is non-positive and for every natural numbers j, k such that $j \leqslant k$ for every element x of X such that $x \in \mathrm{dom}(F(n))$ holds $F_1(n)(j)(x) \geqslant F_1(n)(k)(x)$ and for every element x of X such that $x \in \mathrm{dom}(F(n))$ holds $F_1(n)\#x$ is convergent and $\lim(F_1(n)\#x) = F(n)(x)$.

Proof: Define $\mathcal{Q}[\text{element of } \mathbb{N}, \text{set}] \equiv$ for every sequence G of partial functions from X into $\overline{\mathbb{R}}$ such that $\$_2 = G$ holds for every natural number m, $G(m)$ is simple function in S and $\mathrm{dom}(G(m)) = \mathrm{dom}(F(\$_1))$ and for every natural number m, $G(m)$ is non-positive and for every natural numbers j, k such that $j \leqslant k$ for every element x of X such that $x \in \mathrm{dom}(F(\$_1))$ holds $G(j)(x) \geqslant G(k)(x)$ and for every element x of X such that $x \in \mathrm{dom}(F(\$_1))$ holds $G\#x$ is convergent and $\lim(G\#x) = F(\$_1)(x)$. For every element n of $\mathbb{N}$, there exists a sequence G of partial functions from X into $\overline{\mathbb{R}}$ such that for every natural number m, $G(m)$ is simple function in S and $\mathrm{dom}(G(m)) = \mathrm{dom}(F(n))$ and for every natural number m, $G(m)$ is non-positive and for every natural numbers j, k such that $j \leqslant k$ for every element x of X such that $x \in \mathrm{dom}(F(n))$ holds $G(j)(x) \geqslant G(k)(x)$ and for every element x of X such that $x \in \mathrm{dom}(F(n))$ holds $G\#x$ is convergent and $\lim(G\#x) = F(n)(x)$. For every element n of $\mathbb{N}$, there exists an element G of $(X \dot{\rightarrow} \overline{\mathbb{R}})^{\mathbb{N}}$ such that $\mathcal{Q}[n, G]$. Consider F_1 being a sequence of $(X \dot{\rightarrow} \overline{\mathbb{R}})^{\mathbb{N}}$ such that for every element n of $\mathbb{N}$, $\mathcal{Q}[n, F_1(n)]$. For every natural number n, for every natural number m, $F_1(n)(m)$ is simple function in S and $\mathrm{dom}(F_1(n)(m)) = \mathrm{dom}(F(n))$ and for every natural number m, $F_1(n)(m)$ is non-positive and for every natural numbers j, k such that $j \leqslant k$ for every element x of X such that $x \in \mathrm{dom}(F(n))$ holds $F_1(n)(j)(x) \geqslant F_1(n)(k)(x)$ and for every element x of X such that $x \in \mathrm{dom}(F(n))$ holds $F_1(n)\#x$ is convergent and $\lim(F_1(n)\#x) = F(n)(x)$. □

(72) Suppose $E = \mathrm{dom}(F(0))$ and F is additive and has the same dom and for every natural number n, $F(n)$ is measurable on E and $F(n)$ is non-positive. Then there exists a sequence I of extended reals such that for every natural number n, $I(n) = \int F(n)\,\mathrm{d}M$ and $\int (\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(n)\,\mathrm{d}M =$

$(\sum_{\alpha=0}^{\kappa} I(\alpha))_{\kappa\in\mathbb{N}}(n)$.

PROOF: Set $G = -F$. $G(0) = -F(0)$. G has the same dom. For every natural number n, $G(n)$ is measurable on E and $G(n)$ is non-negative. Consider J being a sequence of extended reals such that for every natural number n, $J(n) = \int G(n)\,\mathrm{d}M$ and $\int (\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}}(n)\,\mathrm{d}M = (\sum_{\alpha=0}^{\kappa} J(\alpha))_{\kappa\in\mathbb{N}}(n)$. For every natural number n, $F(n)$ is measurable on E and $F(n)$ is without $+\infty$. □

(73) Suppose $E \subseteq \mathrm{dom}(F(0))$ and F is additive and has the same dom and for every natural number n, $F(n)$ is non-positive and $F(n)$ is measurable on E and for every element x of X such that $x \in E$ holds $F\#x$ is summable. Then there exists a sequence I of extended reals such that

(i) for every natural number n, $I(n) = \int F(n)\restriction E\,\mathrm{d}M$, and

(ii) I is summable, and

(iii) $\int \lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\restriction E\,\mathrm{d}M = \sum I$.

