

M. Carl, B. Z. Moroz

ON A DIOPHANTINE REPRESENTATION OF THE PREDICATE OF PROVABILITY

ABSTRACT. Let \mathcal{P} be the first order predicate calculus with a single binary predicate letter. Making use of the techniques of Diophantine coding developed in the works on Hilbert tenth problem, we construct a polynomial $F(t; x_1, \dots, x_n)$ with integral rational coefficients such that the Diophantine equation

$$F(t_0; x_1, \dots, x_n) = 0$$

is soluble in integers if and only if the formula of \mathcal{P} , numbered t_0 in the chosen numbering of the formulae of \mathcal{P} , is provable in \mathcal{P} . As an application of that construction, we describe a class of Diophantine equations which can be proved insoluble only under some additional axioms of the axiomatic set theory, for instance, assuming existence of an inaccessible cardinal.

§1. INTRODUCTION

By a well-known theorem of Matiyasevich [10, 11], a recursively enumerable set is Diophantine, and therefore there is no algorithm, deciding whether a given Diophantine equation is soluble in \mathbb{Z} . Moreover, given a recursively enumerable set S , one can actually construct a polynomial $P_S(t, \vec{x})$ in $\mathbb{Z}[t, \vec{x}]$, $\vec{x} := (x_1, \dots, x_n)$, such that

$$S = \{a \mid a \in \mathbb{N}, \exists \vec{b} (\vec{b} \in \mathbb{Z}^n \ \& \ P_S(a, \vec{b}) = 0)\}.$$

The set of the theorems in a formalised mathematical theory, say \mathcal{T} , being recursively enumerable, is Diophantine (cf. [3, pp. 327–328], [4]); therefore one can construct a polynomial $F_{\mathcal{T}}(t, \vec{x})$ in $\mathbb{Z}[t, \vec{x}]$ such that the Diophantine equation

$$F_{\mathcal{T}}(a, \vec{x}) = 0$$

is soluble in \mathbb{Z} if and only if $a = \mathcal{N}(\mathfrak{A})$ for a formula \mathfrak{A} provable in \mathcal{T} , where

$$\mathcal{N}: \mathfrak{F} \rightarrow \mathbb{N}$$

Key words and phrases: Diophantine coding, Matiyasevich's theorem, Pell's equation, Gödel-Bernays set theory.

is a suitable numbering of the set \mathfrak{F} of the well-formed formulae of \mathcal{T} . However such a polynomial $F_{\mathcal{T}}$ has not been so far constructed for any non-trivial theory \mathcal{T} . The goal of this work is to construct a polynomial $F_{\mathcal{S}}$, which encodes provability in the Gödel–Bernays axiomatic set theory \mathcal{S} . Since, as it is commonly assumed, any mathematical proof can be formalised in \mathcal{S} , one may say that the polynomial $F_{\mathcal{S}}(t, \vec{x})$ encodes the content of pure mathematics; in this sense, the arithmetic of the affine hypersurface, defined by the equation

$$F_{\mathcal{S}}(t, \vec{x}) = 0,$$

is “exactly as difficult as the whole of mathematics” (cf. [9, p. 2]). As a by-product of our construction, one encounters a presumably true mathematical statement of the shape

$$V(\mathbb{Z}) = \emptyset, \tag{1}$$

where V is a hypersurface defined over \mathbb{Z} , that can not be proved in \mathcal{S} (or, say, in the Zermelo–Fraenkel set theory) if \mathcal{S} is consistent, and for its proof requires new “axioms, which go beyond the usual axioms for mathematics,” cf. [5, p. 804]. Our arithmetic statement (1) seems to be simpler and by far more natural than those combinatorial statements presented in the work of H. M. Friedman we have just cited (an interested reader is referred, however, to Friedman’s new preprints for his latest results in the spirit of [5]). In point of fact, on letting

$$b = \mathcal{N}(\mathfrak{B})$$

for a formula \mathfrak{B} (obviously) false in \mathcal{S} , one obtains a Diophantine equation

$$F_{\mathcal{S}}(b, \vec{x}) = 0, \tag{2}$$

whose insolubility is equivalent to the consistency of \mathcal{S} . Thus in order to prove that Eq. (2) has no solutions in \mathbb{Z} , one has to employ an additional axiom, for instance, the axiom asserting existence of an inaccessible cardinal (cf. [5], where some combinatorial statements, whose provability depends on that axiom, have been constructed).

The Gödel–Bernays set theory \mathcal{S} is finitely axiomatisable in the first order predicate calculus \mathcal{P} with a single binary predicate letter (and no function letters or individual constants) [6], [14, Chap. 4]. By Kalmár’s theorem [8], (cf. also [14, p. 223]), analysis of provability in any first order pure predicate calculus can be reduced to studying provability in \mathcal{P} . In what follows we construct a polynomial $F_{\mathcal{P}}(t, \vec{x})$, encoding provability in \mathcal{P} .

Let \mathfrak{A}_0 denote the conjunction of the proper (non-logical) axioms of \mathcal{S} . Since a formula \mathfrak{B} is a theorem in \mathcal{S} if and only if the formula $(\mathfrak{A}_0 \supset \mathfrak{B})$ is a theorem in \mathcal{P} , the polynomial $F_{\mathcal{S}}$ is easily expressible in terms of $F_{\mathcal{P}}$.

As any other polynomial with integral rational coefficients, the polynomial $F_{\mathcal{P}}$ is a special instance of an universal polynomial (the reader may consult references [7], [12, Chap. 4], and the literature cited in those works for different constructions of an universal polynomial). If the Gödel–Bernays set theory \mathcal{S} is consistent, then the formula

$$(\mathfrak{A}_0 \supset \exists \vec{b} (\vec{b} \in \mathbb{Z}^n \ \& \ f(\vec{b}) = 0)),$$

with $f(\vec{x}) \in \mathbb{Z}[\vec{x}]$, $\vec{x} := (x_1, \dots, x_n)$, is provable in \mathcal{P} if and only if equation $f(\vec{x}) = 0$ is soluble in \mathbb{Z} ; thus, under that assumption, $F_{\mathcal{P}}(t, \vec{x})$ is an universal polynomial (it suffices, of course, to assume the consistency of any theory \mathcal{T} formalisable in \mathcal{P} and such that the formula

$$\exists \vec{b} (\vec{b} \in \mathbb{Z}^n \ \& \ f(\vec{b}) = 0)$$

is provable in \mathcal{T} if and only if the equation $f(\vec{x}) = 0$ is soluble in \mathbb{Z}).

Although one does not expect a polynomial, encoding provability in pure mathematics, to be too simple, it is not known how complicated it *must* be. Both the polynomial $F_{\mathcal{P}}(t, \vec{x})$ constructed in this work and a similar polynomial described in [1] are rather involved; those polynomials can be, however, explicitly written down.

This paper is organised as follows. In Sec. 2, we describe the language of \mathcal{P} , define a numbering

$$\mathcal{N}: \mathcal{P} \rightarrow \mathbb{N},$$

and give a Diophantine description of the first three groups of the axioms of \mathcal{P} . The necessary preliminaries on Diophantine coding are collected in Sec. 3. After proving a few technical lemmata in Sec. 4, we complete the description of the axioms of \mathcal{P} in Sec. 5. Our polynomial $F_{\mathcal{P}}(t, \vec{x})$ is described at the end of Sec. 6; an example of a Diophantine equation of the shape (2), whose insolubility is equivalent to the consistency of the Gödel–Bernays system \mathcal{S} , is given at the end of Sec. 7 (see also §8 for some calculations relating to the description of that Diophantine equation).

1.1. Notation and conventions. As usual, \mathbb{R} , \mathbb{Z} , and \mathbb{N} stand for the field of real numbers, the ring of rational integers, and the semigroup of positive rational integers, respectively. A finite sequence of symbols is denoted by \vec{x} and $L(\vec{x})$ stands for its length (we write, for instance, $\vec{x} := (y_1, \dots, y_n)$)

and $L(\vec{x}) = n$); let

$$\vec{x} * \vec{y} := (a_1, \dots, a_n, b_1, \dots, b_m)$$

stand for the concatenation of the sequences

$$\vec{x} := (a_1, \dots, a_n) \quad \text{and} \quad \vec{y} := (b_1, \dots, b_m).$$

The polynomial

$$p(x_1, x_2) = \frac{(x_1 + x_2 - 2)(x_1 + x_2 - 1)}{2} + x_2$$

defines a bijection

$$p: \mathbb{N}^2 \rightarrow \mathbb{N}, \quad p: \vec{a} \mapsto p(\vec{a}) \text{ for } \vec{a} \in \mathbb{N}^2;$$

moreover, for $\vec{a} \in \mathbb{N}^2$, $\vec{a} := (a_1, a_2)$,

$$p(\vec{a}) \geq \max\{a_1, a_2\} \quad \text{and} \quad p(\vec{a}) \leq a_1^2 + 2a_2^2$$

(cf. [2, p. 237]). Given an arithmetical formula \mathfrak{A} , let

$$(\forall j \leq n) \mathfrak{A} := \forall j ((j \in \mathbb{N} \ \& \ j \leq n) \Rightarrow \mathfrak{A}).$$

For $\vec{a} \in \mathbb{R}^n$, $\vec{a} := (a_1, \dots, a_n)$, let

$$\vec{a}^2 := \sum_{i=1}^n a_i^2 \quad \text{and} \quad |\vec{a}| := \max\{|a_j| \mid 1 \leq j \leq n\}.$$

§2. THE PREDICATE CALCULUS \mathcal{P}

The predicate calculus \mathcal{P} is a first order theory. The alphabet of its language consists of the set

$$\mathcal{X} := \{t_i \mid i \in \mathbb{N}\}$$

of the individual variables, the binary predicate letter ϵ , the logical connectives: $\{\neg, \supset\}$ (“negation” and “implication”), the universal quantifier \forall , and the parentheses $\{(,)\}$. The set \mathfrak{F} of the formulae of \mathcal{P} is defined inductively. An expression of the form $(x \epsilon y)$, with $\{x, y\} \subset \mathcal{X}$, is (an elementary) formula; if \mathfrak{A} and \mathfrak{B} are formulae, then $\neg \mathfrak{A}$, $(\mathfrak{A} \supset \mathfrak{B})$, and $\forall x \mathfrak{A}$ are formulae.

Let us define inductively a map $\mathcal{N}: \mathfrak{F} \rightarrow \mathbb{N}$.

Definition 1. Let $\mathcal{N}(t_i \epsilon t_j) = 4p(i, j) - 3$ for $\{i, j\} \subseteq \mathbb{N}$. For $\{\mathfrak{A}, \mathfrak{B}\} \subseteq \mathfrak{F}$ and $i \in \mathbb{N}$, let $\mathcal{N}(\neg \mathfrak{A}) = 4\mathcal{N}(\mathfrak{A}) - 2$, $\mathcal{N}(\forall t_i \mathfrak{A}) = 4p(i, \mathcal{N}(\mathfrak{A})) - 1$, and $\mathcal{N}(\mathfrak{A} \supset \mathfrak{B}) = 4p(\mathcal{N}(\mathfrak{A}), \mathcal{N}(\mathfrak{B}))$.

Proposition 1. The map $\mathcal{N}: \mathfrak{F} \rightarrow \mathbb{N}$ is a bijection.

