FORMALIZED MATHEMATICS
Vol. 26, No. 1, Pages 81–90, 2018
DOI: 10.2478/forma-2018-0007

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

Diophantine sets. Preliminaries[1]

Karol Pąk
Institute of Informatics
University of Białystok
Poland

Summary. In this article, we define Diophantine sets using the Mizar formalism. We focus on selected properties of multivariate polynomials, i.e., functions of several variables to show finally that the class of Diophantine sets is closed with respect to the operations of union and intersection.

This article is the next in a series [1], [5] aiming to formalize the proof of Matiyasevich's negative solution of Hilbert's tenth problem.

MSC: 11D45 03B35

Keywords: Hilbert's 10th problem; Pell's equation; multivariate polynomials

MML identifier: HILB10_2, version: 8.1.07 5.47.1318

0. Introduction

Multivariate polynomials are often interpreted in informal mathematical practice as a finite sum of terms with each term being a product of a nonzero coefficient $c \in \mathfrak{F} \setminus \{\mathbf{0}\}$ and a monomial $x_1^{e_1} \cdot x_2^{e_2} \cdot \ldots \cdot x_n^{e_n}$ determined by an exponent vector $\langle e_1, e_2, \ldots, e_n \rangle \in \mathbb{N}^n$ where n is a given natural number.

Formal interpretation of multivariate polynomials developed in the Mizar Mathematical Library [4] can be considered as a generalization of the informal approach, where the natural number n is replaced by an ordinal number λ. Additionally, to avoid problems that occur when multiplying an infinite number of nonzero factors, each exponent vector $e : \lambda \mapsto \mathbb{N}$ has only a finite number of nonzero coordinates. Such exponent vectors are called *bags* of λ and the set of all

[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)

bags for a given λ is denoted by *Bags* λ. It is important to note that for a finite λ, each bag b corresponds to a finite sequence (with 0-based numbering). Using bags, multivariate polynomials have been defined in [6] as functions that assign a coefficient (an element of $\mathfrak{F}$) to each bag of λ and are zero almost everywhere. Moreover, the evaluation for a multivariate polynomial p and vector $x : \lambda \mapsto \mathfrak{F}$ has been defined as

$$\operatorname{eval}(p, x) = \sum_{b \in Bags\, \lambda} p(b) \cdot \prod_{i \in \lambda} x(i)^{b(i)}. \tag{0.1}$$

Based on this approach we define Diophantine sets in Def. 6 as follows. Let us consider a natural number n that plays the role of the dimension and a subset D of all finite sequences of length n numbered from 0 (see Def. 5). We call D *Diophantine* if there exist a natural number k and a $n+k$–variable polynomial p such that each coefficient is an integer number and

$$\forall_{x:n \mapsto \mathbb{N}}\, x \in D \iff \exists_{y:k \mapsto \mathbb{N}} \operatorname{eval}(p, x^\frown y) = 0. \tag{0.2}$$

The main aim of our article is to show that the union and intersection of two n–dimension Diophantine sets D_1, D_2 is also Diophantine. The informal proof of these facts as presented by Z. Adamowicz and P. Zbierski in [2] or C. Smorynski [7] is quite obvious. Suppose that p_i is $n + k_i$–variable polynomial which determines D_i for $i = 1, 2$. Then $p'_1 \cdot p'_2$ determines $D_1 \cap D_2$ and $(p'_1)^2 + (p'_2)^2$ determines $D_1 \cup D_2$ where p'_i is the $n + k_1 + k_2$–variable polynomial obtained from p_i by modifying the order of variables and adding insignificant variables. The property of p'_1, p'_2, used in [2] can be formally formulated as follows:

$$\operatorname{eval}(p'_1, x^\frown y_1{}^\frown y_2) = \operatorname{eval}(p_1, x^\frown y_1) \ \wedge\ \operatorname{eval}(p'_2, x^\frown y_1{}^\frown y_2) = \operatorname{eval}(p_2, x^\frown y_2) \tag{0.3}$$

for arbitrary $x : n \mapsto \mathbb{N}$, $y_1 : k_1 \mapsto \mathbb{N}$, $y_2 : k_2 \mapsto \mathbb{N}$. The existence of such polynomials have been showed in Th. 27, 28. The construction of these polynomials is useful for the further development of multivariate polynomials in the Mizar Mathematical Library. Therefore we define and provide basic properties of two transformations that

