FORMALIZED MATHEMATICS
Volume 9, Number 2, 2001
University of Białystok

The Evaluation of Multivariate Polynomials

Christoph Schwarzweller
University of Tübingen

Andrzej Trybulec
University of Białystok

MML Identifier: POLYNOM2.

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

1. Preliminaries

In this article we present several logical schemes. 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 $1 \leqslant n$ and $n < \mathcal{C}$ holds $\mathcal{P}[n, p_n, p_{n+1}]$

provided the parameters meet the following conditions:

- Let n be a natural number. Suppose $1 \leqslant n$ and $n < \mathcal{C}$. Let x be an element of $\mathcal{A}$. Then there exists an element y of $\mathcal{A}$ such that $\mathcal{P}[n, x, y]$, and
- Let n be a natural number. Suppose $1 \leqslant n$ and $n < \mathcal{C}$. 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 $y_1 = y_2$.

The scheme *FinRecUnD2* deals with a non empty 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 parameters meet the following requirements:

- Let n be a natural number. Suppose $1 \leqslant n$ and $n < \mathcal{C}$. 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 $y_1 = y_2$,

ISSN 1426–2630

- len $\mathcal{D} = \mathcal{C}$ but $\mathcal{D}_1 = \mathcal{B}$ or $\mathcal{C} = 0$ but for every natural number n such that $1 \leqslant n$ and $n < \mathcal{C}$ holds $\mathcal{P}[n, \mathcal{D}_n, \mathcal{D}_{n+1}]$, and
- len $\mathcal{E} = \mathcal{C}$ but $\mathcal{E}_1 = \mathcal{B}$ or $\mathcal{C} = 0$ but for every natural number n such that $1 \leqslant n$ and $n < \mathcal{C}$ 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 $\mathcal{A} \leqslant i$ and $i \leqslant \mathcal{B}$ holds $\mathcal{P}[i]$

provided the following conditions are satisfied:

- $\mathcal{P}[\mathcal{A}]$, and
- For every natural number j such that $\mathcal{A} \leqslant j$ 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 $\mathcal{A} \leqslant i$ and $i \leqslant \mathcal{B}$ holds $\mathcal{P}[i]$

provided the parameters satisfy the following conditions:

- $\mathcal{P}[\mathcal{A}]$, and
- Let j be a natural number. Suppose $\mathcal{A} \leqslant j$ and $j < \mathcal{B}$. Suppose that for every natural number j' such that $\mathcal{A} \leqslant j'$ and $j' \leqslant j$ 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 $1 \leqslant i$ and $i \leqslant$ len $\mathcal{B}$ holds $\mathcal{P}[\mathcal{B}(i)]$

provided the following conditions are satisfied:

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

Let us mention that every non empty double loop structure which is commutative and right distributive is also distributive.

The following two propositions are true:

(1) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure and x, y be elements of the carrier of L. Then $(-x) \cdot y = -x \cdot y$.

(2) Let L be a unital associative non trivial non empty double loop structure, a be an element of the carrier of L, and n, m be natural numbers. Then $\text{power}_L(a, n+m) = \text{power}_L(a, n) \cdot \text{power}_L(a, m)$.

Let us note that every non empty multiplicative loop structure which is well unital is also unital.

One can prove the following proposition

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

Let us note 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 D be a set, p be a finite sequence of elements of D, and k be a natural number. Suppose $k \in \operatorname{dom} p$. Let i be a natural number. If $1 \leqslant i$ and $i \leqslant k$, 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 the carrier 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 the carrier 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 $\operatorname{SgmX}(R, A) = \varepsilon$.

(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 $1 \leqslant i$ and $i \leqslant k - 1$, 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 $k \leqslant i$ and $i \leqslant \operatorname{len} \operatorname{SgmX}(R, A)$, 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 $\operatorname{SgmX}(R, B) = \operatorname{Ins}(\operatorname{SgmX}(R, A), k, a)$.

Let n be an ordinal number. Then $\subseteq_n$ is an order in n.

3. Evaluation of Bags

Next we state the proposition

(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. Observe 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.

Next we 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

(i) $\operatorname{len} y = \operatorname{len} \operatorname{SgmX}(\subseteq_n, \operatorname{support} b) + 1$,

(ii) $y_1 = 1_L$,

(iii) $\text{eval}(b, x) = \prod y$, and

(iv) for every natural number i such that $1 < i$ and $i \leqslant \text{len}\, y$ holds $y_i = \text{power}_L((x \cdot \text{SgmX}(\subseteq_n, \text{support}\, b))_{i-1}, (b \cdot \text{SgmX}(\subseteq_n, \text{support}\, b))_{i-1})$.

Next we 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 $\text{eval}(\text{EmptyBag}\, n, x) = 1_L$.

(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 $\text{support}\, b = \{u\}$, then for every function x from n into L holds $\text{eval}(b, x) = \text{power}_L(x(u), b(u))$.

(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 $\text{eval}(b_1 + b_2, x) = \text{eval}(b_1, x) \cdot \text{eval}(b_2, x)$.

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 $\text{Support}\, p = \emptyset$, 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. Note that $\text{Support}\, p$ 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 $\text{BagOrder}\, n$ linearly orders $\text{Support}\, p$.

Let n be an ordinal number and let b be an element of $\text{Bags}\, n$. 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 $\text{eval}(p, x)$ yields an element of L and is defined by the condition (Def. 4).

(Def. 4) There exists a finite sequence y of elements of the carrier of L such that

(i) $\operatorname{len} y = \operatorname{len} \operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p) + 1$,

(ii) $y_1 = 0_L$,

(iii) $\operatorname{eval}(p, x) = \sum y$, and

(iv) for every natural number i such that $1 < i$ and $i \leqslant \operatorname{len} y$ holds $y_i = (p \cdot \operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p))_{i-1} \cdot \operatorname{eval}(((\operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p))_{i-1})^{\mathrm{T}}, x)$.

One can prove the following propositions:

(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 $\operatorname{Support} p = \{b\}$, then for every function x from n into L holds $\operatorname{eval}(p, x) = p(b) \cdot \operatorname{eval}(b, x)$.

(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 $\operatorname{eval}(0\_(n, L), x) = 0_L$.

(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 $\operatorname{eval}(1\_(n, L), x) = 1_L$.

(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 $\operatorname{eval}(-p, x) = -\operatorname{eval}(p, x)$.

(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 $\operatorname{eval}(p + q, x) = \operatorname{eval}(p, x) + \operatorname{eval}(q, x)$.

(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 $\operatorname{eval}(p - q, x) = \operatorname{eval}(p, x) - \operatorname{eval}(q, x)$.

(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 $\operatorname{eval}(p * q, x) = \operatorname{eval}(p, x) \cdot \operatorname{eval}(q, x)$.

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 by:

(Def. 5) For every Polynomial p of n, L holds (Polynom-Evaluation$(n, L, x))(p) =$ 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. One can verify 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. Note 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. One can verify that Polynom-Evaluation(n, L, x) is ring homomorphism.

References

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

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

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

[4] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

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

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

[7] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(**2**):241–245, 1996.

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

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

[10] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.
[11] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[12] Beata Madras. On the concept of the triangulation. *Formalized Mathematics*, 5(**3**):457–462, 1996.
[13] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[14] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.
[15] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[16] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[17] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[18] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[19] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[20] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[21] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[22] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[23] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski - Zorn lemma. *Formalized Mathematics*, 1(**2**):387–393, 1990.
[24] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[25] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[26] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received April 14, 2000