Proof. It follows easily from the definition of the map \mathcal{N} by induction. \square

Notation. For $\mathfrak{A} \in \mathfrak{F}$ and $\{x, y\} \subset \mathcal{X}$, let $[\mathfrak{A}]_f$ and $\mathfrak{A}[x|y]$ stand for the set of the free variables of \mathfrak{A} and the formula obtained from \mathfrak{A} on replacing each of the *free* occurrences of the variable x in \mathfrak{A} by y , respectively.

Definition 2. Let $\mathfrak{A} \in \mathfrak{F}$ and $\{x, y\} \subset \mathcal{X}$. If no free occurrence of x in \mathfrak{A} lies within the scope of a quantifier $\forall y$, then the variable y is free for x in \mathfrak{A} (cf. [14, p. 54]).

There are five groups of axioms in \mathcal{P} (cf. [14, pp. 69–70]):

$$\mathcal{A}_1 := \{\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{A}) \mid \{\mathfrak{A}, \mathfrak{B}\} \subseteq \mathfrak{F}\};$$

$$\mathcal{A}_2 := \{(\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{C})) \supset ((\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \mathfrak{C})) \mid \{\mathfrak{A}, \mathfrak{B}, \mathfrak{C}\} \subseteq \mathfrak{F}\};$$

$$\mathcal{A}_3 := \{(\neg \mathfrak{B} \supset \neg \mathfrak{A}) \supset ((\neg \mathfrak{B} \supset \mathfrak{A}) \supset \mathfrak{B}) \mid \{\mathfrak{A}, \mathfrak{B}\} \subseteq \mathfrak{F}\};$$

$$\mathcal{A}_4 := \{\forall x (\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \forall x \mathfrak{B}) \mid \{\mathfrak{A}, \mathfrak{B}\} \subseteq \mathfrak{F}, x \in \mathcal{X} \setminus [\mathfrak{A}]_f\};$$

$$\mathcal{A}_5 := \{\forall x \mathfrak{A} \supset \mathfrak{A}[x|y] \mid \mathfrak{A} \in \mathfrak{F}, \{x, y\} \subseteq \mathcal{X},$$

the variable y is free for x in $\mathfrak{A}\}$.

The set \mathfrak{T} of the theorems of \mathcal{P} is defined inductively:

$$(\mathcal{B}_0) \quad \bigcup_{j=1}^5 \mathcal{A}_j \subseteq \mathfrak{T}.$$

(\mathcal{B}_1) If $\{\mathfrak{A}, (\mathfrak{A} \supset \mathfrak{B})\} \subseteq \mathfrak{T}$, then $\mathfrak{B} \in \mathfrak{T}$ (“modus ponens”).

(\mathcal{B}_2) If $\mathfrak{A} \in \mathfrak{T}$, then $\forall x \mathfrak{A} \in \mathfrak{T}$ (“generalisation”).

In what follows (see Corollary 3), we shall construct a polynomial $f(t, \vec{x})$ in $\mathbb{Z}[t, \vec{x}]$ such that

$$\mathcal{N}(\mathfrak{T}) = \{a \mid a \in \mathbb{N}, \exists \vec{b} (\vec{b} \in \mathbb{Z}^{L(\vec{x})} \ \& \ f(a, \vec{b}) = 0)\}.$$

Our first task is to give a Diophantine description of the predicate “ \mathfrak{A} is an axiom of \mathcal{P} .” In this section, we provide such a description for the three predicates “ $\mathfrak{A} \in \mathcal{A}_i$,” with $i = 1, 2, 3$.

Proposition 2. Let $g_1(u, \vec{x}) := u - 4p(x_1, 4p(x_2, x_1))$ with $\vec{x} := (x_1, x_2)$. Then

$$\mathcal{N}(\mathcal{A}_1) = \{u \mid \exists \vec{b} (\vec{b} \in \mathbb{N}^2 \ \& \ g_1(u, \vec{b}) = 0)\}.$$

Proof. Let $\mathcal{N}(\mathfrak{A}) = x_1$, $\mathcal{N}(\mathfrak{B}) = x_2$, and $\mathcal{N}(\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{A})) = u$. It follows then from the definition of the map \mathcal{N} that $u = 4p(x_1, 4p(x_2, x_1))$. This proves the proposition. \square

Proposition 3. *Let*

$$g_2(u, \vec{x}) := u - 4p(4p(x_1, 4p(x_2, x_3)), 4p(4p(x_1, x_2), 4p(x_1, x_3)))$$

with $\vec{x} := (x_1, x_2, x_3)$. Then

$$\mathcal{N}(\mathcal{A}_2) = \{u \mid \exists \vec{b} (\vec{b} \in \mathbb{N}^3 \ \& \ g_2(u, \vec{b}) = 0)\}.$$

Proof. Let $\mathfrak{D} := ((\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{C})) \supset ((\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \mathfrak{C})))$ and let $\mathcal{N}(\mathfrak{A}) = x_1$, $\mathcal{N}(\mathfrak{B}) = x_2$, $\mathcal{N}(\mathfrak{C}) = x_3$. An easy calculation shows that, in these notations, $g_2(u, \vec{x}) = 0$ if and only if $\mathcal{N}(\mathfrak{D}) = u$. This proves the proposition. \square

Proposition 4. *Let*

$$g_3(u, \vec{x}) := u - 4p(4p(4x_2 - 2, 4x_1 - 2), 4p(4p(4x_2 - 2, x_1), x_2))$$

with $\vec{x} := (x_1, x_2)$. Then

$$\mathcal{N}(\mathcal{A}_3) = \{u \mid \exists \vec{b} (\vec{b} \in \mathbb{N}^2 \ \& \ g_3(u, \vec{b}) = 0)\}.$$

Proof. Let $\mathfrak{C} := ((\neg \mathfrak{B} \supset \neg \mathfrak{A}) \supset ((\neg \mathfrak{B} \supset \mathfrak{A}) \supset \mathfrak{B}))$, $\mathcal{N}(\mathfrak{A}) = x_1$, and $\mathcal{N}(\mathfrak{B}) = x_2$. The equation $g_3(u, \vec{x}) = 0$ is easily seen to assert that $\mathcal{N}(\mathfrak{C}) = u$. This proves the proposition. \square

To give a Diophantine description of the sets of axioms \mathcal{A}_4 and \mathcal{A}_5 , we shall make use of the techniques developed in the works, relating to the Hilbert tenth problem (cf. [2, 12], and references therein).

§3. ON DIOPHANTINE CODING

In this section, following [2], we state a few lemmata about Diophantine coding.

Lemma 1. *Let $f(t, \vec{x}) \in \mathbb{Z}[t, \vec{x}]$ with $L(\vec{x}) = n$ and suppose that*

$$S = \{a \mid a \in \mathbb{N}, \exists \vec{b} (\vec{b} \in \mathbb{N}^n \ \& \ f(a, \vec{b}) = 0)\}.$$

Then

$$S = \{a \mid a \in \mathbb{N}, \exists \vec{b} (\vec{b} \in \mathbb{Z}^{4n} \ \& \ g(a, \vec{b}) = 0)\},$$

where

$$g(t, \vec{y}) := f(t, \vec{z}), \quad \vec{z} := (z_1, \dots, z_n), \quad z_j := \sum_{i=1}^4 y_{ji}^2 + 1, \quad 1 \leq j \leq n.$$

Proof. See, for instance, [12, §1.3]. \square

Lemma 2. Let $f_3(m, n, k; \vec{x})$

$$\begin{aligned} &:= (x_1^2 - (x_2^2 - 1)x_3^2 - 1)^2 + (x_4^2 - (x_5^2 - 1)x_6^2 - 1)^2 + (x_7^2 - (x_8^2 - 1)x_9^2 - 1)^2 \\ &+ (x_{10} - x_{11}x_{12})^2 + (x_{13} - 1 - 4x_{14}x_{15})^2 + (x_{16} - x_{17} - x_{18}x_{19})^2 + (x_{20} - x_{21} - x_{22}x_{23})^2 \\ &+ (x_8 - k - 4(x_{13} - 1)x_3)^2 + (x_3 - k - x_{14} + 1)^2 + (x_{17} - n - x_{18})^2 + (x_{17} - k - x_{19})^2 \\ &\quad + ((x_1 - x_3(x_2 - n) - m)^2 - (x_{15} - 1)^2(2x_2n - n^2 - 1)^2)^2 \\ &\quad + (m + x_{16} - 2x_2n + n^2 + 1)^2 + (x_2^2 - (x_{17}^2 - 1)(x_{17} - 1)^2x_{20}^2 - 1)^2, \end{aligned}$$

where $\vec{x} := (x_1, \dots, x_{20})$. Then $m = n^k$ if and only if

$$\exists \vec{a} (\vec{a} \in \mathbb{N}^{20} \ \& \ f_3(m, n, k; \vec{a}) = 0).$$

Proof. See [2, pp. 244–248].

Lemma 3. Let $f_4(m, n, k; \vec{x})$

$$\begin{aligned} &:= f_3(x_1, 2, n; \vec{x}^{(1)}) + f_3(x_5, x_4, n; \vec{x}^{(2)}) + f_3(x_6, x_3, k; \vec{x}^{(3)}) \\ &\quad + (x_1 + x_2 - x_3)^2 + (x_4 - x_3 - 1)^2 + (x_6x_7 + x_8 - x_5 - 1)^2 \\ &\quad + (x_5 + x_9 - (x_7 + 1)x_6)^2 + (x_7 - m - (x_{10} - 1)x_3)^2 + (m + x_{11} - x_3)^2, \end{aligned}$$

where $\vec{x} = \vec{x}^{(0)} * \dots * \vec{x}^{(3)}$ with $\vec{x}^{(0)} := (x_1, \dots, x_{11})$, $\vec{x}^{(1)} := (x_{12}, \dots, x_{31})$,
 $\vec{x}^{(2)} := (x_{32}, \dots, x_{51})$, $\vec{x}^{(3)} := (x_{52}, \dots, x_{71})$. Then

$$m = \frac{n!}{(n-k)!k!}$$

if and only if

$$\exists \vec{a} (\vec{a} \in \mathbb{N}^{71} \ \& \ f_4(m, n, k; \vec{a}) = 0).$$

Proof. See [2, pp. 249–250]. □

Lemma 4. Let $f_2(m, n; \vec{x})$

$$\begin{aligned} &:= f_3(x_3, x_1, x_2; \vec{x}^{(1)}) + f_3(x_4, x_3, n; \vec{x}^{(2)}) + f_4(x_5, x_3, n; \vec{x}^{(3)}) \\ &\quad + (x_1 - 2n - 1)^2 + (x_2 - n - 1)^2 + (mx_5 + x_6 - 1 - x_4)^2 + (x_4 + x_7 - (m + 1)x_5)^2, \end{aligned}$$

where $\vec{x} = \vec{x}^{(0)} * \dots * \vec{x}^{(3)}$ with $\vec{x}^{(0)} := (x_1, \dots, x_7)$, $\vec{x}^{(1)} := (x_8, \dots, x_{27})$,
 $\vec{x}^{(2)} := (x_{28}, \dots, x_{47})$, $\vec{x}^{(3)} := (x_{48}, \dots, x_{118})$. Then $m = n!$ if and only if

$$\exists \vec{a} (\vec{a} \in \mathbb{N}^{118} \ \& \ f_2(m, n; \vec{a}) = 0).$$