- add an additional variable to the polynomial, preserving its value, i.e.

$$\forall_{x:n \mapsto \mathbb{N}, a \in \mathbb{N}} \operatorname{eval}(p \text{ extended by } 0, x^\frown \langle a \rangle) = \operatorname{eval}(p, x), \tag{0.4}$$

- permute the order of variables, preserving its value, i.e.

$$\forall_{x:n \mapsto \mathbb{N}} \operatorname{eval}(p \text{ permuted by } \sigma, x) = \operatorname{eval}(p, x \cdot \sigma^{-1}). \tag{0.5}$$

1. PRELIMINARIES

From now on i, j, k, n, m denote natural numbers and b, b_1, b_2 denote bags of n.

Let X be a non empty set and n be a natural number. Note that there exists a finite 0-sequence of X which is n-element and there exists a finite 0-sequence which is n-element and real-valued.

Let n, m be natural numbers, p be an n-element finite 0-sequence, and q be an m-element finite 0-sequence. One can check that $p \frown q$ is $(n+m)$-element.

Let p be a real-valued finite 0-sequence and q be a real-valued finite 0-sequence. Let us observe that $p \frown q$ is real-valued.

Let n be a natural number and p be an n-element, real-valued finite 0-sequence. The functor ${}^{@}p$ yielding a function from n into $\mathbb{R}_{\mathrm{F}}$ is defined by the term

(Def. 1) p.

Let X be a non empty set and p be a function from n into X. The functor ${}^{@}p$ yielding an n-element finite 0-sequence of X is defined by the term

(Def. 2) p.

Let X be a set, p be a permutation of X, and M be a many sorted set indexed by X. Observe that $M \cdot p$ is total.

Let F be a finite-support function and f be a one-to-one function. Let us observe that $F \cdot f$ is finite-support.

Now we state the propositions:

(1) Let us consider finite 0-sequences F, G. Suppose $F \frown G$ is one-to-one. Then $\operatorname{rng} F$ misses $\operatorname{rng} G$.

(2) Let us consider a set X, an X-defined function f, and a permutation σ of X. Then $\overline{\overline{\operatorname{support} f \cdot \sigma}} = \overline{\overline{\operatorname{support} f}}$.
PROOF: Set $P = \sigma^{-1}$. $P^{\circ}(\operatorname{support} f) \subseteq \operatorname{support} f \cdot \sigma$. $\operatorname{support} f \cdot \sigma \subseteq P^{\circ}(\operatorname{support} f)$. $\square$

Let X be a set. Observe that $0_X(\mathbb{R}_{\mathrm{F}})$ is natural-valued and $1\_(X, \mathbb{R}_{\mathrm{F}})$ is natural-valued.

Let x be an element of X. Note that $1\_1(x, \mathbb{R}_{\mathrm{F}})$ is natural-valued and there exists a series of X, $\mathbb{R}_{\mathrm{F}}$ which is $\mathbb{Z}$-valued.

Let O be an ordinal number. Let us note that there exists a polynomial of O,$\mathbb{R}_{\mathrm{F}}$ which is $\mathbb{Z}$-valued.

Let X be a set and p be a $\mathbb{Z}$-valued series of X, $\mathbb{R}_{\mathrm{F}}$. One can check that $-p$ is $\mathbb{Z}$-valued.

Let q be a $\mathbb{Z}$-valued series of X, $\mathbb{R}_{\mathrm{F}}$. Observe that $p+q$ is $\mathbb{Z}$-valued and $p-q$ is $\mathbb{Z}$-valued.

Let X be an ordinal number and p, q be $\mathbb{Z}$-valued series of X, $\mathbb{R}_{\mathrm{F}}$. One can verify that $p * q$ is $\mathbb{Z}$-valued.

Let X be a set. Let us note that there exists a function from X into $\mathbb{R}_{\mathrm{F}}$ which is natural-valued.

Let O be an ordinal number. One can check that there exists a function from O into $\mathbb{R}_{\mathrm{F}}$ which is $\mathbb{Z}$-valued.

Let b be a bag of O and x be a $\mathbb{Z}$-valued function from O into $\mathbb{R}_{\mathrm{F}}$. Note that $\mathrm{eval}(b, x)$ is integer.

Let p be a $\mathbb{Z}$-valued polynomial of O,$\mathbb{R}_{\mathrm{F}}$. One can check that $\mathrm{eval}(p, x)$ is integer.