PROOF: Set $G = -F$. $G(0) = -F(0)$. G is additive. G has the same dom. For every natural number n, $G(n)$ is non-negative and $G(n)$ is measurable on E. For every element x of X such that $x \in E$ holds $G\#x$ is summable. Consider J being a sequence of extended reals such that for every natural number n, $J(n) = \int G(n)\restriction E\,\mathrm{d}M$ and J is summable and $\int \lim(\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}}\restriction E\,\mathrm{d}M = \sum J$. For every natural number n, $I(n) = \int F(n)\restriction E\,\mathrm{d}M$. Define $\mathcal{H}(\text{natural number}) = F(\$_1)\restriction E$. Consider H being a sequence of partial functions from X into $\overline{\mathbb{R}}$ such that for every natural number n, $H(n) = \mathcal{H}(n)$. $\lim(\sum_{\alpha=0}^{\kappa} H(\alpha))_{\kappa\in\mathbb{N}} = \lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa\in\mathbb{N}}\restriction E$. Define $\mathcal{K}(\text{natural number}) = G(\$_1)\restriction E$. Consider K being a sequence of partial functions from X into $\overline{\mathbb{R}}$ such that for every natural number n, $K(n) = \mathcal{K}(n)$. $\lim(\sum_{\alpha=0}^{\kappa} K(\alpha))_{\kappa\in\mathbb{N}} = \lim(\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}}\restriction E$. For every element n of $\mathbb{N}$, $H(n) = (-K)(n)$. $\lim(\sum_{\alpha=0}^{\kappa} H(\alpha))_{\kappa\in\mathbb{N}} = -\lim(\sum_{\alpha=0}^{\kappa} K(\alpha))_{\kappa\in\mathbb{N}}$. For every natural number n, $K(n)$ is measurable on E and $K(n)$ is without $-\infty$. $\int(-\lim(\sum_{\alpha=0}^{\kappa} K(\alpha))_{\kappa\in\mathbb{N}})\restriction E\,\mathrm{d}M = -\int \lim(\sum_{\alpha=0}^{\kappa} K(\alpha))_{\kappa\in\mathbb{N}}\restriction E\,\mathrm{d}M$. □

(74) Suppose $E = \mathrm{dom}(F(0))$ and $F(0)$ is non-positive and F has the same dom and for every natural number n, $F(n)$ is measurable on E and for every natural numbers n, m such that $n \leqslant m$ for every element x of X such that $x \in E$ holds $F(n)(x) \geqslant F(m)(x)$ and for every element x of X such that $x \in E$ holds $F\#x$ is convergent. Then there exists a sequence I of extended reals such that

(i) for every natural number n, $I(n) = \int F(n)\,\mathrm{d}M$, and

(ii) I is convergent, and

(iii) $\int \lim F \, \mathrm{d}M = \lim I$.

Proof: Set $G = -F$. $G(0) = -F(0)$. For every natural number n, $G(n)$ is measurable on E by [4, (63)], (37). For every natural numbers n, m such that $n \leqslant m$ for every element x of X such that $x \in E$ holds $G(n)(x) \leqslant G(m)(x)$. For every element x of X such that $x \in E$ holds $G\#x$ is convergent. Consider J being a sequence of extended reals such that for every natural number n, $J(n) = \int G(n) \, \mathrm{d}M$ and J is convergent and $\int \lim G \, \mathrm{d}M = \lim J$. Set $I = -J$. For every natural number n, $I(n) = \int F(n) \, \mathrm{d}M$. For every element x of X such that $x \in \operatorname{dom} \lim G$ holds $(\lim G)(x) = (-\lim F)(x)$ by (38), [3, (17)]. $\int \lim G \, \mathrm{d}M = -\int \lim F \, \mathrm{d}M$. □

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] Vladimir Igorevich Bogachev and Maria Aparecida Soares Ruas. *Measure theory*, volume 1. Springer, 2007.

[3] Noboru Endou. Extended real-valued double sequence and its convergence. *Formalized Mathematics*, 23(**3**):253–277, 2015. doi:10.1515/forma-2015-0021.

