FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 209–221, 2019
DOI: 10.2478/forma-2019-0020

sciendo
https://www.sciendo.com/

# Formalization of the MRDP Theorem in the Mizar System[1]

Karol Pąk
Institute of Informatics
University of Białystok
Poland

**Summary.** This article is the final step of our attempts to formalize the negative solution of Hilbert's tenth problem.

In our approach, we work with the Pell's Equation defined in [2]. We analyzed this equation in the general case to show its solvability as well as the cardinality and shape of all possible solutions. Then we focus on a special case of the equation, which has the form $x^2-(a^2-1)y^2=1$ [8] and its solutions considered as two sequences $\{x_i(a)\}_{i=0}^{\infty}$, $\{y_i(a)\}_{i=0}^{\infty}$. We showed in [1] that the $n$-th element of these sequences can be obtained from lists of several basic Diophantine relations as linear equations, finite products, congruences and inequalities, or more precisely that the equation $x=y_i(a)$ is Diophantine. Following the post-Matiyasevich results we show that the equality determined by the value of the power function $y=x^z$ is Diophantine, and analogously property in cases of the binomial coefficient, factorial and several product [9].

In this article, we combine analyzed so far Diophantine relation using conjunctions, alternatives as well as substitution to prove the bounded quantifier theorem. Based on this theorem we prove MDPR-theorem that *every recursively enumerable set is Diophantine,* where recursively enumerable sets have been defined by the Martin Davis normal form.

The formalization by means of Mizar system [5], [7], [4] follows [10], Z. Adamowicz, P. Zbierski [3] as well as M. Davis [6].

MSC: 11D45 68T99 03B35

Keywords: Hilbert's 10th problem; Diophantine relations

MML identifier: HILB10_5, version: 8.1.09 5.57.1355

[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)

## 1. Preliminaries

From now on $i$, $j$, $n$, $n_1$, $n_2$, $m$, $k$, $l$, $u$ denote natural numbers, $i_1$, $i_2$, $i_3$, $i_4$, $i_5$, $i_6$ denote elements of $n$, $p$, $q$ denote $n$-element finite 0-sequences of $\mathbb{N}$, and $a$, $b$, $c$, $d$, $e$, $f$ denote integers.

Let $n$ be a natural number. Let us note that $\operatorname{idseq}(n)$ is $\mathbb{Z}$-valued.

Let $x$ be an $n$-element, natural-valued finite 0-sequence and $p$ be a $\mathbb{Z}$-valued polynomial of $n$,$\mathbb{R}_{\mathrm{F}}$. One can check that $\operatorname{eval}(p, {}^{@}x)$ is integer.

Now we state the proposition:

(1) Let us consider a $\mathbb{Z}$-valued polynomial $p$ of $n$,$\mathbb{R}_{\mathrm{F}}$, and $n$-element finite 0-sequences $x$, $y$ of $\mathbb{N}$. Suppose $k \neq 0$ and for every $i$ such that $i \in n$ holds $k \mid x(i)-y(i)$. Then $k \mid (\operatorname{eval}(p, {}^{@}x)$ **qua** integer$)-(\operatorname{eval}(p, {}^{@}y)$ **qua** integer$)$.
Proof: Reconsider $f_1 = \mathbb{R}_{\mathrm{F}}$ as a field. Reconsider $p_1 = p$ as a polynomial of $n$,$f_1$. Reconsider $x_2 = {}^{@}x$, $y_2 = {}^{@}y$ as a function from $n$ into the carrier of $f_1$. Set $s_3 = \operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p_1)$. Consider $X$ being a finite sequence of elements of the carrier of $f_1$ such that $\operatorname{len} X = \operatorname{len} s_3$ and $\operatorname{eval}(p_1, x_2) = \sum X$ and for every element $i$ of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} X$ holds $X_{/i} = p_1 \cdot s_{3/i} \cdot (\operatorname{eval}(s_{3/i}, x_2))$.

Consider $Y$ being a finite sequence of elements of the carrier of $f_1$ such that $\operatorname{len} Y = \operatorname{len} s_3$ and $\operatorname{eval}(p_1, y_2) = \sum Y$ and for every element $i$ of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} Y$ holds $Y_{/i} = p_1 \cdot s_{3/i} \cdot (\operatorname{eval}(s_{3/i}, y_2))$. Reconsider $Y_2 = Y$, $X_4 = X$ as a finite sequence of elements of $\mathbb{R}$. Define $\mathcal{P}[$natural number$] \equiv$ if $\$_1 \leqslant \operatorname{len} X$, then $\sum(X_4 \restriction \$_1) - \sum(Y_2 \restriction \$_1)$ is an integer and for every integer $d$ such that $d = \sum(X_4 \restriction \$_1) - \sum(Y_2 \restriction \$_1)$ holds $k \mid d$. For every natural number $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. □

Let $f$ be a $\mathbb{Z}$-valued function. Let us note that $-f$ is $\mathbb{Z}$-valued.

The scheme *SCH1* deals with a binary predicate $\mathcal{P}$ and a finite-0-sequence-yielding finite 0-sequence $f$ and states that

(Sch. 1) $\{f(i)(j)$, where $i$, $j$ are natural numbers : $\mathcal{P}[i,j]\}$ is finite.

Now we state the propositions:

(2) If $m \geqslant n > 0$, then $1 + m! \cdot (\operatorname{idseq}(n))$ is a CR-sequence.
Proof: Set $h = 1 + m! \cdot (\operatorname{idseq}(n))$. Define $\mathcal{F}($natural number$) = m! \cdot \$_1 + 1$. For every $i$ such that $i \in \operatorname{dom} h$ holds $h(i) = \mathcal{F}(i)$. $h$ is positive yielding. For every natural numbers $i$, $j$ such that $i$, $j \in \operatorname{dom} h$ and $i < j$ holds $h(i)$ and $h(j)$ are relatively prime. $h$ is Chinese remainder. □

(3) Let us consider a prime number $p$, and a finite sequence $f$ of elements of $\mathbb{N}$. Suppose $f$ is positive yielding and $p \mid \prod f$. Then there exists $i$ such that

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

(ii) $p \mid f(i)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence $f$ of elements of $\mathbb{N}$ such that $\operatorname{len} f = \$_1$ and $f$ is positive yielding and $p \mid \prod f$ there exists $i$ such that $i \in \operatorname{dom} f$ and $p \mid f(i)$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. □

## 2. Selected Operations on Polynomials

Let $n$ be a set and $p$ be a series of $n$, $\mathbb{R}_{\rm F}$. The functor $|p|$ yielding a series of $n$, $\mathbb{R}_{\rm F}$ is defined by

(Def. 1) for every bag $b$ of $n$, $it(b) = |p(b)|$.