2. Polynomial Extended by 0

Now we state the propositions:

(3) Let us consider a many sorted set b indexed by n. If $k \leqslant n$, then $\langle b(0), \ldots, b(k)\rangle = b{\restriction}k$.
Proof: For every object x such that $x \in k$ holds $\langle b(0), \ldots, b(k)\rangle(x) = (b{\restriction}k)(x)$. □

(4) Let us consider a bag b of $n{+}1$. Then $b = \langle b(0), \ldots, b(n)\rangle$ extended by $b(n)$.
Proof: Set $C = \langle b(0), \ldots, b(n)\rangle$. Set $B = C$ extended by $b(n)$. $C = b{\restriction}n$. For every object x such that $x \in n + 1$ holds $B(x) = b(x)$ by [8, (2)]. □

(5) $\langle b$ extended by $k(0), \ldots, b$ extended by $k(n)\rangle = b$. The theorem is a consequence of (3).

Let us consider n. Let L be a non empty zero structure and p be a series of n, L. The p extended by 0 yielding a series of $n + 1$, L is defined by

(Def. 3) for every bag b of $n + 1$, if $b(n) \neq 0$, then $it(b) = 0_L$ and if $b(n) = 0$, then $it(b) = p(\langle b(0), \ldots, b(n)\rangle)$.

Now we state the propositions:

(6) Let us consider a non empty zero structure L, and a series p of n, L. Then (the p extended by 0)(b extended by 0) $= p(b)$. The theorem is a consequence of (5).

(7) Let us consider a non empty zero structure L, a series p of n, L, and a bag b of $n{+}1$. Suppose $b \in$ Support(the p extended by 0). Then $b(n) = 0$.

(8) Let us consider a non empty zero structure L, and a series p of n, L. Then b extended by $0 \in$ Support(the p extended by 0) if and only if $b \in$ Support p. The theorem is a consequence of (5).

(9) Let us consider a non empty zero structure L, a series p of n, L, and a bag b of $n{+}1$. Suppose $b(n) = 0$. Then $b \in$ Support(the p extended by 0)

if and only if $\langle b(0), \ldots, b(n)\rangle \in \operatorname{Support} p$. The theorem is a consequence of (4) and (8).

Let us consider n. Let L be a non empty zero structure and p be a polynomial of n,L. Let us observe that the p extended by 0 is finite-Support.

Now we state the propositions:

(10) Let us consider a non empty zero structure L, and a series p of n, L. Then $\{0_L\} \cup \operatorname{rng} p = \operatorname{rng}(\text{the } p \text{ extended by } 0)$. The theorem is a consequence of (6).

(11) $\operatorname{support} b = \operatorname{support}(b \text{ extended by } 0)$.

PROOF: Set $E = b$ extended by 0. $\operatorname{support} b \subseteq \operatorname{support} E$. □

(12) $\operatorname{SgmX}({\subseteq}_n, \operatorname{support} b) = \operatorname{SgmX}({\subseteq}_{n+1}, \operatorname{support}(b \text{ extended by } 0))$. The theorem is a consequence of (11).

(13) Let us consider a well unital, non trivial double loop structure L, a function x from n into L, and a function y from $n+1$ into L. Suppose $y{\restriction}n = x$. Then $\operatorname{eval}(b, x) = \operatorname{eval}(b \text{ extended by } 0, y)$.

PROOF: Set $S = \operatorname{SgmX}({\subseteq}_n, \operatorname{support} b)$. Set $B = b$ extended by 0. Set $S_1 = \operatorname{SgmX}({\subseteq}_{n+1}, \operatorname{support} B)$. Consider P being a finite sequence of elements of L such that $\operatorname{len} P = \operatorname{len} S$ and $\operatorname{eval}(b, x) = \prod P$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} P$ holds $P_{/i} = \operatorname{power}_L(x \cdot S_{/i}, b \cdot S_{/i})$. Consider P_1 being a finite sequence of elements of L such that $\operatorname{len} P_1 = \operatorname{len} S_1$ and $\operatorname{eval}(B, y) = \prod P_1$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} P_1$ holds $P_{1/i} = \operatorname{power}_L(y \cdot S_{1/i}, B \cdot S_{1/i})$. $S = S_1$. $b = \langle B(0), \ldots, B(n)\rangle$. For every natural number i such that $1 \leqslant i \leqslant \operatorname{len} P$ holds $P(i) = P_1(i)$. □

(14) $b_1 < b_2$ if and only if b_1 extended by $k < b_2$ extended by k.