[4] Noboru Endou. Fubini's theorem on measure. *Formalized Mathematics*, 25(**1**):1–29, 2017. doi:10.1515/forma-2017-0001.

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

[6] 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.

[7] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[8] P. R. Halmos. *Measure Theory*. Springer-Verlag, 1974.

Received September 3, 2017

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.

FORMALIZED MATHEMATICS
Vol. 25, No. 3, Pages 241–248, 2017
DOI: 10.1515/forma-2017-0023

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

Formal Introduction to Fuzzy Implications

Adam Grabowski
Institute of Informatics
University of Białystok
Poland

Summary. In the article we present in the Mizar system the catalogue of nine basic fuzzy implications, used especially in the theory of fuzzy sets. This work is a continuation of the development of fuzzy sets in Mizar; it could be used to give a variety of more general operations, and also it could be a good starting point towards the formalization of fuzzy logic (together with t-norms and t-conorms, formalized previously).

MSC: 03B52 68T37 03B35

Keywords: fuzzy implication; fuzzy set; fuzzy logic

MML identifier: FUZIMPL1, version: 8.1.06 5.44.1305

0. Introduction

As it is well known, the implication operator plays a crucial role in the classical two-valued logic. Based on this logical connective, we can define binary conjunction and disjunction, and also unary negation operator. In the field of fuzzy logic, the notions of t-norm and t-conorm are an abstraction of the classical conjunction and disjunction. Similarly, we can treat the notion of a fuzzy implication, as a generalization of a classical implication.

Fuzzy sets, a tool for modelling uncertainty, proposed by Zadeh [12], were formally introduced in Mizar in [10]. This approach is quite natural in the Mizar Mathematical Library [9], has rich continuation there [3] as it is significantly closer to set theory than another tool for doing so, namely rough sets by Pawlak [11], as recalled in the context of lattice theory in [5].

In order to cope with basic constructions present in the theory of fuzzy implications, we had to define a number of examples of binary connectives. It is

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

especially important to have some, because taking into account the expressive power of registrations of clusters in the Mizar system and the role of attributes, most of theorems are stated in the form of the abovementioned registrations. Having prepared such formal background, properties can be calculated automatically via the mechanism of the type expansion.

In our formal approach, we follow closely the book [1].

A function $I : [0,1]^2 \to [0,1]$ is called a fuzzy implication if it satisfies, for all $x, x_1, x_2, y_1, y_2 \in [0,1]$, the following conditions:

$$\text{if } x_1 \leqslant x_2, \text{ then } I(x_1, y) \geqslant I(x_2, y), \tag{I3}$$

$$\text{if } y_1 \leqslant y_2, \text{ then } I(x, y_1) \leqslant I(x, y_2), \tag{I4}$$

$$I(0,0) = 1, \tag{I5}$$

$$I(1,1) = 1, \tag{I6}$$

$$I(1,0) = 0. \tag{I7}$$

The functions satisfying equations (I3), (I4), and (I5) are called in our formalism, `00-dominant` (Def. 3), `11-dominant` (Def. 4), and `10-weak` (Def. 5), respectively.

The mutual independence of the axioms was shown using I_{-1}, I_{-2}, I_{-3}, I_{-4}, I_{-5} (see definitions Def. 9 – Def. 13 in the present paper) – each one violating exactly one among properties (I1) – (I5). Of course, these are not examples of fuzzy implications in the current setting, although Zadeh implication I_{-1} is considered in the literature as multi-valued implication.

In the set of all fuzzy implications, denoted by $\mathcal{FI}$, we have I_0 and I_1 as the least and the greatest elements (with the ordinary pointwise ordering of functions) for arbitrary $x, y \in [0,1]$ as

$$I_0(x,y) = \begin{cases} 1, & \text{if } x = 0 \text{ or } y = 1 \\ 0, & \text{otherwise} \end{cases}$$

$$I_1(x,y) = \begin{cases} 1, & \text{if } x < 1 \text{ or } y > 0 \\ 0, & \text{otherwise} \end{cases}$$

Together with formal description of triangular norms and conorms (introduced in [2] and described in [7]) introducing fuzzy implications is the fundamental step towards defining fuzzy logic within the Mizar Mathematical Library. Both formal aproaches to the theory of rough and fuzzy sets could be compared in a more sophisticated way as initiated in [8]. Of course, the Mizar system is much more efficient in the logical reasoning than in calculations in the style of computer algebra systems (although in the field of rough sets it resulted in a number

