JOURNAL OF FORMALIZED MATHEMATICS
Volume 12, Released 2000, Published 2003
Inst. of Computer Science, Univ. of Białystok

The Evaluation of Multivariate Polynomials

Christoph Schwarzweller
University of Tübingen

Andrzej Trybulec
University of Białystok

MML Identifier: POLYNOM2.

WWW: http://mizar.org/JFM/Vol12/polynom2.html

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

1. Preliminaries

In this article we present several logical schemes. The scheme *SeqExD* deals with a non empty set $\mathcal{A}$, a natural number $\mathcal{B}$, and a binary predicate $\mathcal{P}$, and states that:

> There exists a finite sequence p of elements of $\mathcal{A}$ such that $\operatorname{dom} p = \operatorname{Seg}\mathcal{B}$ and for every natural number k such that $k \in \operatorname{Seg}\mathcal{B}$ holds $\mathcal{P}[k, p_k]$

provided the parameters have the following property:

- For every natural number k such that $k \in \operatorname{Seg}\mathcal{B}$ there exists an element x of $\mathcal{A}$ such that $\mathcal{P}[k,x]$.

The scheme *FinRecExD2* deals with a non empty set $\mathcal{A}$, an element $\mathcal{B}$ of $\mathcal{A}$, a natural number $\mathcal{C}$, and a ternary predicate $\mathcal{P}$, and states that:

> There exists a finite sequence p of elements of $\mathcal{A}$ such that $\operatorname{len} p = \mathcal{C}$ but $p_1 = \mathcal{B}$ or $\mathcal{C} = 0$ but for every natural number n such that $1 \leq n$ and $n \leq \mathcal{C} - 1$ holds $\mathcal{P}[n, p_n, p_{n+1}]$

provided the parameters have the following property:

- Let n be a natural number. Suppose $1 \leq n$ and $n \leq \mathcal{C} - 1$. Let x be an element of $\mathcal{A}$. Then there exists an element y of $\mathcal{A}$ such that $\mathcal{P}[n,x,y]$.

The scheme *FinRecUnD2* deals with a set $\mathcal{A}$, an element $\mathcal{B}$ of $\mathcal{A}$, a natural number $\mathcal{C}$, finite sequences $\mathcal{D}$, $\mathcal{E}$ of elements of $\mathcal{A}$, and a ternary predicate $\mathcal{P}$, and states that:

> $\mathcal{D} = \mathcal{E}$

provided the following requirements are met:

- Let n be a natural number. Suppose $1 \leq n$ and $n \leq \mathcal{C} - 1$. Let x, y_1, y_2 be elements of $\mathcal{A}$. If $\mathcal{P}[n,x,y_1]$ and $\mathcal{P}[n,x,y_2]$, then $y_1 = y_2$,
- $\operatorname{len}\mathcal{D} = \mathcal{C}$ but $\mathcal{D}_1 = \mathcal{B}$ or $\mathcal{C} = 0$ but for every natural number n such that $1 \leq n$ and $n \leq \mathcal{C} - 1$ holds $\mathcal{P}[n, \mathcal{D}_n, \mathcal{D}_{n+1}]$, and
- $\operatorname{len}\mathcal{E} = \mathcal{C}$ but $\mathcal{E}_1 = \mathcal{B}$ or $\mathcal{C} = 0$ but for every natural number n such that $1 \leq n$ and $n \leq \mathcal{C} - 1$ holds $\mathcal{P}[n, \mathcal{E}_n, \mathcal{E}_{n+1}]$.

The scheme *FinInd* deals with natural numbers $\mathcal{A}$, $\mathcal{B}$ and a unary predicate $\mathcal{P}$, and states that:

> For every natural number i such that $\mathcal{A} \leq i$ and $i \leq \mathcal{B}$ holds $\mathcal{P}[i]$

provided the following requirements are met:

- $\mathcal{P}[\mathcal{A}]$, and
- For every natural number j such that $\mathcal{A} \leq j$ and $j < \mathcal{B}$ holds if $\mathcal{P}[j]$, then $\mathcal{P}[j+1]$.