PROOF: Set $B_1 = b_1$ extended by k. Set $B_2 = b_2$ extended by k. If $b_1 < b_2$, then b_1 extended by $k < b_2$ extended by k. Consider o being an ordinal number such that $B_1(o) < B_2(o)$ and for every ordinal number l such that $l \in o$ holds $B_1(l) = B_2(l)$. For every ordinal number l such that $l \in o$ holds $b_1(l) = b_2(l)$. □

(15) Let us consider a non empty set X, a finite subset A of X, and an order R in X. Suppose R linearly orders A. Suppose $1 \leqslant i \leqslant k \leqslant \overline{\overline{A}}$. Then $(\operatorname{SgmX}(R, \operatorname{rng}(\operatorname{SgmX}(R, A){\restriction}k)))_{/i} = (\operatorname{SgmX}(R, A))_{/i}$.

PROOF: Set $S_1 = \operatorname{SgmX}(R, A)$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every i such that $1 \leqslant i \leqslant \$_1 \leqslant \overline{\overline{A}}$ holds $(\operatorname{SgmX}(R, \operatorname{rng}(S_1{\restriction}\$_1)))_{/i} = S_{1/i}$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [3, (83)]. For every k, $\mathcal{P}[k]$. □

(16) Let us consider an ordinal number O, and a finite subset A of $\operatorname{Bags} O$. Suppose n, $m \in \operatorname{dom} \operatorname{SgmX}(\operatorname{BagOrder} O, A)$ and $n < m$.

Then $(\operatorname{SgmX}(\operatorname{BagOrder} O, A))_{/n} < (\operatorname{SgmX}(\operatorname{BagOrder} O, A))_{/m}$.

(17) Let us consider a right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure L, and a polynomial p of n,L. Then

(i) $\operatorname{len}\operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p) =$
$\operatorname{len}\operatorname{SgmX}(\operatorname{BagOrder}(n+1), \operatorname{Support}(\text{the } p \text{ extended by } 0))$, and

(ii) for every natural number i such that
$1 \leqslant i \leqslant \operatorname{len}\operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p)$ holds
$(\operatorname{SgmX}(\operatorname{BagOrder}(n+1), \operatorname{Support}(\text{the } p \text{ extended by } 0)))_{/i} =$
$(\operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p))_{/i}$ extended by 0.

PROOF: Set $B = \operatorname{BagOrder} n$. Set $B_1 = \operatorname{BagOrder}(n+1)$. Set $P =$ the p extended by 0. Define $\mathcal{F}(\text{bag of } n) = \$_1$ extended by 0. Consider f being a function from $\operatorname{Bags} n$ into $\operatorname{Bags}(n+1)$ such that for every element x of $\operatorname{Bags} n$, $f(x) = \mathcal{F}(x)$. Set $F = f \restriction \operatorname{Support} p$. Set $S_1 = \operatorname{SgmX}(B, \operatorname{Support} p)$. Set $S_2 = \operatorname{SgmX}(B_1, \operatorname{Support} P)$. $\operatorname{rng} F \subseteq \operatorname{Support} P$. $\operatorname{Support} P \subseteq \operatorname{rng} F$. F is one-to-one. Define $\mathcal{P}[\text{natural number}] \equiv$ if $1 \leqslant \$_1 \leqslant \operatorname{len} S_1$, then for every i such that $1 \leqslant i \leqslant \$_1$ holds $S_{2/i} = S_{1/i}$ extended by0. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every k, $\mathcal{P}[k]$. □

(18) Let us consider a right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure L, a polynomial p of n,L, a function x from n into L, and a function y from $n+1$ into L. Suppose $y \restriction n = x$. Then $\operatorname{eval}(p, x) = \operatorname{eval}(\text{the } p \text{ extended by } 0, y)$.
PROOF: Set $n_1 = n+1$. Set $S = \operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p)$. Set $P =$ the p extended by 0. Set $S_1 = \operatorname{SgmX}(\operatorname{BagOrder} n_1, \operatorname{Support} P)$. Consider T being a finite sequence of elements of L such that $\operatorname{len} T = \operatorname{len} S$ and $\operatorname{eval}(p, x) = \sum T$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} T$ holds $T_{/i} = p \cdot S_{/i} \cdot \operatorname{eval}(S_{/i}, x)$. Consider T_1 being a finite sequence of elements of L such that $\operatorname{len} T_1 = \operatorname{len} S_1$ and $\operatorname{eval}(P, y) = \sum T_1$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} T_1$ holds $T_{1/i} = P \cdot S_{1/i} \cdot \operatorname{eval}(S_{1/i}, y)$. $\operatorname{len} S = \operatorname{len} S_1$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} S$ holds $S_{1/i} = S_{/i}$ extended by 0. For every natural number i such that $1 \leqslant i \leqslant \operatorname{len} S$ holds $T(i) = T_1(i)$. □