Table 0.1: Nine basic fuzzy implications ([1], p. 4)

Name	Def.	Defining formula
Łukasiewicz	Def. 14	$I_{\mathrm{LK}}(x,y) = \min(1, 1-x+y)$
Gödel	Def. 16	$I_{\mathrm{GD}}(x,y) = \begin{cases} 1, & \text{if } x \leqslant y \\ y, & \text{otherwise} \end{cases}$
Reichenbach	Def. 17	$I_{\mathrm{RC}}(x,y) = 1 - x + xy$
Kleene-Dienes	Def. 18	$I_{\mathrm{KD}}(x,y) = \max(1-x, y)$
Goguen	Def. 19	$I_{\mathrm{GG}}(x,y) = \begin{cases} 1, & \text{if } x \leqslant y \\ \frac{y}{x}, & \text{otherwise} \end{cases}$
Rescher	Def. 20	$I_{\mathrm{RS}}(x,y) = \begin{cases} 1, & \text{if } x \leqslant y \\ 0, & \text{if } x > y \end{cases}$
Yager	Def. 21	$I_{\mathrm{YG}}(x,y) = \begin{cases} 1, & \text{if } x = 0 \text{ and } y = 0 \\ y^x, & \text{if } x > 0 \text{ or } y > 0 \end{cases}$
Weber	Def. 22	$I_{\mathrm{WB}}(x,y) = \begin{cases} 1, & \text{if } x < 1 \\ y, & \text{if } x = 1 \end{cases}$
Fodor	Def. 23	$I_{\mathrm{FD}}(x,y) = \begin{cases} 1, & \text{if } x \leqslant y \\ \max(1-x, y), & \text{if } x > y \end{cases}$

of quite interesting observations [6]), hence formalizing fuzzy numbers [4] is less promising than the present one.

The main aim of the Mizar article was to introduce formally nine important examples of fuzzy implications (see Table 0.1).

1. Preliminaries

Let us consider elements a, b of $[0,1]$. Now we state the propositions:

(1) $\max(b, \min(1-a, 1-b)) \in [0,1]$.

(2) $\min(1, 1-a+b) \in [0,1]$.

(3) $1 - a + (a \cdot b) \in [0,1]$.

(4) $\max(1-a, b) \in [0,1]$.

(5) If $a > 0$ or $b > 0$, then $b^a \in [0,1]$.

(6) If $a > b$, then $\frac{b}{a} \in [0,1]$.

2. Basic Attributes Defining Fuzzy Implications

Let f be a binary operation on $[0, 1]$. We say that f is antitone w.r.t. 1st coordinate if and only if

(Def. 1) for every elements x_1, x_2, y of $[0, 1]$ such that $x_1 \leqslant x_2$ holds $f(x_1, y) \geqslant f(x_2, y)$.

We say that f is isotone w.r.t. 2nd coordinate if and only if

(Def. 2) for every elements x, y_1, y_2 of $[0, 1]$ such that $y_1 \leqslant y_2$ holds $f(x, y_1) \leqslant f(x, y_2)$.

We say that f is 00-dominant if and only if

(Def. 3) $f(0, 0) = 1$.

We say that f is 11-dominant if and only if

(Def. 4) $f(1, 1) = 1$.

We say that f is 10-weak if and only if

(Def. 5) $f(1, 0) = 0$.

We say that f is 01-dominant if and only if

(Def. 6) $f(0, 1) = 1$.

We say that f has properties of a fuzzy implication if and only if

(Def. 7) f is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

We say that f has properties of a classical implication if and only if

(Def. 8) f is 00-dominant, 01-dominant, 11-dominant, and 10-weak.

3. Examples Showing Independence of Axioms

The functor I_{-1} yielding a binary operation on $[0, 1]$ is defined by

(Def. 9) for every elements x, y of $[0, 1]$, $it(x, y) = \max(1 - x, \min(x, y))$.

One can verify that I_{-1} is isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

The functor I_{-2} yielding a binary operation on $[0, 1]$ is defined by

(Def. 10) for every elements x, y of $[0, 1]$, $it(x, y) = \max(y, \min(1 - x, 1 - y))$.