Proof. See [2, pp. 251–252]. □

Lemma 5. Let $f_1(m, n, a, b; \vec{x})$

$$\begin{aligned} := & (x_1 - a - bn)^2 + (x_3 - bx_2 - 1)^2 + (bx_4 - a - x_3x_5)^2 + (m + x_8 - x_3)^2 \\ & + (x_9 - x_4 - n)^2 + (m + x_3x_{11} - x_6x_7x_{10})^2 + f_3(x_2, x_1, n; \vec{x}^{(1)}) \\ & + f_3(x_6, b, n; \vec{x}^{(2)}) + f_2(x_7, n; \vec{x}^{(3)}) + f_4(x_{10}, x_9, n; \vec{x}^{(4)}), \end{aligned}$$

where

$$\begin{aligned} \vec{x} &= \vec{x}^{(0)} * \dots * \vec{x}^{(4)}, \quad \vec{x}^{(0)} := (x_1, \dots, x_{11}), \quad \vec{x}^{(1)} := (x_{12}, \dots, x_{31}), \\ \vec{x}^{(2)} &:= (x_{32}, \dots, x_{51}), \quad \vec{x}^{(3)} := (x_{52}, \dots, x_{169}), \quad \vec{x}^{(4)} := (x_{170}, \dots, x_{240}). \end{aligned}$$

Then

$$m = \prod_{k=1}^n (a + bk)$$

if and only if

$$\exists \vec{c} (\vec{c} \in \mathbb{N}^{240} \ \& \ f_1(m, n, a, b; \vec{c}) = 0).$$

Proof. See [2, p. 252]. \square

Proposition 5. Let

$$\sigma(u, j, w; \vec{z}) := 4((u - p(z_1, z_2))^2 + (w + z_3(1 + jz_2) - z_1)^2 + (w + z_4 - jz_2 - 2)^2)$$

with $\vec{z} := (z_1, \dots, z_4)$. There is a function

$$S: \mathbb{N}^2 \rightarrow \mathbb{N},$$

satisfying the following conditions:

- (i) $w = S(j, u)$ if and only if $\exists \vec{b} (\vec{b} \in \mathbb{N}^4 \ \& \ \sigma(u, j, w; \vec{b}) = 0)$;
- (ii) $\forall j, u (S(j, u) \leq u)$;
- (iii) if $\{a_k \mid 1 \leq k \leq n\} \subseteq \mathbb{N}$ for some n in \mathbb{N} , then there is a number u in \mathbb{N} such that $a_k = S(k, u)$ for $1 \leq k \leq n$.

Proof. See [2, pp. 237–238]. \square

Proposition 6. Let $P(u_1, u_2; \vec{y}, \vec{z}) \in \mathbb{Z}[u_1, u_2; \vec{y}, \vec{z}]$ with $L(\vec{z}) = l$, and suppose there is a polynomial $R(u_1, u_2; \vec{y})$ in $\mathbb{Z}[u_1, u_2; \vec{y}]$ such that

$$|P(n, j; \vec{a}, \vec{d})| \leq R(n, T; \vec{a})$$

for $\vec{a} \in \mathbb{N}^{L(\vec{y})}$, $\{n, j\} \subseteq \mathbb{N}$, $j \leq n$, $\vec{d} \in \mathbb{N}^l$, $|\vec{d}| \leq T$ and

$$R(c_1, c_2; \vec{a}) > \max\{c_1, c_2\}$$

for $\{c_1, c_2\} \subseteq \mathbb{N}$, $\vec{a} \in \mathbb{N}^{L(\vec{y})}$. Write, for brevity,

$$H_l(\vec{x}, \vec{b}) := f_2(b_5, b_4; \vec{x}^{(2)}) + f_1(b_6, n, 1, b_5; \vec{x}^{(3)}) + (b_6 - b_1b_5 - 1)^2$$

$$+(b_2 - b_6 b_7)^2 + (\vec{x}^{(4)} - \vec{x}^{(1)} + \vec{\beta})^2 + \sum_{i=1}^l f_1(b_6 x_i^{(5)}, b_3, x_i^{(4)}, 1; \vec{x}^{(5+i)}),$$

where

$$\vec{b} := (b_1, \dots, b_7), \quad \vec{\beta} := (\beta_1, \dots, \beta_l)$$

with

$$\beta_i = b_3 + 1 \quad \text{for } 1 \leq i \leq l,$$

$$\vec{x} = \vec{x}^{(1)} * \dots * \vec{x}^{(5+l)}$$

with

$$\vec{x}^{(j)} := (x_1^{(j)}, \dots, x_{L(\vec{x}^{(j)})}^{(j)}) \quad \text{for } 1 \leq j \leq 5+l,$$

$$L(\vec{x}^{(1)}) = L(\vec{x}^{(4)}) = L(\vec{x}^{(5)}) = l, \quad L(\vec{x}^{(2)}) = 118,$$

$$L(\vec{x}^{(3)}) = L(\vec{x}^{(5+i)}) = 240 \quad \text{for } 1 \leq i \leq l,$$

and

$$L(\vec{x}) = \sum_{1 \leq i \leq 5+l} L(\vec{x}^{(i)}) = 243l + 358.$$

Then

$$(\forall j \leq n) \exists \vec{c} (\vec{c} \in \mathbb{N}^l \ \& \ P(n, j; \vec{a}, \vec{c}) = 0) \iff$$

$$\exists \vec{x}, \vec{b} (\vec{b} \in \mathbb{N}^7 \ \& \ \vec{x} \in \mathbb{N}^{L(\vec{x})} \ \& \ (P(n, b_1; \vec{a}, \vec{x}^{(1)}) - b_2)^2$$

$$+ (R(n, b_3; \vec{a}) - b_4)^2 + H_l(\vec{x}, \vec{b}) = 0)$$

for $\vec{a} \in \mathbb{N}^{L(\vec{y})}$.

Proof. See [2, pp. 253–256]. □

§4. A FEW TECHNICAL LEMMATA

Notation. For $\mathfrak{A} \in \mathfrak{F}$, let $m(\mathfrak{A})$ stand for the number of occurrences of the logical connectives \neg , \supset , or \forall .

Definition 3. Let $i \in \mathbb{N}$. A sequence of formulae $\{\varphi_1, \dots, \varphi_n\}$ in \mathfrak{F} is i -admissible if, for every j in the interval $1 \leq j \leq n$, one of the following conditions holds true:

- (a) $\varphi_j := (t_k \in t_l)$ and $i \notin \{k, l\}$,
- (b) $\varphi_j := \forall t_i \psi$ for some ψ in \mathfrak{F} ,
- (c) $\varphi_j := (\varphi_k \supset \varphi_l)$ with $1 \leq k, l < j$,
- (d) $\varphi_j := \neg \varphi_k$ with $1 \leq k < j$,
- (e) $\varphi_j := \forall t_\nu \varphi_k$ with $\nu \in \mathbb{N}$ $1 \leq k < j$.

Lemma 6. *The variable t_i does not occur as a free variable in a formula φ if and only if there is an i -admissible sequence of formulae $\{\varphi_1, \dots, \varphi_n\}$ with $\varphi_n = \varphi$.*

Proof. Let $m(\varphi) = 0$ and suppose that $t_i \notin [\varphi]_f$. Then $\varphi := (t_k \in t_l)$ with $i \notin \{k, l\}$ and we may take $n = 1$, $\varphi_1 = \varphi$. Conversely, if $m(\varphi) = 0$ and there is an i -admissible sequence of formulae $\{\varphi_1, \dots, \varphi_n\}$ with $\varphi_n = \varphi$, then φ_n must satisfy condition (a) (since $m(\varphi_n) = m(\varphi) = 0$) and therefore t_i is not a free variable of φ ($= \varphi_n$).

Let $m(\varphi) = l$ with $l \in \mathbb{N}$ and suppose the assertion be true for every formula φ' with $m(\varphi') < l$. Let $\{\varphi_1, \dots, \varphi_n\}$ be an i -admissible sequence of formulae with $\varphi_n = \varphi$. Since $m(\varphi) > 0$ and $\varphi_n = \varphi$, the formula φ satisfies one of the conditions (b) – (e). If $\varphi := \forall t_i \psi$ for some ψ in \mathfrak{F} , then $t_i \notin [\varphi]_f$; if $\varphi := (\varphi_k \supset \varphi_l)$ with $1 \leq k, l < n$, then, by the inductive supposition, $t_i \notin [\varphi_k]_f \cup [\varphi_l]_f$ and therefore $t_i \notin [\varphi]_f$; finally, if either $\varphi := \neg \varphi_k$ with $1 \leq k < n$ or $\varphi := \forall t_\nu \varphi_k$ with $\nu \in \mathbb{N}$, $1 \leq k < n$, then, by the inductive supposition, $t_i \notin [\varphi_k]_f$ and therefore $t_i \notin [\varphi]_f$. In either case, t_i is not a free variable of φ . Conversely, suppose that t_i is not a free variable of φ . Since $m(\varphi) > 0$, the formula φ must contain one of the logical connectives \neg , \supset , or \forall . If $\varphi \in \{\neg \psi, \forall t_\nu \psi\}$ with $\psi \in \mathfrak{F}$ and $\nu \neq i$, then t_i is not a free variable of ψ , therefore, by the inductive supposition, there is an i -admissible sequence of formulae $\{\varphi_1, \dots, \varphi_\mu\}$ with $\varphi_\mu := \psi$ and we may let $n = \mu + 1$, $\varphi_n = \varphi$. If $\varphi := (\psi_1 \supset \psi_2)$ with $\{\psi_1, \psi_2\} \subseteq \mathfrak{F}$, then t_i is not a free variable of both ψ_1 and ψ_2 , and therefore, by the inductive supposition, there are two i -admissible sequences of formulae $\{\varphi_1, \dots, \varphi_\mu\}$ and $\{\varphi'_1, \dots, \varphi'_\nu\}$ with $\varphi_\mu := \psi_1$ and $\varphi'_\nu := \psi_2$; it is clear that in this case the sequence of formulae $\{\varphi_1, \dots, \varphi_\mu, \varphi'_1, \dots, \varphi'_\nu, \varphi\}$ is i -admissible. Finally, if $\varphi := \forall t_i \psi$ for some ψ in \mathfrak{F} , then we may take $n = 1$ and let $\varphi_1 = \varphi$. \square

Definition 4. *Let $\{r_1, r_2\} \subseteq \mathbb{N}$. An (r_1, r_2) -admissible triple consists of two sequences of formulae $\{\varphi_1, \dots, \varphi_n\}$, $\{\psi_1, \dots, \psi_n\}$ and a sequence of integers $\{d_1, \dots, d_n\}$ such that $\{\varphi_j, \psi_j\} \subseteq \mathfrak{F}$, $d_j \in \{1, 2\}$ for $1 \leq j \leq n$ and, for every j in the interval $1 \leq j \leq n$, one of the following conditions holds true:*

- (1) $\varphi_j := (t_{r_3} \in t_{r_4})$ with $r_1 \notin \{r_3, r_4\}$, $d_j = 2$, $\psi_j := \varphi_j$;
- (2) $\varphi_j := (t_{r_3} \in t_{r_4})$ with $r_1 \in \{r_3, r_4\}$, $d_j = 1$, $\psi_j := \varphi_j[t_{r_1}|t_{r_2}]$;
- (3) $\varphi_j := \neg \varphi_k$, $d_j = d_k$, $\psi_j := \neg \psi_k$ with $1 \leq k < j$,

- (4) $\varphi_j := (\varphi_k \supset \varphi_l)$, $\psi_j := (\psi_k \supset \psi_l)$, $d_j = (d_k - 1)(d_l - 1) + 1$ with $1 \leq k, l < j$;
(5) $\varphi_j := \forall t_{r_3} \varphi_k$ with $r_3 \notin \{r_1, r_2\}$, $\psi_j := \forall t_{r_3} \psi_k$, $d_j = d_k$, $1 \leq k < j$;
(6) $\varphi_j := \forall t_{r_1} \chi$ with $\chi \in \mathfrak{F}$, $\psi_j := \varphi_j$, $d_j = 2$;
(7) $\varphi_j := \forall t_{r_2} \varphi_k$ with $r_1 \neq r_2$, $\psi_j := \varphi_j$, $d_j = d_k = 2$, $1 \leq k < j$.