Now we state the proposition:

(4) Let us consider a set $n$, and a series $p$ of $n$, $\mathbb{R}_{\rm F}$. Then $\operatorname{Support} p = \operatorname{Support} |p|$.

Let $n$ be an ordinal number and $p$ be a polynomial of $n$,$\mathbb{R}_{\rm F}$. Let us note that $|p|$ is finite-Support.

Let $n$ be a set, $S$ be a non empty zero structure, and $p$ be a finite-Support series of $n$, $S$. One can check that $\operatorname{Support} p$ is finite.

Let $n$ be an ordinal number, $L$ be an add-associative, right zeroed, right complementable, non empty additive loop structure, and $p$ be a polynomial of $n$,$L$. The functor $\sum \texttt{coeff}(p)$ yielding an element of $L$ is defined by the term

(Def. 2) $\sum p \cdot (\operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p))$.

The functor degree($p$) yielding a natural number is defined by

(Def. 3) (i) there exists a bag $s$ of $n$ such that $s \in \operatorname{Support} p$ and $it = \operatorname{degree}(s)$ and for every bag $s_1$ of $n$ such that $s_1 \in \operatorname{Support} p$ holds $\operatorname{degree}(s_1) \leqslant it$, **if** $p \neq 0_n L$,

(ii) $it = 0$, **otherwise**.

Now we state the propositions:

(5) Let us consider an ordinal number $n$, and a bag $b$ of $n$. Then $\operatorname{degree}(b) = \sum b \cdot (\operatorname{SgmX}(\subseteq_n, \operatorname{support} b))$.

(6) Let us consider an ordinal number $n$, an add-associative, right zeroed, right complementable, non empty additive loop structure $L$, and a polynomial $p$ of $n$,$L$. Then $\operatorname{degree}(p) = 0$ if and only if $\operatorname{Support} p \subseteq \{\operatorname{EmptyBag} n\}$.

Proof: If $\operatorname{degree}(p) = 0$, then $\operatorname{Support} p \subseteq \{\operatorname{EmptyBag} n\}$. Consider $s$ being a bag of $n$ such that $s \in \operatorname{Support} p$ and $\operatorname{degree}(p) = \operatorname{degree}(s)$. □

(7) Let us consider an ordinal number $n$, an add-associative, right zeroed, right complementable, non empty additive loop structure $L$, a polynomial $p$ of $n$,$L$, and a bag $b$ of $n$. If $b \in \operatorname{Support} p$, then $\operatorname{degree}(p) \geqslant \operatorname{degree}(b)$.

(8) Let us consider an ordinal number $n$, and a polynomial $p$ of $n$,$\mathbb{R}_{\mathrm{F}}$. If $|p| = 0_n(\mathbb{R}_{\mathrm{F}})$, then $p = 0_n(\mathbb{R}_{\mathrm{F}})$.

Let $n$ be a set. One can verify that $|0_n(\mathbb{R}_{\mathrm{F}})|$ reduces to $0_n(\mathbb{R}_{\mathrm{F}})$. Now we state the propositions:

(9) Let us consider an ordinal number $n$, and a polynomial $p$ of $n$,$\mathbb{R}_{\mathrm{F}}$. Then $\mathrm{degree}(p) = \mathrm{degree}(|p|)$. The theorem is a consequence of (8) and (4).

(10) Let us consider an ordinal number $n$, a bag $b$ of $n$, and a real number $r$. Suppose $r \geqslant 1$. Let us consider a function $x$ from $n$ into the carrier of $\mathbb{R}_{\mathrm{F}}$. Suppose for every object $i$ such that $i \in \mathrm{dom}\, x$ holds $|x(i)| \leqslant r$. Then $|\,\mathrm{eval}(b, x)| \leqslant r^{\mathrm{degree}(b)}$.

Proof: Reconsider $f_1 = \mathbb{R}_{\mathrm{F}}$ as a field. Set $s_2 = \mathrm{SgmX}(\subseteq_n, \mathrm{support}\, b)$. Set $B = b \cdot s_2$. Consider $y$ being a finite sequence of elements of $f_1$ such that $\mathrm{len}\, y = \mathrm{len}\, s_2$ and $\mathrm{eval}(b, x) = \prod y$ and for every element $i$ of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y$ holds $y_{/i} = \mathrm{power}_{\mathbb{R}_{\mathrm{F}}}(x \cdot s_{2/i}, B_{/i})$.

Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant \mathrm{len}\, y$, then $\prod(y \restriction \$_1)$ is a real number and for every real number $P$ such that $P = \prod(y \restriction \$_1)$ holds $|P| \leqslant r^{\sum(B \restriction \$_1)}$. For every $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every $i$, $\mathcal{P}[i]$. □

(11) Let us consider an ordinal number $n$, a polynomial $p$ of $n$,$\mathbb{R}_{\mathrm{F}}$, and a real number $r$. Suppose $r \geqslant 1$. Let us consider a function $x$ from $n$ into the carrier of $\mathbb{R}_{\mathrm{F}}$. Suppose for every object $i$ such that $i \in \mathrm{dom}\, x$ holds $|x(i)| \leqslant r$. Then $|\,\mathrm{eval}(p, x)| \leqslant (\sum \mathtt{coeff}(|p|)) \cdot (r^{\mathrm{degree}(p)})$.

Proof: Reconsider $f_1 = \mathbb{R}_{\mathrm{F}}$ as a field. Reconsider $p_1 = p$, $A_1 = |p|$ as a polynomial of $n$,$f_1$. Reconsider $x_2 = x$ as a function from $n$ into the carrier of $f_1$. Set $S_1 = \mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p_1)$. Reconsider $H = A_1 \cdot S_1$ as a finite sequence of elements of the carrier of $\mathbb{R}_{\mathrm{F}}$. $\sum \mathtt{coeff}(|p|) = \sum A_1 \cdot S_1$.