3. Polynomial Permuted by Permutation

Now we state the propositions:

(19) Let us consider an ordinal number O, a well unital, commutative, associative, non trivial double loop structure L, a function x from O into L, a bag b of O, and a one-to-one finite sequence S of elements of O. Suppose

$\operatorname{rng} S = \operatorname{support} b$. Then there exists a finite sequence y of elements of L such that

(i) $\operatorname{len} y = \overline{\overline{\operatorname{support} b}}$, and

(ii) $\operatorname{eval}(b, x) = \prod y$, and

(iii) for every i such that $1 \leqslant i \leqslant \operatorname{len} y$ holds $y_{/i} = \operatorname{power}_L(x \cdot S_{/i}, b \cdot S_{/i})$.

(20) Let us consider an ordinal number O, a well unital, commutative, associative, non trivial double loop structure L, a function x from O into L, a bag b of O, and a permutation σ of O. Then $\operatorname{eval}(b, x) = \operatorname{eval}(b \cdot \sigma, x \cdot \sigma)$. PROOF: Set $S_1 = \operatorname{SgmX}(\subseteq_n, \operatorname{support} b)$. Consider y being a finite sequence of elements of L such that $\operatorname{len} y = \operatorname{len} S_1$ and $\operatorname{eval}(b, x) = \prod y$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} y$ holds $y_{/i} = \operatorname{power}_L(x \cdot S_{1/i}, b \cdot S_{1/i})$. Set $P = \sigma^{-1}$. $\operatorname{rng} P \cdot S_1 \subseteq \operatorname{support} b \cdot \sigma$. $\operatorname{support} b \cdot \sigma \subseteq \operatorname{rng} P \cdot S_1$. Reconsider $S = P \cdot S_1$ as a one-to-one finite sequence of elements of n. Consider Y being a finite sequence of elements of L such that $\operatorname{len} Y = \overline{\overline{\operatorname{support} b \cdot \sigma}}$ and $\operatorname{eval}(b \cdot \sigma, x \cdot \sigma) = \prod Y$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} Y$ holds $Y_{/i} = \operatorname{power}_L(x \cdot \sigma \cdot S_{/i}, b \cdot \sigma \cdot S_{/i})$. $\operatorname{len} Y = \operatorname{len} y$. For every natural number i such that $1 \leqslant i \leqslant \operatorname{len} Y$ holds $Y(i) = y(i)$. □

Let O be an ordinal number, L be a non empty zero structure, s be a series of O, L, and σ be a permutation of O. The s permuted by σ yielding a series of O, L is defined by

(Def. 4) for every bag b of O, $it(b) = s(b \cdot \sigma)$.

Let us consider an ordinal number O, a non empty zero structure L, a permutation σ of O, a series s of O, L, and a bag b of O. Now we state the propositions:

(21) $b \in \operatorname{Support}$(the s permuted by σ) if and only if $b \cdot \sigma \in \operatorname{Support} s$.

(22) $b \cdot \sigma^{-1} \in \operatorname{Support}$(the s permuted by σ) if and only if $b \in \operatorname{Support} s$.

(23) Let us consider an ordinal number O, a non empty zero structure L, a permutation σ of O, and a series s of O, L. Then $\overline{\overline{\operatorname{Support} s}} = \overline{\overline{\operatorname{Support} \alpha}}$, where α is the s permuted by σ.
PROOF: Set $P =$ the s permuted by σ. Define $\mathcal{R}[\text{bag of } O, \text{bag of } O] \equiv \$_2 = \$_1 \cdot \sigma$. For every element x of $\operatorname{Bags} O$, there exists an element y of $\operatorname{Bags} O$ such that $\mathcal{R}[x, y]$. Consider f being a function from $\operatorname{Bags} O$ into $\operatorname{Bags} O$ such that for every element x of $\operatorname{Bags} O$, $\mathcal{R}[x, f(x)]$. f is one-to-one. $f^\circ(\operatorname{Support} P) \subseteq \operatorname{Support} s$. $\operatorname{Support} s \subseteq f^\circ(\operatorname{Support} P)$. □