Lemma 7. *Let $\{r_1, r_2\} \subseteq \mathbb{N}$ and $\{\varphi, \psi\} \subseteq \mathfrak{F}$. Then the variable t_{r_2} is free for t_{r_1} in φ and $\psi := \varphi[t_{r_1}|t_{r_2}]$ if and only if there is an (r_1, r_2) -admissible triple*

$$\{\varphi_1, \dots, \varphi_n\}, \quad \{\psi_1, \dots, \psi_n\}, \quad \{d_1, \dots, d_n\} \quad (3)$$

with $\varphi_n = \varphi$, $\psi_n = \psi$. Moreover, any (r_1, r_2) -admissible triple (2) satisfies the condition

$$d_j = \begin{cases} 1 & \text{if } t_{r_1} \in [\varphi_j]_f \\ 2 & \text{if } t_{r_1} \notin [\varphi_j]_f \end{cases} \quad (4)$$

for $1 \leq j \leq n$.

Proof. For any (r_1, r_2) -admissible triple (3) relation (4) can be easily proved by induction on n .

Let $m(\varphi) = 0$, then $\varphi := (t_{r_3} \in t_{r_4})$ with $\{r_3, r_4\} \subseteq \mathbb{N}$, so that the variable t_{r_2} is free for t_{r_1} in φ . Let $\psi := \varphi[t_{r_1}|t_{r_2}]$, $n = 1$, and

$$d_1 = \begin{cases} 1 & \text{if } r_1 \in \{r_3, r_4\} \\ 2 & \text{if } r_1 \notin \{r_3, r_4\}; \end{cases}$$

it is clear then that $\{\varphi\}$, $\{\psi\}$, $\{d_1\}$ is an (r_1, r_2) -admissible triple. Conversely, if (3) is an (r_1, r_2) -admissible triple with $\varphi_n = \varphi$, $\psi_n = \psi$, then, since $m(\varphi) = 0$, for $j = n$ one of the conditions 1) or 2) holds; in either case $\psi := \varphi[t_{r_1}|t_{r_2}]$.

Let now $m(\varphi) = l$ with $l \in \mathbb{N}$ and suppose the assertion be true for every formula φ' with $m(\varphi') < l$. If $\varphi := \forall t_{r_1} \varphi'$ with $\varphi' \in \mathfrak{F}$, then $t_{r_1} \notin [\varphi]_f$ and the assertion is obvious; if $\varphi := \forall t_{r_2} \varphi'$ with $\varphi' \in \mathfrak{F}$ and $r_1 \neq r_2$, then t_{r_2} is free for t_{r_1} in φ if and only if $t_{r_1} \notin [\varphi']_f$ (and therefore $t_{r_1} \notin [\varphi]_f$) and the assertion follows from the inductive supposition. Finally, if

$$\varphi \in \{\neg \varphi', \forall t_{r_3} \varphi', \varphi' \supset \varphi''\} \quad \text{with } \{\varphi', \varphi''\} \subseteq \mathfrak{F}, r_3 \notin \{r_1, r_2\},$$

then one can deduce the assertion from the inductive supposition arguing as in the proof of Lemma 6. \square

Notation. Let

$$h_0(\vec{j}; \vec{x}) := (j_2 - j_1 + x_1)^2 + (j_3 - j_1 + x_2)^2$$

with

$$\vec{j} := (j_1, j_2, j_3), \quad \vec{x} := (x_1, x_2).$$

It is clear that, for $\vec{j} \in \mathbb{N}^3$,

$$\exists \vec{x} (\vec{x} \in \mathbb{N}^2 \ \& \ h_0(\vec{j}; \vec{x}) = 0) \Leftrightarrow \max\{j_2, j_3\} < j_1.$$

The following lemma is a Diophantine reformulation of Lemma 6.

Lemma 8. *Let $\mathcal{C}_i := \{\mathfrak{A} \mid \mathfrak{A} \in \mathfrak{F}, t_i \notin [\mathfrak{A}]_f\}$. Then*

$$\mathcal{N}(\mathcal{C}_i) = \{v \mid \mathfrak{B}_4(i, v)\},$$

where

$$\mathfrak{B}_4(i, v) := \exists w, n (\{w, n\} \subseteq \mathbb{N} \ \& \ (\forall j_1 \leq n) \exists \vec{y} (\vec{y} \in \mathbb{N}^{27} \ \& \ P_4(n, j_1; i, v, w; \vec{y}) = 0))$$

with

$$\begin{aligned} P_4(n, j_1; i, v, w; \vec{y}) &:= \sigma(w, n, v; \vec{z}^{(4)}) \\ &+ \sum_{\nu=1}^3 \sigma(w, j_\nu, x_\nu; \vec{z}^{(\nu)}) + h_0(\vec{j}; z_1, z_2) + \prod_{\nu=1}^5 q_\nu(i, \vec{x}). \end{aligned}$$

Here

$$\begin{aligned} q_1(i, \vec{x}) &:= (x_1 - 4p(x_4, x_5) + 3)^2 + ((x_4 - i)^2 - x_6)^2 + ((x_5 - i)^2 - x_7)^2, \\ q_2(i, \vec{x}) &:= x_1 - 4p(i, x_4) + 1, \quad q_3(i, \vec{x}) := x_1 - 4p(x_2, x_3), \\ q_4(i, \vec{x}) &:= x_1 - 4x_2 + 2, \quad q_5(i, \vec{x}) := x_1 - 4p(x_4, x_2) + 1 \end{aligned}$$

with

$$\begin{aligned} \vec{j} &:= (j_1, j_2, j_3), \quad \vec{x} := (x_1, \dots, x_7), \quad \vec{y} := (j_2, j_3) * (z_1, z_2) * \vec{x} * \vec{z}, \\ \vec{z} &:= \vec{z}^{(1)} * \dots * \vec{z}^{(4)}, \text{ and } L(\vec{z}^{(\nu)}) = 4 \text{ for } 1 \leq \nu \leq 4, \text{ so that } L(\vec{y}) = 27. \end{aligned}$$

Proof. Let $\{\varphi_1, \dots, \varphi_n\}$ be a sequence of formulae in \mathfrak{F} with $\mathcal{N}(\varphi_\mu) = a_\mu$ for $1 \leq \mu \leq n$. In view of Proposition 5, there is a natural number w such that the formula $\exists \vec{b} (\vec{b} \in \mathbb{N}^4 \ \& \ \sigma(w, j, x; \vec{b}) = 0)$ holds true if and only if $x = a_j$ for $1 \leq j \leq n$. Therefore the formula

$$\exists \vec{z} \left(\vec{z} \in \mathbb{N}^{16} \ \& \ \sigma(w, n, v; \vec{z}^{(4)}) + \sum_{\nu=1}^3 \sigma(w, j_\nu, x_\nu; \vec{z}^{(\nu)}) = 0 \right)$$

asserts that $a_{j_\nu} = x_\nu$ for $1 \leq \nu \leq 3$ and $a_n = v$. Moreover, the formula $\exists z_1, z_2 (h_0(\vec{j}; z_1, z_2) = 0)$ asserts that $\max\{j_2, j_3\} < j_1$. It follows further that $q_1(i, \vec{x}) = 0$ if and only if $m(\varphi_{j_1}) = 0$, $\varphi_{j_1} := (t_k \in t_l)$ and $i \notin \{k, l\}$,

where $k := x_4$, $l := x_5$, that $q_2(i, \vec{x}) = 0$ if and only if $\varphi_{j_1} := \forall t_i \psi$ for some ψ in \mathfrak{F} , that $q_3(i, \vec{x}) = 0$ if and only if $\varphi_{j_1} := (\varphi_{j_2} \supset \varphi_{j_3})$ with $1 \leq j_2, j_3 < j_1$, that $q_4(i, \vec{x}) = 0$ if and only if $\varphi_{j_1} := \neg \varphi_{j_2}$ with $1 \leq j_2 < j_1$, and that $q_5(i, \vec{x}) = 0$ if and only if $\varphi_{j_1} := \forall t_\mu \varphi_{j_2}$ with $\mu \in \mathbb{N}$, $1 \leq j_2 < j_1$. Thus, by Lemma 6, the variable t_i does not occur as a free variable in the formula $\mathcal{N}^{-1}(v)$ if and only if the formula $\mathfrak{B}_4(i, v)$ holds true. \square

Corollary 1. *Let*

$$\mathfrak{A}_4(u) := \exists i, v (\{i, v\} \subseteq \mathbb{N} \ \& \ \mathfrak{B}_4(i, v) \ \& \ \exists y (y \in \mathbb{N} \ \& \ h_4(u; i, v, y) = 0)),$$

where

$$h_4(u; i, v, y) := u - 4p(4p(i, 4p(v, y)) - 1, 4p(v, 4p(i, y) - 1)).$$

Then

$$\mathcal{N}(\mathfrak{A}_4) = \{u \mid \mathfrak{A}_4(u)\}.$$

Proof. Let

$$\mathfrak{C} := \forall t_i (\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \forall t_i \mathfrak{B}),$$

$\mathcal{N}(\mathfrak{A}) = v$, and $\mathcal{N}(\mathfrak{B}) = y$. An easy calculation shows then that

$$\mathcal{N}(\mathfrak{C}) = 4p(4p(i, 4p(v, y)) - 1, 4p(v, 4p(i, y) - 1)).$$

The assertion follows now from Lemma 8. \square

The following lemma is a Diophantine reformulation of Lemma 7.