The scheme *FinInd2* deals with natural numbers $\mathcal{A}$, $\mathcal{B}$ and a unary predicate $\mathcal{P}$, and states that:

For every natural number i such that $\mathcal{A} \leq i$ and $i \leq \mathcal{B}$ holds $\mathcal{P}[i]$

provided the following conditions are satisfied:

- $\mathcal{P}[\mathcal{A}]$, and
- Let j be a natural number. Suppose $\mathcal{A} \leq j$ and $j < \mathcal{B}$. Suppose that for every natural number j' such that $\mathcal{A} \leq j'$ and $j' \leq j$ holds $\mathcal{P}[j']$. Then $\mathcal{P}[j+1]$.

The scheme *IndFinSeq* deals with a set $\mathcal{A}$, a finite sequence $\mathcal{B}$ of elements of $\mathcal{A}$, and a unary predicate $\mathcal{P}$, and states that:

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

provided the following conditions are met:

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

The following propositions are true:

(2)[1] Let L be a unital associative non empty groupoid, a be an element of L, and n, m be natural numbers. Then $\mathrm{power}_L(a, n+m) = \mathrm{power}_L(a, n) \cdot \mathrm{power}_L(a, m)$.

(3) For every well unital non empty double loop structure L holds $\mathbf{1}_L = 1_L$.

Let us observe that there exists a non empty double loop structure which is Abelian, right zeroed, add-associative, right complementable, unital, well unital, distributive, commutative, associative, and non trivial.

2. About Finite Sequences and the Functor SgmX

Next we state a number of propositions:

(4) Let p be a finite sequence and k be a natural number. Suppose $k \in \operatorname{dom} p$. Let i be a natural number. If $1 \leq i$ and $i \leq k$, then $i \in \operatorname{dom} p$.

(5) Let L be a left zeroed right zeroed non empty loop structure, p be a finite sequence of elements of the carrier of L, and i be a natural number. Suppose $i \in \operatorname{dom} p$ and for every natural number i' such that $i' \in \operatorname{dom} p$ and $i' \neq i$ holds $p_{i'} = 0_L$. Then $\sum p = p_i$.

(6) Let L be an add-associative right zeroed right complementable distributive unital non empty double loop structure and p be a finite sequence of elements of the carrier of L. If there exists a natural number i such that $i \in \operatorname{dom} p$ and $p_i = 0_L$, then $\prod p = 0_L$.

(7) Let L be an Abelian add-associative non empty loop structure, a be an element of L, and p, q be finite sequences of elements of the carrier of L. Suppose that

(i) $\operatorname{len} p = \operatorname{len} q$, and

(ii) there exists a natural number i such that $i \in \operatorname{dom} p$ and $q_i = a + p_i$ and for every natural number i' such that $i' \in \operatorname{dom} p$ and $i' \neq i$ holds $q_{i'} = p_{i'}$.

Then $\sum q = a + \sum p$.

(8) Let L be a commutative associative non empty double loop structure, a be an element of L, and p, q be finite sequences of elements of the carrier of L. Suppose that

(i) $\operatorname{len} p = \operatorname{len} q$, and

(ii) there exists a natural number i such that $i \in \operatorname{dom} p$ and $q_i = a \cdot p_i$ and for every natural number i' such that $i' \in \operatorname{dom} p$ and $i' \neq i$ holds $q_{i'} = p_{i'}$.

Then $\prod q = a \cdot \prod p$.

(9) Let X be a set, A be an empty subset of X, and R be an order in X. If R linearly orders A, then $\mathrm{SgmX}(R, A) = \emptyset$.

[1] The proposition (1) has been removed.