Let us note that I_{-2} is antitone w.r.t. 1st coordinate, 00-dominant, 11-dominant, and 10-weak.

The functor I_{-3} yielding a binary operation on $[0, 1]$ is defined by

(Def. 11) for every elements x, y of $[0, 1]$, if $y < 1$, then $it(x, y) = 0$ and if $y = 1$, then $it(x, y) = 1$.

Let us observe that I_{-3} is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, non 00-dominant, 11-dominant, and 10-weak.

The functor I_{-4} yielding a binary operation on $[0,1]$ is defined by

(Def. 12) for every elements x, y of $[0,1]$, if $x = 0$, then $it(x,y) = 1$ and if $x > 0$, then $it(x,y) = 0$.

Observe that I_{-4} is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, non 11-dominant, and 10-weak.

The functor I_{-5} yielding a binary operation on $[0,1]$ is defined by

(Def. 13) for every elements x, y of $[0,1]$, $it(x,y) = 1$.

Observe that I_{-5} is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and non 10-weak.

4. Catalogue of Fuzzy Implications

The Łukasiewicz implication yielding a binary operation on $[0,1]$ is defined by

(Def. 14) for every elements x, y of $[0,1]$, $it(x,y) = \min(1, 1 - x + y)$.

Note that the Łukasiewicz implication is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak and there exists a binary operation on $[0,1]$ which has properties of a fuzzy implication and every binary operation on $[0,1]$ which has properties of a fuzzy implication is also antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, 10-weak.

Every binary operation on $[0,1]$ which is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 01-dominant, 11-dominant, and 10-weak has also properties of a fuzzy implication and every binary operation on $[0,1]$ which has properties of a classical implication is also 00-dominant, 01-dominant, 11-dominant, 10-weak.

Every binary operation on $[0,1]$ which is 00-dominant, 01-dominant, 11-dominant, and 10-weak has also properties of a classical implication and every binary operation on $[0,1]$ which has properties of a fuzzy implication has also properties of a classical implication.

A fuzzy implication is an antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, 10-weak binary operation on $[0,1]$. The functor $\mathcal{FI}$ yielding a set is defined by the term

(Def. 15) the set of all f where f is a fuzzy implication.

The Gödel implication yielding a binary operation on $[0,1]$ is defined by

(Def. 16) for every elements x, y of $[0,1]$, if $x \leqslant y$, then $it(x,y) = 1$ and if $x > y$, then $it(x,y) = y$.

Let us note that the Gödel implication is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

The Reichenbach implication yielding a binary operation on $[0,1]$ is defined by

(Def. 17) for every elements x, y of $[0,1]$, $it(x,y) = 1 - x + (x \cdot y)$.

Let us note that the Reichenbach implication is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

The Kleene-Dienes implication yielding a binary operation on $[0,1]$ is defined by

(Def. 18) for every elements x, y of $[0,1]$, $it(x,y) = \max(1 - x, y)$.

Let us observe that the Kleene-Dienes implication is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

The Goguen implication yielding a binary operation on $[0,1]$ is defined by

(Def. 19) for every elements x, y of $[0,1]$, if $x \leqslant y$, then $it(x,y) = 1$ and if $x > y$, then $it(x,y) = \frac{y}{x}$.

One can verify that the Goguen implication is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

The Rescher implication yielding a binary operation on $[0,1]$ is defined by

(Def. 20) for every elements x, y of $[0,1]$, if $x \leqslant y$, then $it(x,y) = 1$ and if $x > y$, then $it(x,y) = 0$.

Let us note that the Rescher implication is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

The Yager implication yielding a binary operation on $[0,1]$ is defined by

(Def. 21) for every elements x, y of $[0,1]$, if $x = y = 0$, then $it(x,y) = 1$ and if $x > 0$ or $y > 0$, then $it(x,y) = y^x$.

One can check that the Yager implication is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

The Weber implication yielding a binary operation on $[0,1]$ is defined by

(Def. 22) for every elements x, y of $[0,1]$, if $x < 1$, then $it(x,y) = 1$ and if $x = 1$, then $it(x,y) = y$.

Let us note that the Weber implication is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

The Fodor implication yielding a binary operation on $[0,1]$ is defined by

(Def. 23) for every elements x, y of $[0,1]$, if $x \leqslant y$, then $it(x,y) = 1$ and if $x > y$, then $it(x,y) = \max(1 - x, y)$.