(24) Let us consider an ordinal number O, an Abelian, right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure L, a polynomial p of O,L, a function x from O into L, and a one-to-one finite sequence S of elements of $\operatorname{Bags} O$. Suppose

rng S = Support p. Then there exists a finite sequence y of elements of L such that

(i) $\operatorname{len} y = \overline{\overline{\text{Support } p}}$, and

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

(iii) for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} y$ holds $y_{/i} = p \cdot S_{/i} \cdot \operatorname{eval}(S_{/i}, x)$.

Let O be an ordinal number, L be a non empty zero structure, σ be a permutation of O, and p be a polynomial of O,L. One can check that the p permuted by σ is finite-Support.

(25) Let us consider an ordinal number O, an Abelian, right zeroed, add-associative, right complementable, well unital, distributive, commutative, associative, non trivial double loop structure L, a polynomial p of O,L, a function x from O into L, and a permutation σ of O. Then $\operatorname{eval}(p, x) = \operatorname{eval}(\text{the } p \text{ permuted by } \sigma, x \cdot (\sigma^{-1}))$.

Proof: Set $S_2 = \operatorname{SgmX}(\operatorname{BagOrder} O, \text{Support } p)$. Consider y being a finite sequence of elements of L such that $\operatorname{len} y = \operatorname{len} S_2$ and $\operatorname{eval}(p, x) = \sum y$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} y$ holds $y_{/i} = p \cdot S_{2/i} \cdot \operatorname{eval}(S_{2/i}, x)$. Set P = the p permuted by σ. Define $\mathcal{R}[\text{bag of } O, \text{bag of } O] \equiv \$_2 = \$_1 \cdot \sigma^{-1}$. For every element x of Bags O, there exists an element y of Bags O such that $\mathcal{R}[x, y]$. Consider f being a function from Bags O into Bags O such that for every element x of Bags O, $\mathcal{R}[x, f(x)]$. f is one-to-one. Reconsider $f_1 = f \cdot S_2$ as a one-to-one finite sequence of elements of Bags O. rng $f_1 \subseteq$ Support P. Support $P \subseteq$ rng f_1. Consider z being a finite sequence of elements of L such that $\operatorname{len} z = \overline{\overline{\text{Support } P}}$ and $\operatorname{eval}(P, x \cdot \sigma^{-1}) = \sum z$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} z$ holds $z_{/i} = P \cdot f_{1/i} \cdot \operatorname{eval}(f_{1/i}, x \cdot \sigma^{-1})$. $\operatorname{len} y = \operatorname{len} z$. For every natural number i such that $1 \leqslant i \leqslant \operatorname{len} y$ holds $y(i) = z(i)$. □

(26) Let us consider an ordinal number O, a non empty zero structure L, a series s of O, L, and a permutation σ of O. Then $\operatorname{rng}(\text{the } s \text{ permuted by } \sigma) = \operatorname{rng} s$.

4. Main Lemmas

Now we state the propositions:

(27) Let us consider a right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure L, and a polynomial p of n,L. Then there exists a polynomial q of $n + m$,L such that

(i) $\operatorname{rng} q \subseteq \operatorname{rng} p \cup \{0_L\}$, and

(ii) for every function x from n into L and for every function y from $n+m$ into L such that $y\restriction n = x$ holds $\mathrm{eval}(p,x) = \mathrm{eval}(q,y)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ there exists a polynomial q of $n+\$_1$,$L$ such that $\mathrm{rng}\, q \subseteq \mathrm{rng}\, p \cup \{0_L\}$ and for every function x from n into L and for every function y from $n+\$_1$ into L such that $y\restriction n = x$ holds $\mathrm{eval}(p,x) = \mathrm{eval}(q,y)$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

(28) Let us consider an Abelian, right zeroed, add-associative, right complementable, well unital, distributive, commutative, associative, non trivial double loop structure L, and a polynomial p of $n+m$,L. Then there exists a polynomial q of $n+k+m$,L such that

(i) $\mathrm{rng}\, q \subseteq \mathrm{rng}\, p \cup \{0_L\}$, and

(ii) for every function X_1 from $n+m$ into L and for every function X_2 from $n+k+m$ into L such that $X_1\restriction n = X_2\restriction n$ and $({}^{@}X_1)_{\lfloor n} = ({}^{@}X_2)_{\lfloor n+k}$ holds $\mathrm{eval}(p,X_1) = \mathrm{eval}(q,X_2)$.