(10) Let X be a set, A be a finite subset of X, and R be an order in X. Suppose R linearly orders A. Let i, j be natural numbers. If $i \in \operatorname{dom} \operatorname{SgmX}(R,A)$ and $j \in \operatorname{dom} \operatorname{SgmX}(R,A)$, then if $(\operatorname{SgmX}(R,A))_i = (\operatorname{SgmX}(R,A))_j$, then $i = j$.

(11) Let X be a set, A be a finite subset of X, and a be an element of X. Suppose $a \notin A$. Let B be a finite subset of X. Suppose $B = \{a\} \cup A$. Let R be an order in X. Suppose R linearly orders B. Let k be a natural number. Suppose $k \in \operatorname{dom} \operatorname{SgmX}(R,B)$ and $(\operatorname{SgmX}(R,B))_k = a$. Let i be a natural number. If $1 \leq i$ and $i \leq k-1$, then $(\operatorname{SgmX}(R,B))_i = (\operatorname{SgmX}(R,A))_i$.

(12) Let X be a set, A be a finite subset of X, and a be an element of X. Suppose $a \notin A$. Let B be a finite subset of X. Suppose $B = \{a\} \cup A$. Let R be an order in X. Suppose R linearly orders B. Let k be a natural number. Suppose $k \in \operatorname{dom} \operatorname{SgmX}(R,B)$ and $(\operatorname{SgmX}(R,B))_k = a$. Let i be a natural number. If $k \leq i$ and $i \leq \operatorname{len} \operatorname{SgmX}(R,A)$, then $(\operatorname{SgmX}(R,B))_{i+1} = (\operatorname{SgmX}(R,A))_i$.

(13) Let X be a non empty set, A be a finite subset of X, and a be an element of X. Suppose $a \notin A$. Let B be a finite subset of X. Suppose $B = \{a\} \cup A$. Let R be an order in X. Suppose R linearly orders B. Let k be a natural number. If $k+1 \in \operatorname{dom} \operatorname{SgmX}(R,B)$ and $(\operatorname{SgmX}(R,B))_{k+1} = a$, then $\operatorname{SgmX}(R,B) = \operatorname{Ins}(\operatorname{SgmX}(R,A),k,a)$.

3. Evaluation of Bags

The following proposition is true

(14) For every set X and for every bag b of X such that $\operatorname{support} b = \emptyset$ holds $b = \operatorname{EmptyBag} X$.

Let X be a set and let b be a bag of X. We say that b is empty if and only if:

(Def. 1) $b = \operatorname{EmptyBag} X$.

Let X be a non empty set. Note that there exists a bag of X which is non empty.

Let X be a set and let b be a bag of X. Then $\operatorname{support} b$ is a finite subset of X.

We now state the proposition

(15) For every ordinal number n and for every bag b of n holds $\subseteq_n$ linearly orders $\operatorname{support} b$.

Let X be a set, let x be a finite sequence of elements of X, and let b be a bag of X. Then $b \cdot x$ is a partial function from $\mathbb{N}$ to $\mathbb{N}$.

Let n be an ordinal number, let b be a bag of n, let L be a non trivial unital non empty double loop structure, and let x be a function from n into L. The functor $\operatorname{eval}(b,x)$ yields an element of L and is defined by the condition (Def. 2).

(Def. 2) There exists a finite sequence y of elements of the carrier of L such that $\operatorname{len} y = \operatorname{len} \operatorname{SgmX}(\subseteq_n, \operatorname{support} b)$ and $\operatorname{eval}(b,x) = \prod y$ and for every natural number i such that $1 \leq i$ and $i \leq \operatorname{len} y$ holds $y_i = \operatorname{power}_L((x \cdot \operatorname{SgmX}(\subseteq_n, \operatorname{support} b))_i, (b \cdot \operatorname{SgmX}(\subseteq_n, \operatorname{support} b))_i)$.