Lemma 9. *Let*

$$\mathcal{C}(\vec{r}) := \{\vec{v} \mid v_1 = \mathcal{N}(\varphi), v_2 = \mathcal{N}(\psi), \varphi \in \mathfrak{F},$$

$$\psi := \varphi[t_{r_1} | t_{r_2}], t_{r_2} \text{ is free for } t_{r_1} \text{ in } \varphi\},$$

where $\vec{r} := (r_1, r_2)$ and $\vec{v} := (v_1, v_2)$. Then

$$\mathcal{C}(\vec{r}) = \{\vec{v} \mid \vec{v} \in \mathbb{N}^2 \ \& \ \mathfrak{B}_5(\vec{v}, \vec{r})\},$$

where

$$\mathfrak{B}_5(\vec{v}, \vec{r}) := \exists \vec{w}, n (\vec{w} \in \mathbb{N}^3 \ \& \ n \in \mathbb{N} \ \&$$

$$(\forall j_1 \leq n) \exists \vec{y} (\vec{y} \in \mathbb{N}^{60} \ \& \ P_5(n, j_1; \vec{v}, \vec{r}, \vec{w}; \vec{y}) = 0))$$

and

$$P_5(n, j_1; \vec{v}, \vec{r}, \vec{w}; \vec{y}) := h_0(\vec{j}; z_1, z_2) + \sum_{1 \leq i, \nu \leq 3} \sigma(w_i, j_\nu, x_{3(i-1)+\nu}; z_i^{(\nu)})$$

$$+ \sum_{i \in \{1,2\}} \sigma(w_i, n, v_i; \vec{z}_i^{(4)}) + \sum_{i=7}^9 (x_i - 1)^2 (x_i - 2)^2 + \prod_{i=1}^7 q_i(\vec{r}, \vec{x}).$$

Here

$$q_1(\vec{r}, \vec{x}) := (x_7 - 2)^2 + (x_4 - x_1)^2 + (x_1 - 4p(r_3, r_4) + 3)^2 \\ + ((r_3 - r_1)^2 (r_4 - r_1)^2 - x_{10})^2;$$

$$q_2(\vec{r}, \vec{x}) := (x_7 - 1)^2 + \prod_{i=1}^3 q_2^{(i)}(\vec{r}, \vec{x})$$

with

$$q_2^{(1)}(\vec{r}, \vec{x}) := (x_1 - 4p(r_1, r_4) + 3)^2 + (x_4 - 4p(r_2, r_4) + 3)^2 + ((r_4 - r_1)^2 - x_{10})^2,$$

$$q_2^{(2)}(\vec{r}, \vec{x}) := (x_1 - 4p(r_3, r_1) + 3)^2 + (x_4 - 4p(r_3, r_2) + 3)^2 + ((r_3 - r_1)^2 - x_{10})^2,$$

$$q_2^{(3)}(\vec{r}, \vec{x}) := (x_1 - 4p(r_1, r_1) + 3)^2 + (x_4 - 4p(r_2, r_2) + 3)^2;$$

$$q_3(\vec{r}, \vec{x}) := (x_1 - 4x_2 + 2)^2 + (x_4 - 4x_5 + 2)^2 + (x_7 - x_8)^2;$$

$$q_4(\vec{r}, \vec{x}) := (x_7 - (x_8 - 1)(x_9 - 1) - 1)^2 + (x_1 - 4p(x_2, x_3))^2 + (x_4 - 4p(x_5, x_6))^2;$$

$$q_5(\vec{r}, \vec{x}) := (x_1 - 4p(r_3, x_2) + 1)^2 + (x_4 - 4p(r_3, x_5) + 1)^2$$

$$+ (x_7 - x_8)^2 + ((r_3 - r_1)^2 (r_3 - r_2)^2 - x_{10})^2;$$

$$q_6(\vec{r}, \vec{x}) := (x_1 - 4p(r_1, x_{10}) + 1)^2 + (x_7 - 2)^2 + (x_4 - x_1)^2;$$

$$q_7(\vec{r}, \vec{x}) := (x_1 - 4p(r_2, x_2) + 1)^2 + (x_7 - 2)^2$$

$$+ (x_8 - 2)^2 + (x_4 - x_1)^2 + ((r_2 - r_1)^2 - x_{10})^2;$$

$$\vec{w} := (w_1, w_2, w_3), \quad \vec{j} := (j_1, j_2, j_3), \quad \vec{z}^{(\nu)} := \vec{z}_1^{(\nu)} * \vec{z}_2^{(\nu)} * \vec{z}_3^{(\nu)} \text{ for } 1 \leq \nu \leq 3,$$

$$\vec{z}^{(4)} := \vec{z}_1^{(4)} * \vec{z}_2^{(4)}, \quad \text{with } L(\vec{z}_i^{(\nu)}) = 4$$

$$\text{for } 1 \leq i \leq 3, \quad 1 \leq \nu \leq 4, \quad \vec{z} := \vec{z}^{(1)} * \dots * \vec{z}^{(4)};$$

$$\vec{x} := (r_3, r_4) * (z_1, z_2) * (x_1, \dots, x_{10}), \quad \vec{y} := (j_2, j_3) * \vec{x} * \vec{z},$$

so that $L(\vec{y}) = 60$.

Proof. Let

$$\{\varphi_1, \dots, \varphi_n\}, \quad \{\psi_1, \dots, \psi_n\}, \quad \{d_1, \dots, d_n\}$$

be two sequences of formulae and a sequence of natural numbers, so that $\{\varphi_j, \psi_j\} \subseteq \mathfrak{F}$, $d_j \in \mathbb{N}$ for $1 \leq j \leq n$. In view of Proposition 5, there are three natural numbers w_1, w_2, w_3 such that the formula

$$\exists \vec{b} (\vec{b} \in \mathbb{N}^4 \ \& \ \sigma(w_i, j, x; \vec{b}) = 0)$$

holds true if and only if

$$x = \begin{cases} \mathcal{N}(\varphi_j) & \text{if } i = 1 \\ \mathcal{N}(\psi_j) & \text{if } i = 2 \\ d_j & \text{if } i = 3 \end{cases}$$

for $1 \leq j \leq n$. Therefore the formula

$$\exists \vec{z} (\vec{w} \in \mathbb{N}^3 \ \& \ \vec{z} \in \mathbb{N}^{44} \ \& \ \sum_{1 \leq i, \nu \leq 3} \sigma(w_i, j_\nu, x_{3(i-1)+\nu}; \vec{z}_i^{(\nu)}) + \sum_{i \in \{1,2\}} \sigma(w_i, n, v_i; \vec{z}_i^{(4)}) = 0),$$

with $\vec{w} := (w_1, w_2, w_3)$, implies that there are three sequences

$$\{\varphi_1, \dots, \varphi_n\}, \quad \{\psi_1, \dots, \psi_n\}, \quad \{d_1, \dots, d_n\}$$

such that $\{\varphi_j, \psi_j\} \subseteq \mathfrak{F}$, $d_j \in \mathbb{N}$ for $1 \leq j \leq n$, $\mathcal{N}(\varphi_n) = v_1$, $\mathcal{N}(\psi_n) = v_2$, and $\mathcal{N}(\varphi_{j_\nu}) = x_\nu$, $\mathcal{N}(\psi_{j_\nu}) = x_{\nu+3}$, $d_{j_\nu} = x_{\nu+6}$ for $1 \leq \nu \leq 3$. The formula $\exists z_1, z_2 (\{z_1, z_2\} \subseteq \mathbb{N} \ \& \ h_0(\vec{j}; z_1, z_2) = 0)$ asserts that $\max\{j_2, j_3\} < j_1$. Moreover, for $1 \leq i \leq 7$, the formula

$$\exists \vec{x} (\vec{x} \in \mathbb{N}^{10} \ \& \ q_i(\vec{r}, \vec{x}) = 0)$$

is equivalent to condition *i*) in the definition of an (r_1, r_2) -admissible triple.

Finally, the equation $\sum_{i=7}^9 (x_i - 1)^2 (x_i - 2)^2 = 0$ implies that $d_j \in \{1, 2\}$ for $1 \leq j \leq n$. Lemma 9 follows now from Lemma 7. \square

Corollary 2. *Let*

$$\mathfrak{A}_5(u) := \exists \vec{v}, \vec{r} (\{\vec{v}, \vec{r}\} \subseteq \mathbb{N}^2 \ \& \ \mathfrak{B}_5(\vec{v}, \vec{r}) \ \& \ (h_5(u; \vec{v}, r_1) = 0)),$$

where

$$\vec{r} := (r_1, r_2), \quad \vec{v} := (v_1, v_2), \quad \text{and} \quad h_5(u; \vec{v}, r_1) := u - 4p(4p(r_1, v_1) - 1, v_2).$$

Then

$$\mathcal{N}(\mathcal{A}_5) = \{u \mid \mathfrak{A}_5(u)\}.$$

Proof. Let $\mathfrak{C} := (\forall t_{r_1} \mathfrak{D} \supset \mathfrak{D}[t_{r_1}|t_{r_2}])$, $v_1 := \mathcal{N}(\mathfrak{D})$, and $v_2 := \mathcal{N}(\mathfrak{D}[t_{r_1}|t_{r_2}])$. It follows then that $\mathcal{N}(\mathfrak{C}) = 4p(4p(r_1, v_1) - 1, v_2)$. In view of Lemma 9, this proves the corollary. \square

§5. ELIMINATION OF UNIVERSAL QUANTIFIERS

It follows from Proposition 6 that formulae $\mathfrak{A}_4(u)$ and $\mathfrak{A}_5(u)$ define Diophantine predicates. In this section, we construct two polynomials $g_4(u, \vec{x}^{(4)})$ and $g_5(u, \vec{x}^{(5)})$ such that

$$\{u \mid \mathfrak{A}_\nu(u)\} = \{u \mid \exists \vec{b} (\vec{b} \in \mathbb{N}^{L(\vec{x}^{(\nu)})} \ \& \ g_\nu(u, \vec{b}) = 0)\}$$

for $\nu = 4, 5$.

Lemma 10. *Let*

$$R_4(t_1, t_2; i, v, w) := 32w^2 + 16v^2 + 300t_1^4 + 2 \cdot 10^6 t_2^{14} + 2 \cdot 10^5 i^{16}$$

with $\{i, v, w\} \subseteq \mathbb{N}$. Then

$$|P_4(n, j_1; i, v, w; \vec{y})| \leq R_4(n, T; i, v, w)$$

for $j_1 \leq n$, $|\vec{y}| \leq T$, $\vec{y} \in \mathbb{N}^{27}$, $\{n, j_1\} \subseteq \mathbb{N}$.

Proof. Suppose that

$$j_1 \leq n, |\vec{y}| \leq T, \vec{y} \in \mathbb{N}^{27}, \{i, v, w, n, j_1\} \subseteq \mathbb{N}.$$

An easy calculation shows that

$$\begin{aligned} h_0(\vec{j}; x_4, x_5) &\leq 16T^2 + 4n^2, \\ \sigma(w, j_\nu, x_\nu, \vec{z}^{(\nu)}) &\leq 8w^2 + 240T^6 \quad \text{for } \nu = 2, 3, \\ \sigma(w, j_1, x_1, \vec{z}^{(1)}) &\leq 8w^2 + 288T^4 n^2, \\ \text{and } \sigma(w, n, v, \vec{z}^{(4)}) &\leq 8w^2 + 16v^2 + 280T^4 n^2. \end{aligned}$$

Moreover, under the same conditions, we have

$$q_1(i, \vec{x}) \leq 16i^4 + 160T^4, \quad |q_2(i, \vec{x})| \leq 12T^2,$$

$$|q_3(i, \vec{x})| \leq 12T^2, \quad |q_4(i, \vec{x})| \leq 4T, \quad \text{and } |q_5(i, \vec{x})| \leq 12T^2.$$

The assertion of the lemma follows from these estimates and the definition of the polynomial $P_4(n, j_1; i, v, w; \vec{y})$ in Lemma 8. \square

Lemma 11. *Let*

$$R_5(z_1, z_2; \vec{v}, \vec{r}, \vec{w}) := 32\vec{w}^2 + 16\vec{v}^2 + 800t_1^4 + 10^{23}t_2^{64} + 5 \cdot 10^{20}(r_1^{64} + r_2^{32})$$

with $\{\vec{v}, \vec{r}\} \subseteq \mathbb{N}^2$, $\vec{w} \in \mathbb{N}^3$. Then

$$|P_5(n, j_1; \vec{v}, \vec{r}, \vec{w}; \vec{y})| \leq R_5(n, T; \vec{v}, \vec{r}, \vec{w})$$

for $j_1 \leq n$, $|\vec{y}| \leq T$, $\vec{y} \in \mathbb{N}^{60}$, $\{n, j_1\} \subseteq \mathbb{N}$.