Consider $y$ being a finite sequence of elements of the carrier of $f_1$ such that $\mathrm{len}\, y = \mathrm{len}\, S_1$ and $\mathrm{eval}(p, x) = \sum y$ and for every element $i$ of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, y$ holds $y_{/i} = p_1 \cdot S_{1/i} \cdot (\mathrm{eval}(S_{1/i}, x_2))$. Reconsider $Y = y$ as a finite sequence of elements of $\mathbb{R}$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant \mathrm{len}\, y$, then $|\sum(Y \restriction \$_1)| \leqslant (\sum(H \restriction \$_1)) \cdot (r^{\mathrm{degree}(p)})$. For every natural number $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number $i$, $\mathcal{P}[i]$. □

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

Let $O$ be an ordinal number and $p$ be a natural-valued polynomial of $O$,$\mathbb{R}_{\mathrm{F}}$. Let us observe that $\sum \mathtt{coeff}(p)$ is natural.

## 3. Selected Subsets of Zero Based Finite Sequences of $\mathbb{N}$ as Diophantine Sets

The scheme *SubsetDioph* deals with a natural number $n$ and a 4-ary predicate $\mathcal{P}$ and a set $\mathcal{S}$ and states that

(Sch. 2) For every elements $i_2$, $i_3$, $i_4$ of $n$, $\{p$, where $p$ is an $n$-element finite 0-sequence of $\mathbb{N}$ : for every natural number $i$ such that $i \in \mathcal{S}$ holds $\mathcal{P}[p(i), p(i_2), p(i_3), p(i_4)]\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$

provided

- for every elements $i_1$, $i_2$, $i_3$, $i_4$ of $n$, $\{p$, where $p$ is an $n$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}[p(i_1), p(i_2), p(i_3), p(i_4)]\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$ and
- $\mathcal{S} \subseteq \mathbb{Z}_n$.

Now we state the propositions:

(12) Suppose $n_1 + n_2 \leqslant n$.
Then $\{p : p(i_1) \geqslant k \cdot ((p(i_2))^{\mathbf{2}} + 1) \cdot (\prod(1 + p_{\lfloor n_1} \restriction n_2)) \cdot (l \cdot p(i_3) + m)^{i \cdot p(i_4) + j})\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$.
Proof: Define $\mathcal{F}_0$(natural number, natural number, natural number) $= {\$_1}^{\$_2}$. Define $\mathcal{P}_0$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv 1 \cdot \$_1 \geqslant k \cdot \$_3 + 0$. For every $i_1$, $i_2$, $i_3$, $i_4$, and $i_5$, $\{p : \mathcal{P}_0[p(i_1), p(i_2), \mathcal{F}_0(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$. Define $\mathcal{F}_1$(natural number, natural number, natural number) $= i \cdot \$_1 + j$. Define $\mathcal{P}_1$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 \geqslant k \cdot ({\$_2}^{\$_3})$. For every $i_1$, $i_2$, $i_3$, $i_4$, and $i_5$, $\{p : \mathcal{P}_1[p(i_1), p(i_2), \mathcal{F}_1(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$. Define $\mathcal{F}_2$(natural number, natural number, natural number) $= 1 \cdot \$_1 \cdot \$_2$.

Define $\mathcal{P}_2$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 \geqslant k \cdot ({\$_3}^{i \cdot \$_2 + j})$. For every $i_1$, $i_2$, $i_3$, $i_4$, and $i_5$, $\{p : \mathcal{P}_2[p(i_1), p(i_2), \mathcal{F}_2(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_3$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 \geqslant k \cdot (\$_6 \cdot {\$_3}^{i \cdot \$_2 + j})$. For every $i_1$, $i_2$, $i_3$, $i_4$, and $i_5$, $\{p : \mathcal{P}_3[p(i_1), p(i_2), \mathcal{F}_2(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$. Define $\mathcal{F}_5$(natural number, natural number, natural number) $= 1 \cdot \$_1 + 1$. Define $\mathcal{P}_5$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_1 \geqslant k \cdot (\$_3 \cdot \$_5 \cdot {\$_6}^{i \cdot \$_2 + j})$. For every $i_1$, $i_2$, $i_3$, $i_4$, and $i_5$, $\{p : \mathcal{P}_5[p(i_1), p(i_2), \mathcal{F}_5(p(i_3),$

$p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$. Define $\mathcal{G}(\text{natural number}, \text{natural number}, \text{natural number}) = l \cdot \$_1 + m$. Define $\mathcal{R}_1[\text{natural number}, \text{natural number}, \text{natural object}, \text{natural number}, \text{natural number}, \text{natural number}] \equiv \$_1 \geqslant k \cdot (\$_3 \cdot \$_5 \cdot (\$_6 + 1)^{i \cdot \$_2 + j})$. For every $i_1$, $i_2$, $i_3$, $i_4$, and $i_5$, $\{p : \mathcal{R}_1[p(i_1), p(i_2), \mathcal{G}(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_6[\text{natural number}, \text{natural number}, \text{natural object}, \text{natural number}, \text{natural number}, \text{natural number}] \equiv \$_1 \geqslant k \cdot ((\$_3 + 1) \cdot \$_5 \cdot (l \cdot \$_6 + m)^{i \cdot \$_2 + j})$. Define $\mathcal{F}_6(\text{natural number}, \text{natural number}, \text{natural number}) = 1 \cdot \$_1 \cdot \$_1$. For every $n$, $i_1$, $i_2$, $i_3$, $i_4$, and $i_5$, $\{p : \mathcal{P}_6[p(i_1), p(i_2), \mathcal{F}_6(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$. Set $X = n + 1$. Reconsider $N = n$, $I_1 = i_1$, $I_2 = i_2$, $I_3 = i_3$, $I_4 = i_4$ as an element of $X$. Define $\mathcal{P}_7[\text{finite 0-sequence of } \mathbb{N}] \equiv \$_1(I_1) \geqslant k \cdot ((1 \cdot \$_1(I_2) \cdot \$_1(I_2) + 1) \cdot \$_1(N) \cdot (l \cdot \$_1(I_3) + m)^{i \cdot \$_1(I_4) + j})$. Define $\mathcal{Q}_7[\text{finite 0-sequence of } \mathbb{N}] \equiv \$_1(N) = \prod(1 + \$_{1\,\lfloor n_1} \restriction n_2)$. Set $P_1 = \{p$, where $p$ is an $X$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_7[p]$ and $\mathcal{Q}_7[p]\}$. $P_1$ is a Diophantine subset of the $X$-xtuples of $\mathbb{N}$. Define $\mathcal{S}[\text{finite 0-sequence of } \mathbb{N}] \equiv \$_1(i_1) \geqslant k \cdot ((\$_1(i_2)^{\mathbf{2}} + 1) \cdot (\prod(1 + \$_{1\,\lfloor n_1} \restriction n_2)) \cdot (l \cdot \$_1(i_3) + m)^{i \cdot \$_1(i_4) + j})$. Set $S = \{p : \mathcal{S}[p]\}$. $S \subseteq$ the $n$-xtuples of $\mathbb{N}$. □