PROOF: Consider P being a polynomial of $n+m+k$,L such that $\mathrm{rng}\, P \subseteq \mathrm{rng}\, p \cup \{0_L\}$ and for every function x from $n+m$ into L and for every function y from $n+m+k$ into L such that $y\restriction(n+m) = x$ holds $\mathrm{eval}(p,x) = \mathrm{eval}(P,y)$. Reconsider $P_1 = P$ as a polynomial of $n+k+m$,L. Set $I = \mathrm{id}_{n+k+m}$. Set $n_1 = n+m$. Set $I_2 = I\restriction n_1$. $\mathrm{rng}\, I_2$ misses $\mathrm{rng}\, I_{\lfloor n_1}$. $\mathrm{rng}(I_2\restriction n)$ misses $\mathrm{rng}\, I_{2\lfloor n}$. Reconsider $I_1 = ((I_2\restriction n)^\frown I_{\lfloor n_1})^\frown I_{2\lfloor n}$ as a function from $n+k+m$ into $n+k+m$. Reconsider $R = {}^{@}X_1{}^\frown({}^{@}X_2\restriction(n+k))_{\lfloor n}$ as a function from $n+m+k$ into L. Reconsider $r = R$ as a function from $n+k+m$ into L. $\mathrm{eval}(P_1,r) = \mathrm{eval}(T, r\cdot I_1)$. For every k such that $k \in \mathrm{dom}\, {}^{@}X_2$ holds $({}^{@}r\cdot I_1)(k) = ({}^{@}X_2)(k)$. □

5. DIOPHANTINE SETS

From now on x, s denote objects.

Let D be a non empty set and n be a natural number. The n-xtuples of D yielding a subset of D^ω is defined by

(Def. 5) $x \in it$ iff x is an n-element finite 0-sequence of D.

Observe that the n-xtuples of D is non empty and every element of the n-xtuples of D is n-element and D-valued.

Let A be a subset of the n-xtuples of $\mathbb{N}$. We say that A is diophantine if and only if

(Def. 6) there exists a natural number m and there exists a $\mathbb{Z}$-valued polynomial p of $n+m$,$\mathbb{R}_{\mathrm{F}}$ such that for every s, $s \in A$ iff there exists an n-element

finite 0-sequence x of $\mathbb{N}$ and there exists an m-element finite 0-sequence y of $\mathbb{N}$ such that $s = x$ and $\operatorname{eval}(p, @(x \frown y)) = 0$.

One can verify that every subset of the n-xtuples of $\mathbb{N}$ which is empty is also diophantine and $\Omega_{\text{the } n\text{-xtuples of } \mathbb{N}}$ is diophantine.

Let n be a zero natural number. One can verify that every subset of the n-xtuples of $\mathbb{N}$ is diophantine.

Let n be a natural number. Let us observe that there exists a subset of the n-xtuples of $\mathbb{N}$ which is non empty and diophantine and there exists a subset of the n-xtuples of $\mathbb{N}$ which is empty and diophantine.

Let A, B be diophantine subsets of the n-xtuples of $\mathbb{N}$. One can check that $A \cap B$ is diophantine as a subset of the n-xtuples of $\mathbb{N}$ and $A \cup B$ is diophantine as a subset of the n-xtuples of $\mathbb{N}$.

References

[1] Marcin Acewicz and Karol Pąk. Pell's equation. *Formalized Mathematics*, 25(**3**):197–204, 2017. doi:10.1515/forma-2017-0019.

[2] Zofia Adamowicz and Paweł Zbierski. *Logic of Mathematics: A Modern Course of Classical Logic*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley-Interscience, 1997.

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

[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] Karol Pąk. The Matiyasevich theorem. Preliminaries. *Formalized Mathematics*, 25(**4**): 315–322, 2017. doi:10.1515/forma-2017-0029.

[6] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.

[7] Craig Smorynski. *Logical Number Theory I, An Introduction*. Universitext. Springer-Verlag Berlin Heidelberg, 1991. ISBN 978-3-642-75462-3.

[8] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.

Received March 27, 2018