Proof. Suppose that

$$j_1 \leq n, \quad |\vec{y}| \leq T, \quad \vec{y} \in \mathbb{N}^{60}, \quad \{n, j_1\} \subseteq \mathbb{N}, \quad \{\vec{v}, \vec{r}\} \subseteq \mathbb{N}^2, \quad \vec{w} \in \mathbb{N}^3.$$

An easy calculation shows that $h_0(\vec{j}; x_{13}, x_{14}) \leq 16T^2 + 4n^2$,

$$\sum_{1 \leq i \leq 3} \sigma(w_i, j_\nu, x_{3(i-1)+\nu}, \vec{z}_i^{(\nu)}) \leq 8\vec{w}^2 + 720T^6 \quad \text{for } \nu = 2, 3,$$

$$\sum_{1 \leq i \leq 3} \sigma(w_i, j_1, x_{3i-2}, \vec{z}_i^{(1)}) \leq 8\vec{w}^2 + 432(T^8 + n^4),$$

and

$$\sum_{i \in \{1, 2\}} \sigma(w_i, n, v_i, \vec{z}_i^{(4)}) \leq 8\vec{w}^2 + 16\vec{v}^2 + 280(T^8 + 70n^4).$$

Moreover, under the same conditions, we have

$$\sum_{i=7}^9 (x_i - 1)^2 (x_i - 2)^2 \leq 100T^4, \quad q_1(\vec{r}, \vec{x}) \leq 300T^8 + 130r_1^8,$$

$$q_2^{(1)}(\vec{r}, \vec{x}) \leq 32T^4 + 128r_1^4, \quad q_2^{(2)}(\vec{r}, \vec{x}) \leq 100T^4 + 140(r_1^4 + r_2^4),$$

$$q_2^{(3)}(\vec{r}, \vec{x}) \leq 100T^2 + 300(r_1^4 + r_2^4), \quad q_3(\vec{r}, \vec{x}) \leq 40T^2, \quad q_4(\vec{r}, \vec{x}) \leq 300T^4,$$

$$q_5(\vec{r}, \vec{x}) \leq 500T^8 + 100(r_1^8 + r_2^8), \quad q_6(\vec{r}, \vec{x}) \leq 150T^4 + 32r_1^4,$$

and $q_7(\vec{r}, \vec{x}) \leq 140T^4 + 16r_1^4 + 50r_2^4$. The assertion of the lemma follows from those estimates and the definition of the polynomial $P_5(n, j_1; \vec{v}, \vec{r}, \vec{w}; \vec{y})$ in Lemma 9. \square

By construction,

$$P_4(n, j_1; i, v, w; \vec{y}) \in \mathbb{Z}[n, j_1; i, v, w; \vec{y}]$$

and

$$P_5(n, j_1; \vec{v}, \vec{r}, \vec{w}; \vec{y}) \in \mathbb{Z}[n, j_1; \vec{v}, \vec{r}, \vec{w}; \vec{y}].$$

Therefore one concludes as follows.

Proposition 7. *Let*

$$g_4(u, \vec{z}) := h_4(u; i, v, y)^2 + H_{27}(\vec{x}, \vec{b}) \\ + (P_4(n, b_1; i, v, w; \vec{x}^{(1)}) - b_2)^2 + (R_4(n, b_3; i, v, w) - b_4)^2,$$

where $\vec{z} = \vec{x} * \vec{b} * (i, v, w, n, y)$ with $L(\vec{z}) = 6931$. Then

$$\mathcal{N}(\mathcal{A}_4) = \{u \mid \exists \vec{a} (\vec{a} \in \mathbb{N}^{6931} \ \& \ g_4(u, \vec{a}) = 0)\}.$$

Proof. In notations of Lemma 8,

$$\mathfrak{B}_4(i, v) := \exists w, n (\{w, n\} \subseteq \mathbb{N} \ \& \ (\forall j_1 \leq n) \\ \exists \vec{c} (\vec{c} \in \mathbb{N}^{27} \ \& \ P_4(n, j_1; i, v, w; \vec{c}) = 0)).$$

In view of Lemma 10, it follows from Proposition 6 that

$$\mathfrak{B}_4(i, v) \iff \exists w, n, \vec{x}, \vec{b} (\{w, n\} \subseteq \mathbb{N} \ \& \ \vec{b} \in \mathbb{N}^7 \ \& \ \vec{x} \in \mathbb{N}^{6919} \ \&$$

$H_{27}(\vec{x}, \vec{b}) + (P_4(n, b_1; i, v, w; \vec{x}^{(1)}) - b_2)^2 + (R_4(n, b_3; i, v, w) - b_4)^2 = 0$ for $\{i, v\} \subseteq \mathbb{N}$, since $L(\vec{x}) = 243l + 358 = 6919$ with $l := L(\vec{c}) = 27$. The assertion of Proposition 7 follows now from Corollary 1. \square

Proposition 8. *Let*

$$g_5(u, \vec{z}) := h_5(u; \vec{v}, r_1)^2 + H_{60}(\vec{x}, \vec{b}) \\ + (P_5(n, b_1; \vec{v}, \vec{r}, \vec{w}; \vec{x}^{(1)}) - b_2)^2 + (R_5(n, b_3; \vec{v}, \vec{r}, \vec{w}) - b_4)^2,$$

where $\vec{z} = \vec{x} * \vec{b} * \vec{v} * \vec{r} * \vec{w} * (n)$ with $L(\vec{z}) = 14953$. Then

$$\mathcal{N}(\mathcal{A}_5) = \{u \mid \exists \vec{a} (\vec{a} \in \mathbb{N}^{L(\vec{z})} \ \& \ g_5(u, \vec{a}) = 0)\}.$$

Proof. In notations of Lemma 9,

$$\mathfrak{B}_5(\vec{v}, \vec{r}) := \exists \vec{w}, n (\vec{w} \in \mathbb{N}^3 \ \& \ n \in \mathbb{N} \ \& \\ (\forall j_1 \leq n) \exists \vec{c} (\vec{c} \in \mathbb{N}^{60} \ \& \ P_5(n, j_1; \vec{v}, \vec{r}, \vec{w}; \vec{c}) = 0)).$$

In view of Lemma 11, it follows from Proposition 6 that

$$\mathfrak{B}_5(\vec{v}, \vec{r}) \iff \exists \vec{w}, n, \vec{x}, \vec{b} (\vec{w} \in \mathbb{N}^3 \ \& \ n \in \mathbb{N} \ \& \ \vec{b} \in \mathbb{N}^7 \ \& \ \vec{x} \in \mathbb{N}^{L(\vec{x})} \ \&$$

$H_{60}(\vec{x}, \vec{b}) + (P_5(n, b_1; \vec{v}, \vec{r}, \vec{w}; \vec{x}^{(1)}) - b_2)^2 + (R_5(n, b_3; \vec{v}, \vec{r}, \vec{w}) - b_4)^2 = 0$ with $\{\vec{v}, \vec{r}\} \subseteq \mathbb{N}^2$, $L(\vec{x}) = 243l + 358 = 14938$, and $l := L(\vec{c}) = 60$. The assertion of Proposition 8 follows now from Corollary 2. \square

§6. THE MAIN THEOREM

Proposition 9. *Let $u_i := \mathcal{N}(\mathfrak{A}_i)$ for some \mathfrak{A}_i in \mathfrak{F} , $1 \leq i \leq 3$, and let $G_1(\vec{u}; x) := x(u_3 - 4p(u_2, u_1))$, where $\vec{u} := (u_1, u_2, u_3)$. The formula \mathfrak{A}_1 follows from the formulae \mathfrak{A}_2 and \mathfrak{A}_3 by the rule (\mathcal{B}_1) if and only if*

$$\exists b (b \in \mathbb{N} \ \& \ G_1(\vec{u}; b) = 0).$$

Proof. Since the formula $u_3 = 4p(u_2, u_1)$ asserts that $\mathfrak{A}_3 := \mathfrak{A}_2 \supset \mathfrak{A}_1$, the assertion follows from the definition of inference rule (\mathcal{B}_1) . \square

Proposition 10. *Let $u_i := \mathcal{N}(\mathfrak{A}_i)$ for some \mathfrak{A}_i in \mathfrak{F} , $i = 1, 2$, and let $G_2(\vec{u}; r) := u_1 - 4p(r, u_2) + 1$, where $\vec{u} := (u_1, u_2)$. The formula \mathfrak{A}_1 follows from the formula \mathfrak{A}_2 by the rule (\mathcal{B}_2) if and only if $\exists r (r \in \mathbb{N} \ \& \ G_2(\vec{u}; r) = 0)$.*

Proof. Since the formula $\exists r (r \in \mathbb{N} \ \& \ G_2(\vec{u}; r) = 0)$ asserts that $\mathfrak{A}_2 := \forall t_r \mathfrak{A}_1$ for some t_r in \mathcal{X} , the assertion follows from the definition of inference rule (\mathcal{B}_2) . \square

The following lemma is a Diophantine reformulation of the definition of the set \mathfrak{T} of the theorems of \mathcal{P} .

Lemma 12. *Let*

$$Q(n, j_1; v, u; \vec{w}) := \sum_{i=1}^3 \sigma(u, j_i, x_i; \vec{z}^{(i)}) + \sigma(u, n, v; \vec{z}^{(4)})$$

$$+ h_0(\vec{j}; x_4, x_5) + G_1(x_1, x_2, x_3; y_1)^2 G_2(x_1, x_2; y_1)^2 \prod_{i=1}^5 g_i(x_1, \vec{y}^{(i)}),$$

where

$$\vec{j} := (j_1, j_2, j_3), \quad \vec{x} := (x_1, \dots, x_5), \quad \vec{w} := (j_2, j_3) * \vec{x} * \vec{z} * \vec{y}, \quad \vec{z} := \vec{z}^{(1)} * \dots * \vec{z}^{(4)},$$

$$\vec{y}^{(1)} = \vec{y}^{(3)} := (y_1, y_2), \quad \vec{y}^{(2)} := (y_1, y_2, y_3), \quad \vec{y}^{(4)} := (y_1, \dots, y_{6931}),$$

$$\vec{y}^{(5)} = \vec{y} := (y_1, \dots, y_{14953}), \quad L(\vec{z}^{(i)}) = 4 \quad \text{for } 1 \leq i \leq 4,$$

so that $L(\vec{w}) = 14976$. Then

$$\mathcal{N}(\mathfrak{T}) = \{v \mid \exists u, n (\{u, n\} \subseteq \mathbb{N} \ \& \ \mathfrak{A}(v; u, n))\},$$

where

$$\mathfrak{A}(v; u, n) := (\forall j_1 \leq n) \exists \vec{w} (\vec{w} \in \mathbb{N}^{L(\vec{w})} \ \& \ Q(n, j_1; v, u; \vec{w}) = 0).$$