(13) Let us consider a $\mathbb{Z}$-valued polynomial $P$ of $k$,$\mathbb{R}_{\mathrm{F}}$, an integer $a$, a permutation $p_2$ of $n$, and $i_1$. Suppose $k \leqslant n$. Then $\{p$ : for every $k$-element finite 0-sequence $q$ of $\mathbb{N}$ such that $q = p \cdot p_2 \restriction k$ holds $a \cdot p(i_1) = \operatorname{eval}(P, {}^{@}q)\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$.

(14) Let us consider a $\mathbb{Z}$-valued polynomial $P$ of $k+1$,$\mathbb{R}_{\mathrm{F}}$, an integer $a$, $n$, $i_1$, and $i_2$. Suppose $k + 1 \leqslant n$ and $k \in i_2$. Then $\{p$ : for every $(k+1)$-element finite 0-sequence $q$ of $\mathbb{N}$ such that $q = \langle p(i_2) \rangle \frown (p \restriction k)$ holds $a \cdot p(i_1) = \operatorname{eval}(P, {}^{@}q)\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$.

Proof: Set $k_1 = k + 1$. Reconsider $I_5 = \mathrm{id}_k$ as a finite 0-sequence. Set $f = \langle i_2 \rangle \frown I_5$. Set $R = \operatorname{rng} f$. Consider $g$ being a function such that $g$ is one-to-one and $\operatorname{dom} g = n \setminus k_1$ and $\operatorname{rng} g = n \setminus R$. Reconsider $f_1 = f {+\cdot} g$ as a function from $n$ into $n$. Define $\mathcal{Q}[\text{finite 0-sequence of } \mathbb{N}] \equiv$ for every $k_1$-element finite 0-sequence $q$ of $\mathbb{N}$ such that $q = \$_1 \cdot f_1 \restriction k_1$ holds $a \cdot \$_1(i_1) = \operatorname{eval}(P, {}^{@}q)$. Define $\mathcal{R}[\text{finite 0-sequence of } \mathbb{N}] \equiv$ for every $(k+1)$-element finite 0-sequence $q$ of $\mathbb{N}$ such that $q = \langle \$_1(i_2) \rangle \frown (\$_1 \restriction k)$ holds $a \cdot \$_1(i_1) = \operatorname{eval}(P, {}^{@}q)$. For every $n$-element finite 0-sequence $p$ of $\mathbb{N}$, $\mathcal{Q}[p]$ iff $\mathcal{R}[p]$. $\{p : \mathcal{Q}[p]\} = \{q : \mathcal{R}[q]\}$. □

(15) Let us consider a $\mathbb{Z}$-valued polynomial $P$ of $k{+}1$,$\mathbb{R}_{\mathrm{F}}$, $n$, $i_1$, and $i_2$. Suppose $k + 1 \leqslant n$ and $k \in i_1$. Then $\{p$ : for every $(k+1)$-element finite 0-sequence $q$ of $\mathbb{N}$ such that $q = \langle p(i_1) \rangle \frown (p \restriction k)$ holds $\operatorname{eval}(P, {}^{@}q) \equiv 0 \pmod{p(i_2)}\}$ is

a Diophantine subset of the $n$-xtuples of $\mathbb{N}$.

PROOF: Set $k_1 = k + 1$. Set $X = n + 1$. Reconsider $N = n$, $I_1 = i_1$, $I_2 = i_2$ as an element of $X$. Define $\mathcal{P}$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(N) \equiv 0 \cdot \$_1(I_1) \pmod{1 \cdot \$_1(I_2)}$. Define $\mathcal{O}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every $k_1$-element finite 0-sequence $q$ of $\mathbb{N}$ such that $q = \langle \$_1(I_1) \rangle \frown (\$_1 \restriction k)$ holds $1 \cdot \$_1(N) = \mathrm{eval}(P, {}^{@}q)$. Define $\mathcal{M}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every $k_1$-element finite 0-sequence $q$ of $\mathbb{N}$ such that $q = \langle \$_1(I_1) \rangle \frown (\$_1 \restriction k)$ holds $(-1) \cdot \$_1(N) = \mathrm{eval}(P, {}^{@}q)$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{O}[\$_1]$ or $\mathcal{M}[\$_1]$. $\{p$, where $p$ is an $X$-element finite 0-sequence of $\mathbb{N} : \mathcal{O}[p]\}$ is a Diophantine subset of the $X$-xtuples of $\mathbb{N}$. $\{p$, where $p$ is an $X$-element finite 0-sequence of $\mathbb{N} : \mathcal{M}[p]\}$ is a Diophantine subset of the $X$-xtuples of $\mathbb{N}$. $\{p$, where $p$ is an $X$-element finite 0-sequence of $\mathbb{N} : \mathcal{O}[p]$ or $\mathcal{M}[p]\}$ is a Diophantine subset of the $X$-xtuples of $\mathbb{N}$. Set $P_1 = \{p$, where $p$ is an $X$-element finite 0-sequence of $\mathbb{N} : \mathcal{P}[p]$ and $\mathcal{Q}[p]\}$. $P_1$ is a Diophantine subset of the $X$-xtuples of $\mathbb{N}$.