We now state three propositions:

(16) Let n be an ordinal number, L be a non trivial unital non empty double loop structure, and x be a function from n into L. Then $\operatorname{eval}(\operatorname{EmptyBag} n, x) = 1_L$.

(17) Let n be an ordinal number, L be a unital non trivial non empty double loop structure, u be a set, and b be a bag of n. If $\operatorname{support} b = \{u\}$, then for every function x from n into L holds $\operatorname{eval}(b,x) = \operatorname{power}_L(x(u), b(u))$.

(18) Let n be an ordinal number, L be a right zeroed add-associative right complementable unital distributive Abelian non trivial commutative associative non empty double loop structure, b_1, b_2 be bags of n, and x be a function from n into L. Then $\operatorname{eval}(b_1 + b_2, x) = \operatorname{eval}(b_1,x) \cdot \operatorname{eval}(b_2,x)$.

4. Evaluation of Polynomials

Let n be an ordinal number, let L be an add-associative right zeroed right complementable non empty loop structure, and let p, q be polynomials of n, L. Note that $p-q$ is finite-Support.

The following proposition is true

(19) Let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, n be an ordinal number, and p be a polynomial of n, L. If $\mathrm{Support}\, p = \emptyset$, then $p = 0_n L$.

Let n be an ordinal number, let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, and let p be a polynomial of n, L. One can verify that $\mathrm{Support}\, p$ is finite.

Next we state the proposition

(20) Let n be an ordinal number, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, and p be a polynomial of n, L. Then $\mathrm{BagOrder}\, n$ linearly orders $\mathrm{Support}\, p$.

Let n be an ordinal number and let b be an element of $\mathrm{Bags}\, n$. The functor b^{T} yields a bag of n and is defined as follows:

(Def. 3) $b^{\mathrm{T}} = b$.

Let n be an ordinal number, let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, let p be a polynomial of n, L, and let x be a function from n into L. The functor $\mathrm{eval}(p,x)$ yielding an element of L is defined by the condition (Def. 4).

(Def. 4) There exists a finite sequence y of elements of the carrier of L such that $\mathrm{len}\, y = \mathrm{len}\,\mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p)$ and $\mathrm{eval}(p,x) = \sum y$ and for every natural number i such that $1 \leq i$ and $i \leq \mathrm{len}\, y$ holds $y_i = (p \cdot \mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p))_i \cdot \mathrm{eval}(((\mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p))_i)^{\mathrm{T}}, x)$.

The following propositions are true:

(21) Let n be an ordinal number, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, p be a polynomial of n, L, and b be a bag of n. If $\mathrm{Support}\, p = \{b\}$, then for every function x from n into L holds $\mathrm{eval}(p,x) = p(b) \cdot \mathrm{eval}(b,x)$.

(22) Let n be an ordinal number, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, and x be a function from n into L. Then $\mathrm{eval}(0_n L, x) = 0_L$.

(23) Let n be an ordinal number, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, and x be a function from n into L. Then $\mathrm{eval}(1\_(n,L),x) = 1_L$.

(24) Let n be an ordinal number, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, p be a polynomial of n, L, and x be a function from n into L. Then $\mathrm{eval}(-p,x) = -\mathrm{eval}(p,x)$.

(25) Let n be an ordinal number, L be a right zeroed add-associative right complementable Abelian unital distributive non trivial non empty double loop structure, p, q be polynomials of n, L, and x be a function from n into L. Then $\mathrm{eval}(p+q,x) = \mathrm{eval}(p,x) + \mathrm{eval}(q,x)$.

(26) Let n be an ordinal number, L be a right zeroed add-associative right complementable Abelian unital distributive non trivial non empty double loop structure, p, q be polynomials of n, L, and x be a function from n into L. Then $\mathrm{eval}(p-q,x) = \mathrm{eval}(p,x) - \mathrm{eval}(q,x)$.