Proof. Let $\mathfrak{C}_1, \dots, \mathfrak{C}_n$ be a sequence of formulae in \mathfrak{F} with $\mathcal{N}(\mathfrak{C}_\mu) = a_\mu$ for $1 \leq \mu \leq n$. In view of Proposition 5, there is a natural number u such that the formula $\exists \vec{b} (\vec{b} \in \mathbb{N}^4 \ \& \ \sigma(u, j, x; \vec{b}) = 0)$ holds true if and only if $x = a_j$ for $1 \leq j \leq n$. Therefore the formula

$$\exists \vec{z} (\vec{z} \in \mathbb{N}^{16} \ \& \ \sigma(u, n, v; \vec{z}^{(4)}) + \sum_{\nu=1}^3 \sigma(u, j_\nu, x_\nu; \vec{z}^{(\nu)}) = 0)$$

asserts that $a_{j_\nu} = x_\nu$ for $1 \leq \nu \leq 3$ and $a_n = v$. Moreover, the formula $\exists x_1, x_2 (h_0(\vec{j}; x_1, x_2) = 0)$ asserts that $\max\{j_2, j_3\} < j_1$. Thus, in view of Propositions 2–4 and Propositions 7–10, the formula $\mathfrak{A}(v; u, n)$ asserts that either $\mathfrak{C}_{j_1} \in \cup_{i=1}^5 \mathcal{C}_i$, or \mathfrak{C}_{j_1} can be deduced from \mathfrak{C}_{j_2} and \mathfrak{C}_{j_3} (respectively, from \mathfrak{C}_{j_2}) by the rule “modus ponens” (respectively, by the rule “generalisation”), where $\max\{j_2, j_3\} < j_1 \leq n$, and that $\mathcal{N}(\mathfrak{C}_n) = v$. The formula $\exists u, n (\{u, n\} \subseteq \mathbb{N} \ \& \ \mathfrak{A}(v; u, n))$ can be now seen to assert that $v \in \mathcal{N}(\mathfrak{T})$, as claimed. \square

Lemma 13. *Let*

$$R(z_1, z_2; v, u) := 32u^2 + 16v^2 + 300z_1^4 + 10^{89}z_2^{182}.$$

Then

$$|Q(n, j_1; v, u; \vec{w})| \leq R(n, T; v, u) \text{ for } j_1 \leq n, \ |\vec{w}| \leq T, \ \vec{w} \in \mathbb{N}^l, \ l := 14976,$$

with $\{v, u, n, j_1\} \subseteq \mathbb{N}$.

Proof. Suppose that $j_1 \leq n$, $|\vec{w}| \leq T$ for $\vec{w} \in \mathbb{N}^l$, and $\{v, u, n, j_1\} \subseteq \mathbb{N}$. Then, arguing as in the proof of Lemma 10, one concludes that

$$\begin{aligned} h_0(\vec{j}; x_4, x_5) + \sum_{i=1}^3 \sigma(u, j_i, x_i; \vec{z}^{(i)}) + \sigma(u, n, v; \vec{z}^{(4)}) \\ \leq 32u^2 + 16v^2 + 300n^4 + 10^3T^8. \end{aligned}$$

Moreover, it follows from the definition of the polynomials G_1, G_2, g_1, g_2 , and g_3 that

$$\begin{aligned} |G_1(x_1, x_2, x_3; \vec{y}_1)| &\leq 12T^2, & |G_2(x_1, x_2; \vec{y}_1)| &\leq 12T^4, \\ |g_1(x_1, \vec{y}^{(1)})| &\leq 1.2 \cdot 10^3T^4, & |g_2(x_1, \vec{y}^{(2)})| &\leq 5 \cdot 10^7T^8, \end{aligned}$$

and $|g_3(x_1, \vec{y}^{(3)})| \leq 10^{14}T^8$. After some calculations, it follows from Lemmas 10 and 11 and the definition of $g_i(x_1, \vec{y}^{(i)})$, $i = 4, 5$, that

$$g_4(x_1, \vec{y}^{(4)}) \leq 10^{14}T^{28} \quad \text{and} \quad g_5(x_1, \vec{y}^{(5)}) \leq 2 \cdot 10^{47}T^{128}.$$

Those estimates and the definition of the polynomial $Q(n, j_1; v, u; \vec{w})$ show that

$$|Q(n, j_1; v, u; \vec{w})| \leq 32u^2 + 16v^2 + 300n^4 + 10^{89}T^{182},$$

as asserted. \square

Theorem 1. *In the notations of Proposition 6, let*

$$F(v, \vec{z}) := (Q(n, b_1; v, u; \vec{x}^{(1)} - b_2)^2 + (R(n, b_3; v, u) - b_4)^2 + H_l(\vec{x}, \vec{b}))$$

with $l := 14976$ and $\vec{z} := (u, n) * \vec{x}$, so that $L(\vec{z}) = 243l + 360 = 3639528$.

Then

$$\mathcal{N}(\mathfrak{I}) = \{a \mid a \in \mathbb{N}, \exists \vec{c} (\vec{c} \in \mathbb{N}^{L(\vec{z})} \ \& \ F(a, \vec{c}) = 0)\}.$$

Proof. By construction, $Q(n, j_1; v, u; \vec{w}) \in \mathbb{Z}[n, j_1; v, u; \vec{w}]$. Therefore, in view of Lemma 13, the assertion follows from Proposition 6 and Lemma 12. \square

Corollary 3. *Let $f(t, \vec{x}) := F(t, \vec{z})$, where $\vec{z} := (z_1, \dots, z_n)$, $n := 3639528$, with*

$$z_j := \sum_{i=1}^4 x_{ji}^2 + 1 \quad \text{for } 1 \leq j \leq n, \quad \vec{x} := (x_{11}, \dots, x_{14}, \dots, x_{n1}, \dots, x_{n4}).$$

Then

$$\mathcal{N}(\mathfrak{I}) = \{a \mid a \in \mathbb{N}, \exists \vec{b} (\vec{b} \in \mathbb{Z}^{4n} \ \& \ f(a, \vec{b}) = 0)\}.$$

Proof. In view of Lemma 1, the assertion follows from Theorem 1. \square

Thus we may let $F_{\mathcal{P}}(t, \vec{x}) := f(t, \vec{x})$.

§7. THE GÖDEL-BERNAYS SYSTEM \mathcal{S}

Let us list the proper (non-logical) axioms of the Gödel-Bernays axiomatic set theory, denoted by \mathcal{S} , in the language of the predicate calculus \mathcal{P} (cf. [14, Chap. 4]).

Notation. For $\{\mathfrak{A}, \mathfrak{B}\} \subseteq \mathfrak{F}$ and $x \in \mathcal{X}$, let

$$\mathfrak{A} \vee \mathfrak{B} := \neg \mathfrak{B} \supset \mathfrak{A}, \quad \mathfrak{A} \& \mathfrak{B} := \neg (\neg \mathfrak{A} \vee \neg \mathfrak{B}),$$

$$\mathfrak{A} \equiv \mathfrak{B} := (\mathfrak{A} \supset \mathfrak{B}) \& (\mathfrak{B} \supset \mathfrak{A}), \quad \exists x \mathfrak{A} := \neg \forall x \neg \mathfrak{A}.$$

For $\{i, j\} \subseteq \mathbb{N} \setminus \{1\}$, write

$$\mathfrak{m}(t_i) := \exists t_1 (t_i \in t_1) \quad \text{and} \quad t_i = t_j := \forall t_1 (t_1 \in t_i \equiv t_1 \in t_j).$$

Assuming that $\{i, j, k\} \subseteq \mathbb{N} \setminus \{1\}$ and $i \notin \{j, k\}$, let

$$t_i = [t_j, t_k] := (\mathbf{m}(t_j) \& \mathbf{m}(t_k) \& \forall t_1 (t_1 \in t_i \equiv (t_1 = t_j \vee t_1 = t_k))) \\ \vee (\neg (\mathbf{m}(t_j) \& \mathbf{m}(t_k)) \& t_i = \emptyset)$$

and

$$t_i = \langle t_j, t_k \rangle := t_i = [[t_j, t_j], [t_j, t_k]].$$

Finally, let

$$t_i = \langle t_j, t_k, t_l \rangle := t_i = \langle \langle t_j, t_k \rangle, t_l \rangle$$

for $\{i, j, k, l\} \subseteq \mathbb{N} \setminus \{1\}$ and $i \notin \{j, k, l\}$. Let us introduce the set of the “set variables” $\{s_i \mid i \in \mathbb{N}, i > 1\}$ by means of the following abbreviations:

$$\forall s_i \mathfrak{A} := \forall t_i (\mathbf{m}(t_i) \supset \mathfrak{A}) \quad \text{and} \quad \exists s_i \mathfrak{A} := \neg \forall s_i \neg \mathfrak{A}$$

for $\mathfrak{A} \in \mathfrak{F}$ and $i \in \mathbb{N} \setminus \{1\}$. Write

$$t_i = \emptyset := \forall t_1 \neg (t_1 \in t_i).$$

There are sixteen proper axioms of \mathcal{S} :

$$\begin{aligned} \mathfrak{A}_1 &:= (t_2 = t_3) \supset (t_2 \in t_4 \equiv t_3 \in t_4); \\ \mathfrak{A}_2 &:= \forall s_2, s_3 \exists s_4 \forall s_1 (t_1 \in t_4 \equiv (t_1 = t_2 \vee t_1 = t_3)); \\ \mathfrak{A}_3 &:= \exists s_2 \forall s_1 \neg (t_1 \in t_2); \\ \mathfrak{A}_4 &:= \exists t_2 \forall s_3, s_4 (\langle t_3, t_4 \rangle \in t_2 \equiv t_3 \in t_4); \\ \mathfrak{A}_5 &:= \forall t_1, t_2 \exists t_3 \forall t_4 (t_4 \in t_3 \equiv (t_4 \in t_1 \& t_4 \in t_2)); \\ \mathfrak{A}_6 &:= \forall t_1 \exists t_2 \forall s_3 (t_3 \in t_2 \equiv \neg (t_3 \in t_1)); \\ \mathfrak{A}_7 &:= \forall t_1 \exists t_2 \forall s_3 (t_3 \in t_2 \equiv \exists s_4 (\langle t_3, t_4 \rangle \in t_1)); \\ \mathfrak{A}_8 &:= \forall t_1 \exists t_2 \forall s_3, s_4 (\langle t_3, t_4 \rangle \in t_2 \equiv t_3 \in t_1); \\ \mathfrak{A}_9 &:= \forall t_1 \exists t_2 \forall s_3, s_4, s_5 (\langle t_3, t_4, t_5 \rangle \in t_2 \equiv \langle t_4, t_5, t_3 \rangle \in t_1); \\ \mathfrak{A}_{10} &:= \forall t_1 \exists t_2 \forall s_3, s_4, s_5 (\langle t_3, t_4, t_5 \rangle \in t_2 \equiv \langle t_3, t_5, t_4 \rangle \in t_1); \\ \mathfrak{A}_{11} &:= \forall s_1 \exists s_2 \forall s_3 (t_3 \in t_2 \equiv \exists s_4 (t_3 \in t_4 \& t_4 \in t_1)); \\ \mathfrak{A}_{12} &:= \forall s_1 \exists s_2 \forall s_3 (t_3 \in t_2 \equiv \forall t_4 (t_4 \in t_3 \supset t_4 \in t_1)); \\ \mathfrak{A}_{13} &:= \forall s_1, t_2 \exists s_3 \forall s_4 (t_4 \in t_3 \equiv (t_4 \in t_1 \& t_4 \in t_2)); \\ \mathfrak{A}_{14} &:= \mathfrak{A}_{14}^{(1)} \supset \mathfrak{A}_{14}^{(2)}, \end{aligned}$$

where

$$\mathfrak{A}_{14}^{(1)} := (R(t_1) \& \forall s_2, s_3, s_4 (\langle t_2, t_3 \rangle \in t_1 \& \langle t_2, t_4 \rangle \in t_1) \supset t_3 = t_4)$$

with

$$R(t_1) := \forall t_2 (t_2 \in t_1 \equiv \exists t_3, t_4 (t_2 = \langle t_3, t_4 \rangle)),$$

and

$$\mathfrak{A}_{14}^{(2)} := \forall s_2 \exists s_3 \forall s_4 (t_4 \in t_3 \equiv \exists s_5 ((t_5, t_4) \in t_1 \& t_5 \in t_2));$$

$$\mathfrak{A}_{15} := \exists s_2 (\exists t_4 (t_4 \in t_2 \& t_4 = \emptyset) \& \forall s_3 (t_3 \in t_2 \supset \exists t_4 (t_4 \in t_2 \& \mathfrak{A}_{15}^{(1)}))),$$

where

$$\mathfrak{A}_{15}^{(1)} := \forall t_5 (t_5 \in t_4 \equiv (t_5 = t_3 \vee (t_5 = [t_3, t_3])));$$

\mathfrak{A}_{16} is the axiom of choice, which need not be stated here (cf., however, [14, p. 275]).