Set $P_2 = \{p \restriction n$, where $p$ is an $X$-element finite 0-sequence of $\mathbb{N} : p \in P_1\}$. Define $\mathcal{S}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every $k_1$-element finite 0-sequence $q$ of $\mathbb{N}$ such that $q = \langle \$_1(i_1) \rangle \frown (\$_1 \restriction k)$ holds $\mathrm{eval}(P, {}^{@}q) \equiv 0 \pmod{\$_1 (i_2)}$. Set $S = \{p : \mathcal{S}[p]\}$. $S \subseteq P_2$. $P_2 \subseteq S$. $\square$

## 4. BOUNDED QUANTIFIER THEOREM AND ITS VARIANT

Let us consider a $\mathbb{Z}$-valued polynomial $p$ of $2 + n + k, \mathbb{R}_{\mathrm{F}}$, an $n$-element finite 0-sequence $X$ of $\mathbb{N}$, and an element $x$ of $\mathbb{N}$. Now we state the propositions:

(16) For every element $z$ of $\mathbb{N}$ such that $z \leqslant x$ there exists a $k$-element finite 0-sequence $y$ of $\mathbb{N}$ such that $\mathrm{eval}(p, {}^{@}((\langle z, x \rangle \frown X) \frown y)) = 0$ if and only if there exists a $k$-element finite 0-sequence $Y$ of $\mathbb{N}$ and there exist elements $Z$, $e$, $K$ of $\mathbb{N}$ such that $K > x$ and $K \geqslant (\sum \mathtt{coeff}(|p|)) \cdot ((x^{\mathbf{2}} + 1) \cdot (\prod(1 + X)) \cdot e^{\mathrm{degree}(p)})$ and for every natural number $i$ such that $i \in k$ holds $Y(i) > e$ and $e > x$ and $1+(Z+1)\cdot(K!) = \prod(1+K!\cdot(\mathrm{idseq}(x+1)))$ and $\mathrm{eval}(p, {}^{@}((\langle Z, x \rangle \frown X) \frown Y)) \equiv 0 \pmod{1 + (Z + 1) \cdot (K!)}$ and for every natural number $i$ such that $i \in k$ holds $\prod(Y(i) + 1 + -\mathrm{idseq}(e)) \equiv 0 \pmod{1 + (Z + 1) \cdot (K!)}$.

PROOF: If for every element $z$ of $\mathbb{N}$ such that $z \leqslant x$ there exists a $k$-element finite 0-sequence $y$ of $\mathbb{N}$ such that $\mathrm{eval}(p, {}^{@}((\langle z, x \rangle \frown X) \frown y)) = 0$, then there exists a $k$-element finite 0-sequence $Y$ of $\mathbb{N}$ and there exist elements $Z$, $e$, $K$ of $\mathbb{N}$ such that $K > x$ and $K \geqslant (\sum \mathtt{coeff}(|p|)) \cdot ((x^{\mathbf{2}} + 1) \cdot (\prod(1 + X)) \cdot e^{\mathrm{degree}(p)})$ and for every natural number $i$ such that $i \in k$ holds $Y(i) > e$ and $e > x$ and $1+(Z+1)\cdot(K!) = \prod(1+K!\cdot(\mathrm{idseq}(x+$

1))) and $\text{eval}(p, {}^{@}((\langle Z, x\rangle \frown X) \frown Y)) \equiv 0 \pmod{1 + (Z+1)\cdot(K!)}$ and for every natural number $i$ such that $i \in k$ holds $\prod(Y(i) + 1 + -\text{idseq}(e)) \equiv 0 \pmod{1+(Z+1)\cdot(K!)}$. Set $K_1 = K!$. Set $z_1 = 1+(z+1)\cdot K_1$. Consider $p_3$ being an element of $\mathbb{N}$ such that $p_3 \mid z_1$ and $p_3 \leqslant z_1$ and $p_3$ is prime. Define $\mathcal{P}(\text{object}) = Y(\$_1) \bmod p_3$.

Consider $Y_3$ being a finite 0-sequence such that $\text{len}\, Y_3 = k$ and for every natural number $i$ such that $i \in k$ holds $Y_3(i) = \mathcal{P}(i)$. $\text{rng}\, Y_3 \subseteq \mathbb{N}$. Reconsider $E_1 = \text{eval}(p, {}^{@}((\langle Z, x\rangle \frown X) \frown Y))$ as an integer. $K < p_3$. For every $i$ such that $i \in 2+k+n$ holds $p_3 \mid (((\langle Z,x\rangle \frown X)\frown Y)(i) - (((\langle z,x\rangle \frown X)\frown Y_3)(i)$. $p_3 \mid E_1 - \text{eval}(p, {}^{@}((\langle z, x\rangle \frown X) \frown Y_3))$. Consider $m$ being a natural number such that $|\text{eval}(p, {}^{@}((\langle z, x\rangle \frown X) \frown Y_3))| = p_3 \cdot m$. For every object $i$ such that $i \in \text{dom}({}^{@}((\langle z,x\rangle \frown X)\frown Y_3))$ holds $|({}^{@}((\langle z,x\rangle \frown X)\frown Y_3))(i)| \leqslant (x^{\mathbf{2}}+1)\cdot(\prod(1+X))\cdot e$. $|\text{eval}(p, {}^{@}((\langle z,x\rangle \frown X)\frown Y_3))| \leqslant (\sum \texttt{coeff}(|p|)) \cdot ((x^{\mathbf{2}}+1)\cdot(\prod(1+X))\cdot e^{\text{degree}(p)})$. □

(17) For every element $z$ of $\mathbb{N}$ such that $z \leqslant x$ there exists a $k$-element finite 0-sequence $y$ of $\mathbb{N}$ such that for every $i$ such that $i \in k$ holds $y(i) \leqslant x$ and $\text{eval}(p, {}^{@}((\langle z,x\rangle \frown X)\frown y)) = 0$ if and only if there exists a $k$-element finite 0-sequence $Y$ of $\mathbb{N}$ and there exist elements $Z$, $K$ of $\mathbb{N}$ such that $K > x$ and $K \geqslant (\sum \texttt{coeff}(|p|))\cdot((x^{\mathbf{2}}+1)\cdot(\prod(1+X))^{\text{degree}(p)})$ and for every natural number $i$ such that $i \in k$ holds $Y(i) > x+1$ and $1+(Z+1)\cdot(K!) = \prod(1+K!\cdot(\text{idseq}(x+1)))$ and $\text{eval}(p, {}^{@}((\langle Z,x\rangle \frown X)\frown Y)) \equiv 0 \pmod{1+(Z+1)\cdot(K!)}$ and for every natural number $i$ such that $i \in k$ holds $\prod(Y(i)+1+-\text{idseq}(x+1)) \equiv 0 \pmod{1+(Z+1)\cdot(K!)}$.