(27) Let n be an ordinal number, L be a right zeroed add-associative right complementable Abelian unital distributive non trivial commutative associative non empty double loop structure, p, q be polynomials of n, L, and x be a function from n into L. Then $\mathrm{eval}(p*q,x) = \mathrm{eval}(p,x)\cdot\mathrm{eval}(q,x)$.

5. Evaluation Homomorphism

Let n be an ordinal number, let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, and let x be a function from n into L. The functor Polynom-Evaluation(n,L,x) yielding a map from Polynom-Ring(n,L) into L is defined as follows:

(Def. 5) For every polynomial p of n, L holds $(\text{Polynom-Evaluation}(n,L,x))(p) = \mathrm{eval}(p,x)$.

Let n be an ordinal number and let L be a right zeroed Abelian add-associative right complementable well unital distributive associative non trivial non empty double loop structure. One can check that Polynom-Ring(n,L) is well unital.

Let n be an ordinal number, let L be an Abelian right zeroed add-associative right complementable well unital distributive associative non trivial non empty double loop structure, and let x be a function from n into L. Note that Polynom-Evaluation(n,L,x) is unity-preserving.

Let n be an ordinal number, let L be a right zeroed add-associative right complementable Abelian unital distributive non trivial non empty double loop structure, and let x be a function from n into L. Note that Polynom-Evaluation(n,L,x) is additive.

Let n be an ordinal number, let L be a right zeroed add-associative right complementable Abelian unital distributive non trivial commutative associative non empty double loop structure, and let x be a function from n into L. One can check that Polynom-Evaluation(n,L,x) is multiplicative.

Let n be an ordinal number, let L be a right zeroed add-associative right complementable Abelian well unital distributive non trivial commutative associative non empty double loop structure, and let x be a function from n into L. Observe that Polynom-Evaluation(n,L,x) is ring homomorphism.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/card_1.html.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/nat_1.html.

[3] Grzegorz Bancerek. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal1.html.

[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finseq_1.html.

[5] Józef Białas. Group and field definitions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/realset1.html.

[6] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/binop_1.html.

[7] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_1.html.

[8] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_2.html.

[9] Czesław Byliński. Partial functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/partfun1.html.

[10] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/zfmisc_1.html.

[11] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/funct_4.html.

[12] Czesław Byliński. Some properties of restrictions of finite sequences. *Journal of Formalized Mathematics*, 7, 1995. http://mizar.org/JFM/Vol7/finseq_5.html.

[13] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finset_1.html.

[14] Adam Grabowski and Robert Milewski. Boolean posets, posets under inclusion and products of relational structures. *Journal of Formalized Mathematics*, 8, 1996. http://mizar.org/JFM/Vol8/yellow_1.html.

[15] Krzysztof Hryniewiecki. Basic properties of real numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/real_1.html.

[16] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/vectsp_1.html.

[17] Beata Madras. On the concept of the triangulation. *Journal of Formalized Mathematics*, 7, 1995. http://mizar.org/JFM/Vol7/triang_1.html.

[18] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/vectsp_2.html.

[19] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/algstr_1.html.

[20] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Journal of Formalized Mathematics*, 11, 1999. http://mizar.org/JFM/Vol11/polynom1.html.

[21] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. http://mizar.org/JFM/Axiomatics/tarski.html.

[22] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. http://mizar.org/JFM/Addenda/numbers.html.

[23] Wojciech A. Trybulec. Partially ordered sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/orders_1.html.

[24] Wojciech A. Trybulec. Vectors in real linear space. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/rlvect_1.html.

[25] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_1.html.

[26] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_4.html.

[27] Wojciech A. Trybulec. Pigeon hole principle. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finseq_4.html.

[28] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski - Zorn lemma. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/orders_2.html.

[29] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/subset_1.html.

[30] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relat_1.html.

[31] Edmund Woronowicz. Relations defined on sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relset_1.html.

[32] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relat_2.html.

Received April 14, 2000

Published January 2, 2004