One can check that the Fodor implication is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

5. Boundary Fuzzy Implications

The functor I_0 yielding a binary operation on $[0,1]$ is defined by

(Def. 24) for every elements x, y of $[0,1]$, if $x = 0$ or $y = 1$, then $it(x, y) = 1$ and if $x > 0$ and $y < 1$, then $it(x, y) = 0$.

One can verify that I_0 is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

The functor I_1 yielding a binary operation on $[0,1]$ is defined by

(Def. 25) for every elements x, y of $[0,1]$, if $x < 1$ or $y > 0$, then $it(x, y) = 1$ and if $x = 1$ and $y = 0$, then $it(x, y) = 0$.

One can verify that I_1 is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak.

Let f be a binary operation on $[0,1]$. We say that f satisfies (LB) if and only if

(Def. 26) for every element y of $[0,1]$, $f(0, y) = 1$.

We say that f satisfies (RB) if and only if

(Def. 27) for every element x of $[0,1]$, $f(x, 1) = 1$.

Now we state the propositions:

(7) Let us consider a fuzzy implication I, and an element y of $[0,1]$. Then $I(0, y) = 1$.

(8) Let us consider a fuzzy implication I, and an element x of $[0,1]$. Then $I(x, 1) = 1$.

Observe that every fuzzy implication satisfies (LB) and (RB).

Let us consider a fuzzy implication I. Now we state the propositions:

(9) $I_0 \leqslant I$. The theorem is a consequence of (7) and (8).

(10) $I \leqslant I_1$.

References

[1] Michał Baczyński and Balasubramaniam Jayaram. *Fuzzy Implications*. Springer Publishing Company, Incorporated, 2008. doi:10.1007/978-3-540-69082-5.

[2] Adam Grabowski. Basic formal properties of triangular norms and conorms. *Formalized Mathematics*, 25(**2**):93–100, 2017. doi:10.1515/forma-2017-0009.

[3] Adam Grabowski. The formal construction of fuzzy numbers. *Formalized Mathematics*, 22(**4**):321–327, 2014. doi:10.2478/forma-2014-0032.

[4] Adam Grabowski. On the computer certification of fuzzy numbers. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *2013 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Federated Conference on Computer Science and Information Systems, pages 51–54, 2013.

[5] Adam Grabowski. Lattice theory for rough sets – a case study with Mizar. *Fundamenta Informaticae*, 147(2–3):223–240, 2016. doi:10.3233/FI-2016-1406.

[6] Adam Grabowski and Magdalena Jastrzębska. Rough set theory from a math-assistant perspective. In *Rough Sets and Intelligent Systems Paradigms, International Conference, RSEISP 2007, Warsaw, Poland, June 28–30, 2007, Proceedings*, pages 152–161, 2007. doi:10.1007/978-3-540-73451-2_17.

[7] Adam Grabowski and Takashi Mitsuishi. *Extending Formal Fuzzy Sets with Triangular Norms and Conorms*, volume 642: *Advances in Intelligent Systems and Computing*, pages 176–187. Springer International Publishing, Cham, 2018. doi:10.1007/978-3-319-66824-6_16.

[8] Adam Grabowski and Takashi Mitsuishi. Initial comparison of formal approaches to fuzzy and rough sets. In Leszek Rutkowski, Marcin Korytkowski, Rafal Scherer, Ryszard Tadeusiewicz, Lotfi A. Zadeh, and Jacek M. Zurada, editors, *Artificial Intelligence and Soft Computing - 14th International Conference, ICAISC 2015, Zakopane, Poland, June 14-18, 2015, Proceedings, Part I*, volume 9119 of *Lecture Notes in Computer Science*, pages 160–171. Springer, 2015. doi:10.1007/978-3-319-19324-3_15.

[9] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[10] Takashi Mitsuishi, Noboru Endou, and Yasunari Shidama. The concept of fuzzy set and membership function and basic properties of fuzzy set operation. *Formalized Mathematics*, 9(**2**):351–356, 2001.

[11] Zdzisław Pawlak. Rough sets. *International Journal of Parallel Programming*, 11:341–356, 1982. doi:10.1007/BF01001956.

[12] Lotfi Zadeh. Fuzzy sets. *Information and Control*, 8(3):338–353, 1965.

Received September 3, 2017

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.