PROOF: Set $x_1 = x+1$. If for every element $z$ of $\mathbb{N}$ such that $z \leqslant x$ there exists a $k$-element finite 0-sequence $y$ of $\mathbb{N}$ such that for every $i$ such that $i \in k$ holds $y(i) \leqslant x$ and $\text{eval}(p, {}^{@}((\langle z,x\rangle \frown X)\frown y)) = 0$, then there exists a $k$-element finite 0-sequence $Y$ of $\mathbb{N}$ and there exist elements $Z$, $K$ of $\mathbb{N}$ such that $K > x$ and $K \geqslant (\sum \texttt{coeff}(|p|))\cdot((x^{\mathbf{2}}+1)\cdot(\prod(1+X))^{\text{degree}(p)})$ and for every natural number $i$ such that $i \in k$ holds $Y(i) > x_1$ and $1+(Z+1)\cdot(K!) = \prod(1+K!\cdot(\text{idseq}(x+1)))$ and $\text{eval}(p, {}^{@}((\langle Z,x\rangle \frown X)\frown Y)) \equiv 0 \pmod{1+(Z+1)\cdot(K!)}$ and for every natural number $i$ such that $i \in k$ holds $\prod(Y(i)+1+-\text{idseq}(x_1)) \equiv 0 \pmod{1+(Z+1)\cdot(K!)}$. Set $K_1 = K!$. Set $z_1 = 1+(z+1)\cdot K_1$.

Consider $p_3$ being an element of $\mathbb{N}$ such that $p_3 \mid z_1$ and $p_3 \leqslant z_1$ and $p_3$ is prime. Define $\mathcal{P}(\text{object}) = Y(\$_1) \bmod p_3$. Consider $Y_3$ being a finite 0-sequence such that $\text{len}\, Y_3 = k$ and for every natural number $i$ such that $i \in k$ holds $Y_3(i) = \mathcal{P}(i)$. $\text{rng}\, Y_3 \subseteq \mathbb{N}$. Reconsider $E_1 = \text{eval}(p, {}^{@}((\langle Z,x\rangle \frown X)\frown Y))$ as an integer. $K < p_3$. For every natural number $i$ such that $i \in k$ holds $Y_3(i) \leqslant x$. For every $i$ such that $i \in 2+k+n$ holds $p_3 \mid (((\langle Z,x\rangle \frown X)\frown Y)(i) - (((\langle z,x\rangle \frown X)\frown Y_3)(i)$. $p_3 \mid E_1 - \text{eval}(p, {}^{@}((\langle z,x\rangle \frown X)\frown Y_3))$. Consider

$m$ being a natural number such that $|\operatorname{eval}(p, {}^{@}((\langle z, x\rangle ^\frown X) ^\frown Y_3))| = p_3 \cdot m$. For every object $i$ such that $i \in \operatorname{dom}({}^{@}((\langle z, x\rangle ^\frown X) ^\frown Y_3))$ holds $|({}^{@}((\langle z, x\rangle ^\frown X) ^\frown Y_3))(i)| \leqslant (x^{\mathbf{2}} + 1) \cdot (\prod(1 + X))$. $|\operatorname{eval}(p, {}^{@}((\langle z, x\rangle ^\frown X) ^\frown Y_3))| \leqslant (\sum \mathtt{coeff}(|p|)) \cdot ((x^{\mathbf{2}} + 1) \cdot (\prod(1 + X))^{\operatorname{degree}(p)})$. $\square$

Let us consider a $\mathbb{Z}$-valued polynomial $p$ of $2 + n + k$,$\mathbb{R}_{\mathrm{F}}$. Now we state the propositions:

(18) $\{X$, where $X$ is an $n$-element finite 0-sequence of $\mathbb{N}$ : there exists an element $x$ of $\mathbb{N}$ such that for every element $z$ of $\mathbb{N}$ such that $z \leqslant x$ there exists a $k$-element finite 0-sequence $y$ of $\mathbb{N}$ such that $\operatorname{eval}(p, {}^{@}((\langle z, x\rangle ^\frown X) ^\frown y)) = 0\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$.

PROOF: Set $X_0 = \{X$, where $X$ is an $n$-element finite 0-sequence of $\mathbb{N}$ : there exists an element $x$ of $\mathbb{N}$ such that for every element $z$ of $\mathbb{N}$ such that $z \leqslant x$ there exists a $k$-element finite 0-sequence $y$ of $\mathbb{N}$ such that $\operatorname{eval}(p, {}^{@}((\langle z, x\rangle ^\frown X) ^\frown y)) = 0\}$. Set $n_1 = 1+n+k$. Set $s_4 = \sum \mathtt{coeff}(|p|)$. Set $D = \operatorname{degree}(p)$. Reconsider $Z_0 = 0$, $i_0 = n_1$, $i_1 = n_1 + 1$, $i_2 = n_1 + 2$, $i_3 = n_1 + 3$ as an element of $n_1 + 4$. Define $\mathcal{P}_2$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $1 \cdot \$_1(i_1) > 1 \cdot \$_1(Z_0) + 0$. Define $\mathcal{P}_3$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(i_1) \geqslant s_4 \cdot ((\$_1(Z_0)^{\mathbf{2}} + 1) \cdot (\prod(1 + \$_{1\,\downharpoonright 1}\restriction n)) \cdot (1 \cdot \$_1(i_0) + 0)^{0 \cdot \$_1(i_0)+D})$. $\{q$, where $q$ is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_3[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_4$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every natural number $i$ such that $i \in k$ holds $\$_1(1+n+i) > \$_1(i_0)$ and $\prod(\$_1(1+n+i)+1+-\operatorname{idseq}(\$_1(i_0))) \equiv 0 \pmod{\$_1(i_2)}$. $\{q$, where $q$ is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_4[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_5$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(i_0) > 1 \cdot \$_1(Z_0) + 0$. Define $\mathcal{P}_6$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 + (\$_1(i_3)+1) \cdot (\$_1(i_1)!) = \$_1(i_2)$. Define $\mathcal{P}_7$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(i_2) = \prod(1+\$_1(i_1)! \cdot (\operatorname{idseq}(1+\$_1(Z_0))))$. Reconsider $R = p$ as a $\mathbb{Z}$-valued polynomial of $1 + n_1$,$\mathbb{R}_{\mathrm{F}}$. Define $\mathcal{P}_8$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every $(1+n_1)$-element finite 0-sequence $Y$ of $\mathbb{N}$ such that $Y = \langle \$_1(i_3)\rangle ^\frown (\$_1 \restriction n_1)$ holds $\operatorname{eval}(R, {}^{@}Y) \equiv 0 \pmod{\$_1(i_2)}$. $\{q$, where $q$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_8[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_{123}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_2[\$_1]$ and $\mathcal{P}_3[\$_1]$. $\{q$, where $q$ is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{123}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{123}[\$_1]$ and $\mathcal{P}_4[\$_1]$. $\{q$, where $q$ is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{1234}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{12345}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{1234}[\$_1]$ and $\mathcal{P}_5[\$_1]$. $\{q$, where $q$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{12345}[q]\}$ is a Diophantine subset of the $n_1+4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{123456}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{12345}[\$_1]$ and $\mathcal{P}_6[\$_1]$. $\{q$, where $q$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{123456}[q]\}$ is a Diophantine subset of the $n_1+4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234567}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{123456}[\$_1]$ and $\mathcal{P}_7[\$_1]$. $\{q$, where $q$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{1234567}[q]\}$ is a Diophantine subset of the $n_1+4$-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_{12345678}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{1234567}[\$_1]$ and $\mathcal{P}_8[\$_1]$. Set $X_3 = \{q$, where $q$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{12345678}[q]\}$. $X_3$ is a Diophantine subset of the $n_1+4$-xtuples of $\mathbb{N}$. Set $X_2 = \{X \restriction (n+1)$, where $X$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $X \in X_3\}$. Define $\mathcal{S}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every element $z$ of $\mathbb{N}$ such that $z \leqslant \$_1(0)$ there exists a $k$-element finite 0-sequence $y$ of $\mathbb{N}$ such that for every $n$-element finite 0-sequence $X_1$ of $\mathbb{N}$ such that $X_1 = \$_{1\lfloor 1}$ holds eval$(p, {}^{@}((\langle z, \$_1(0)\rangle \frown X_1) \frown y)) = 0$. Set $X_1 = \{X$, where $X$ is an $(n+1)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{S}[X]\}$. For every object $s$, $s \in X_1$ iff $s \in X_2$. Set $Y_1 = \{X_{\lfloor 1}$, where $X$ is an $(n+1)$-element finite 0-sequence of $\mathbb{N}$ : $X \in X_1\}$. For every object $s$, $s \in Y_1$ iff $s \in X_0$. □

(19) $\{X$, where $X$ is an $n$-element finite 0-sequence of $\mathbb{N}$ : there exists an element $x$ of $\mathbb{N}$ such that for every element $z$ of $\mathbb{N}$ such that $z \leqslant x$ there exists a $k$-element finite 0-sequence $y$ of $\mathbb{N}$ such that for every natural number $i$ such that $i \in k$ holds $y(i) \leqslant x$ and eval$(p, {}^{@}((\langle z, x\rangle \frown X) \frown y)) = 0\}$ is a Diophantine subset of the $n$-xtuples of $\mathbb{N}$.

PROOF: Set $X_0 = \{X$, where $X$ is an $n$-element finite 0-sequence of $\mathbb{N}$ : there exists an element $x$ of $\mathbb{N}$ such that for every element $z$ of $\mathbb{N}$ such that $z \leqslant x$ there exists a $k$-element finite 0-sequence $y$ of $\mathbb{N}$ such that for every natural number $i$ such that $i \in k$ holds $y(i) \leqslant x$ and eval$(p, {}^{@}((\langle z, x\rangle \frown X) \frown y)) = 0\}$. Set $n_1 = 1 + n + k$. Set $s_4 = \sum \texttt{coeff}(|p|)$. Set $D =$ degree$(p)$. Reconsider $Z_0 = 0$, $i_0 = n_1$, $i_1 = n_1 + 1$, $i_2 = n_1 + 2$, $i_3 = n_1 + 3$ as an element of $n_1 + 4$. Define $\mathcal{P}_2$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(i_1) > 1 \cdot \$_1(Z_0) + 0$. Define $\mathcal{P}_3$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i_1) \geqslant s_4 \cdot ((\$_1(Z_0)^{\mathbf{2}} + 1) \cdot (\prod(1 + \$_{1\lfloor 1}\restriction n)) \cdot (0 \cdot \$_1(i_0) + 1)^{0 \cdot \$_1(i_0) + D})$. $\{q$, where $q$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_3[q]\}$ is a Diophantine subset of the $n_1+4$-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_4$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every natural number $i$ such that $i \in k$ holds $\$_1(1+n+i) > \$_1(i_0)$ and $\prod(\$_1(1+n+i)+1+-\text{idseq}(\$_1(i_0))) \equiv 0 \pmod{\$_1(i_2)}$. $\{q$, where $q$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_4[q]\}$ is a Diophantine subset of the $n_1+4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_5$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i_0) = 1 \cdot \$_1(Z_0) + 1$. Define $\mathcal{P}_6$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 + (\$_1(i_3)+1) \cdot (\$_1(i_1)!) = \$_1(i_2)$. Define $\mathcal{P}_7$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i_2) = \prod(1+\$_1(i_1)! \cdot (\text{idseq}(1+\$_1(Z_0))))$. Reconsider $R = p$ as a $\mathbb{Z}$-valued polynomial of $1 + n_1$,$\mathbb{R}_F$. Define $\mathcal{P}_8$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every $(1+n_1)$-element finite 0-sequence $Y$ of $\mathbb{N}$ such that $Y = \langle \$_1(i_3)\rangle \frown (\$_1 \restriction n_1)$ holds eval($R$, $^{@}Y$) $\equiv 0 \pmod{\$_1(i_2)}$. $\{q$, where $q$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_8[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$.

Define $\mathcal{P}_{123}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_2[\$_1]$ and $\mathcal{P}_3[\$_1]$. $\{q$, where $q$ is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{123}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{123}[\$_1]$ and $\mathcal{P}_4[\$_1]$. $\{q$, where $q$ is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{1234}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{12345}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{1234}[\$_1]$ and $\mathcal{P}_5[\$_1]$. $\{q$, where $q$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{12345}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{123456}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{12345}[\$_1]$ and $\mathcal{P}_6[\$_1]$. $\{q$, where $q$ is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{123456}[q]\}$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{1234567}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}_{123456}[\$_1]$ and $\mathcal{P}_7[\$_1]$. $\{q$, where $q$ is an $(n_1 + 4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{1234567}[q]\}$ is a Diophantine subset of the $n_1+4$-xtuples of $\mathbb{N}$. Define $\mathcal{P}_{12345678}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\mathcal{P}_{1234567}[\$_1]$ and $\mathcal{P}_8[\$_1]$. Set $X_3 = \{q$, where $q$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{P}_{12345678}[q]\}$. $X_3$ is a Diophantine subset of the $n_1 + 4$-xtuples of $\mathbb{N}$. Set $X_2 = \{X \restriction (n+1)$, where $X$ is an $(n_1+4)$-element finite 0-sequence of $\mathbb{N}$ : $X \in X_3\}$.

Define $\mathcal{S}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ for every element $z$ of $\mathbb{N}$ such that $z \leqslant \$_1(0)$ there exists a $k$-element finite 0-sequence $y$ of $\mathbb{N}$ such that for every $n$-element finite 0-sequence $X_1$ of $\mathbb{N}$ such that $X_1 = \$_{1 \downharpoonleft 1}$ holds for every $i$ such that $i \in k$ holds $y(i) \leqslant \$_1(0)$ and eval($p$, $^{@}((\langle z, \$_1(0)\rangle \frown X_1) \frown y)) = 0$. Set $X_1 = \{X$, where $X$ is an $(n + 1)$-element finite 0-sequence of $\mathbb{N}$ : $\mathcal{S}[X]\}$. For every object $s$, $s \in X_1$ iff $s \in X_2$. Set $Y_1 = \{X_{\downharpoonleft 1}$, where $X$ is an $(n+1)$-element finite 0-sequence of $\mathbb{N}$ : $X \in X_1\}$. For every object $s$, $s \in Y_1$ iff $s \in X_0$. □

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

(Def. 4) there exists a natural number $m$ and there exists a $\mathbb{Z}$-valued polynomial $P$ of $2 + n + m$,$\mathbb{R}_F$ such that for every $n$-element finite 0-sequence $X$ of $\mathbb{N}$, $X \in A$ iff there exists an element $x$ of $\mathbb{N}$ such that for every element $z$ of $\mathbb{N}$ such that $z \leqslant x$ there exists an $m$-element finite 0-sequence $Y$ of $\mathbb{N}$ such that for every object $i$ such that $i \in \operatorname{dom} Y$ holds $Y(i) \leqslant x$ and eval($P$, $^{@}((\langle z, x\rangle \frown X) \frown Y)) = 0$.

Now we state the proposition:

(20) Let us consider a natural number $n$, and a subset $A$ of the $n$-xtuples of $\mathbb{N}$. If $A$ is Diophantine, then $A$ is recursively enumerable.

PROOF: Consider $m$ being a natural number, $P$ being a $\mathbb{Z}$-valued polynomial of $n+m$,$\mathbb{R}_{\mathrm{F}}$ such that for every object $s$, $s \in A$ 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 $\mathrm{eval}(P, {}^{@}(x^\frown y)) = 0$. Set $n_4 = n+m$. Reconsider $\mathrm{P}_0 = P$ as a $\mathbb{Z}$-valued polynomial of $0+n_4$,$\mathbb{R}_{\mathrm{F}}$. Consider $q$ being a polynomial of $0+2+n_4$,$\mathbb{R}_{\mathrm{F}}$ such that $\mathrm{rng}\, q \subseteq \mathrm{rng}\, \mathrm{P}_0 \cup \{0_{\mathbb{R}_{\mathrm{F}}}\}$ and for every function $x_1$ from $0+n_4$ into $\mathbb{R}_{\mathrm{F}}$ and for every function $X_1$ from $0+2+n_4$ into $\mathbb{R}_{\mathrm{F}}$ such that $x_1 \restriction 0 = X_1 \restriction 0$ and $({}^{@}x_1)_{\lfloor 0} = ({}^{@}X_1)_{\lfloor 0+2}$ holds $\mathrm{eval}(\mathrm{P}_0, x_1) = \mathrm{eval}(q, X_1)$.

Reconsider $Q = q$ as a $\mathbb{Z}$-valued polynomial of $2+n+m$,$\mathbb{R}_{\mathrm{F}}$. If $X \in A$, then there exists an element $x$ of $\mathbb{N}$ such that for every element $z$ of $\mathbb{N}$ such that $z \leqslant x$ there exists an $m$-element finite 0-sequence $Y$ of $\mathbb{N}$ such that for every object $i$ such that $i \in \mathrm{dom}\, Y$ holds $Y(i) \leqslant x$ and $\mathrm{eval}(Q, {}^{@}((\langle z, x\rangle \frown X) \frown Y)) = 0$. Consider $y$ being an $m$-element finite 0-sequence of $\mathbb{N}$ such that for every object $i$ such that $i \in \mathrm{dom}\, y$ holds $y(i) \leqslant a$ and $\mathrm{eval}(Q, {}^{@}((\langle a, a\rangle \frown X) \frown y)) = 0$. $\square$

## 5. MRDP Theorem

Now we state the proposition:

(21) YURI MATIYASEVICH, JULIA ROBINSON, MARTIN DAVIS, HILARY PUTNAM THEOREM:

Let us consider a natural number $n$, and a subset $A$ of the $n$-xtuples of $\mathbb{N}$. If $A$ is recursively enumerable, then $A$ is Diophantine. The theorem is a consequence of (19).

## References

[1] Marcin Acewicz and Karol Pąk. Basic Diophantine relations. *Formalized Mathematics*, 26(**2**):175–181, 2018. doi:10.2478/forma-2018-0015.

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

[3] 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.

[4] 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.

[5] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[6] Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly, Mathematical Association of America*, 80(3):233–269, 1973. doi:10.2307/2318447.

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

[9] Karol Pąk. Diophantine sets. Part II. *Formalized Mathematics*, 27(**2**):197–208, 2019. doi:10.2478/forma-2019-0019.

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

*Accepted May 27, 2019*