Notation. Let

$$\mathfrak{A}^{(0)} := \mathfrak{A}_1 \& \dots \& \mathfrak{A}_{15}, \quad \mathfrak{A}_0 := \mathfrak{A}^{(0)} \& \mathfrak{A}_{16},$$

$$\mathfrak{T}(\mathcal{S}^{(0)}) := \{\mathfrak{B} \mid \mathfrak{B} \in \mathfrak{F}, (\mathfrak{A}^{(0)} \supset \mathfrak{B}) \in \mathfrak{T}\},$$

and

$$\mathfrak{T}(\mathcal{S}) := \{\mathfrak{B} \mid \mathfrak{B} \in \mathfrak{F}, (\mathfrak{A}_0 \supset \mathfrak{B}) \in \mathfrak{T}\}.$$

The set $\mathfrak{T}(\mathcal{S})$ (respectively, $\mathfrak{T}(\mathcal{S}^{(0)})$) is, by definition, the set of the theorems of the system \mathcal{S} (respectively, of the system $\mathcal{S}^{(0)}$). By a theorem of K. Gödel's [6], the system \mathcal{S} is consistent if and only if $\mathcal{S}^{(0)}$ is. Thus

$$(\mathfrak{T}(\mathcal{S}^{(0)}) = \mathfrak{F}) \equiv (\mathfrak{T}(\mathcal{S}) = \mathfrak{F}).$$

Let $a_j := \mathcal{N}(\mathfrak{A}_j)$ and

$$\mathfrak{C}_1(\mathfrak{B}) := (\mathfrak{A}_1 \supset \mathfrak{B}), \quad \mathfrak{C}_{j+1}(\mathfrak{B}) := (\mathfrak{A}_{j+1} \supset \mathfrak{C}_j(\mathfrak{B})), \quad 1 \leq j < 16,$$

for $\mathfrak{B} \in \mathfrak{F}$. Further, let $b := \mathcal{N}(\mathfrak{B})$ and let

$$f_1(\vec{x}) = 4p(x_1, y), \quad f_{j+1}(\vec{x}, y) = 4p(x_{j+1}, f_j(\vec{x}, y)), \quad 1 \leq j < l, \quad (5)$$

where $\vec{x} := (x_1, \dots, x_l)$. It follows then that

$$\mathcal{N}(\mathfrak{C}_j(\mathfrak{B})) = f_j(\vec{a}, b), \quad 1 \leq j \leq 16,$$

with $\vec{a} := (a_1, \dots, a_{16})$. Thus we can let

$$F_{\mathcal{S}^{(0)}}(t, \vec{x}) := F_{\mathcal{P}}(f_{15}(\vec{a}, t), \vec{x})$$

and

$$F_{\mathcal{S}}(t, \vec{x}) := F_{\mathcal{P}}(f_{16}(\vec{a}, t), \vec{x});$$

let $n := 3639528$. By construction, if

$$\neg \mathfrak{B} \in \mathfrak{T}(\mathcal{S}),$$

then the formula

$$\exists \vec{c} (\vec{c} \in \mathbb{Z}^{4n} \& F_{\mathcal{S}}(b, \vec{c}) = 0)$$

asserts that $\mathfrak{T}(\mathcal{S}) = \mathfrak{F}$; likewise, if

$$\neg \mathfrak{B} \in \mathfrak{T}(\mathcal{S}^{(0)}),$$

then the formula

$$\exists \vec{c} (\vec{c} \in \mathbb{Z}^{4n} \ \& \ F_{\mathcal{S}^{(0)}}(b, \vec{c}) = 0)$$

asserts that $\mathfrak{T}(\mathcal{S}_0) = \mathfrak{F}$. Take, for instance,

$$\mathfrak{B} := \forall t_1 (t_1 \in t_1),$$

then $\mathcal{N}(\mathfrak{B}) = 3$ and

$$\neg \mathfrak{B} \in \mathfrak{T}(\mathcal{S}^{(0)}).$$

Thus the formula

$$\exists \vec{c} (\vec{c} \in \mathbb{Z}^{4n} \ \& \ F_{\mathcal{S}^{(0)}}(3, \vec{c}) = 0)$$

asserts that $\mathfrak{T}(\mathcal{S}^{(0)}) = \mathfrak{T}(\mathcal{S}) = \mathfrak{F}$. In view of Gödel's second theorem [14, pp. 212-213], we can summarise our conclusions as follows.

Theorem 2. *Let $\mathfrak{B} \in \mathfrak{F}$ and suppose that $\neg \mathfrak{B} \in \mathfrak{T}(\mathcal{S}^{(0)})$. If the Gödel-Bernays axiomatic set theory \mathcal{S} is consistent, then although the Diophantine equation*

$$F_{\mathcal{S}^{(0)}}(b, \vec{x}) = 0, \ b := \mathcal{N}(\mathfrak{B}),$$

has no solutions in \mathbb{Z} , the formula

$$\neg \exists \vec{c} (\vec{c} \in \mathbb{Z}^{4n} \ \& \ F_{\mathcal{S}^{(0)}}(b, \vec{c}) = 0)$$

can not be proved in the system \mathcal{S} . The function $b \mapsto f_{15}(\vec{a}, b)$ can be explicitly evaluated by means of (5) and (6)–(20) below.

Corollary 4. *If the Gödel-Bernays axiomatic set theory \mathcal{S} is consistent, then although the Diophantine equation*

$$F_{\mathcal{S}^{(0)}}(3, \vec{x}) = 0$$

has no solutions in \mathbb{Z} , the formula

$$\neg \exists \vec{c} (\vec{c} \in \mathbb{Z}^{4n} \ \& \ F_{\mathcal{S}^{(0)}}(3, \vec{c}) = 0)$$

can not be proved in the system \mathcal{S} .

§8. APPENDIX TO §7

The following formulae (6)–(20) provide explicit expressions for the numbers $a_j := \mathcal{N}(\mathfrak{A}_j)$, $1 \leq j \leq 16$. An easy calculation shows that

$$\begin{aligned} \mathcal{N}(\mathfrak{A} \vee \mathfrak{B}) &= \nu_0(\mathcal{N}(\mathfrak{A}), \mathcal{N}(\mathfrak{B})), & \mathcal{N}(\mathfrak{A} \& \mathfrak{B}) &= \nu_1(\mathcal{N}(\mathfrak{A}), \mathcal{N}(\mathfrak{B})), \\ \mathcal{N}(\mathfrak{A} \equiv \mathfrak{B}) &= \nu_2(\mathcal{N}(\mathfrak{A}), \mathcal{N}(\mathfrak{B})), & \mathcal{N}(\exists t_i \mathfrak{A}) &= \nu_3(i, \mathcal{N}(\mathfrak{A})), \end{aligned}$$

where

$$\begin{aligned} \nu_0(u, v) &:= 4p(4v - 2, u), & \nu_1(u, v) &:= 4\nu_0(4u - 2, 4v - 2) - 2, \\ \nu_2(u, v) &:= \nu_1(4p(u, v), 4p(v, u)), & \nu_3(i, u) &:= 16p(i, 4u - 2) - 6, \end{aligned}$$

and

$$\begin{aligned} \mathcal{N}(\mathfrak{m}(t_i)) &= \nu_4(i), & \mathcal{N}(t_i = \emptyset) &= \nu_5(i), & \mathcal{N}(t_i = t_j) &= \nu_6(i, j), \\ \mathcal{N}(\forall s_i \mathfrak{A}) &= \nu_7(i, \mathcal{N}(\mathfrak{A})), & \mathcal{N}(\exists s_i \mathfrak{A}) &= \nu_8(i, \mathcal{N}(\mathfrak{A})) \end{aligned}$$

with

$$\begin{aligned} \nu_4(i) &:= \nu_3(1, 4p(i, 1) - 3), & \nu_5(i) &:= 4p(1, 16p(1, i) - 14) - 1, \\ \nu_6(i, j) &:= 4p(1, \nu_2(4p(1, i) - 3, 4p(1, j) - 3)) - 1, \\ \nu_7(i, u) &:= 4p(i, 4p(\nu_4(i), u)) - 1, & \nu_8(i, u) &:= 4\nu_7(i, 4u - 2) - 2. \end{aligned}$$

A further calculation shows that

$$\mathcal{N}(t_i = [t_j, t_k]) = \nu_9(i, j, k)$$

with $\nu_9(i, j, k) := \nu_0(u_1, u_2)$, where

$$\begin{aligned} u_1 &:= \nu_1(\nu_1(\nu_4(j), \nu_4(k)), u_3), & u_3 &:= 4p(1, \nu_2(4p(1, i) - 3, u_4)) - 1, \\ u_4 &:= \nu_0(4p(1, j) - 3, 4p(1, k) - 3), & u_2 &:= \nu_1(u_5, \nu_5(i)), \\ u_5 &:= 4\nu_1(\nu_4(j), \nu_4(k)) - 2; \\ \mathcal{N}(t_i = \langle t_j, t_k \rangle) &= \nu_{10}(i, j, k) \end{aligned}$$

with $\nu_{10}(i, j, k) := \nu_3(u_1, \nu_3(u_2, u_3))$, where

$$\begin{aligned} u_1 &:= i + j + k, & u_2 &:= u_1 + 1, & u_3 &:= \nu_2(u_4, \nu_9(i, u_1, u_2)), \\ u_4 &:= \nu_1(\nu_9(u_1, j, j), \nu_9(u_2, j, k)); \\ \mathcal{N}(t_i = \langle t_j, t_k, t_l \rangle) &= \nu_{11}(i, j, k, l) \end{aligned}$$

with $\nu_{11}(i, j, k, l) := \nu_3(u_1, u_2)$, where

$$u_1 := i + j + k + l, \quad u_2 := \nu_1(\nu_{10}(u_1, j, k), \nu_{10}(i, u_1, k)).$$

It follows now that

$$a_1 = 4p(\nu_6(2, 3), \nu_2(4p(2, 4) - 3, 4p(3, 4) - 3)); \quad (6)$$

$$a_2 = \nu_7(2, \nu_7(3, \nu_8(4, \nu_7(1, u)))) \quad (7)$$

with $u = \nu_2(4p(1, 4) - 3, \nu_0(\nu_6(1, 2), \nu_6(1, 3)))$;

$$a_3 = \nu_8(2, \nu_7(1, 4p(1, 2) - 3)); \quad (8)$$

$$a_4 = \nu_3(2, \nu_7(3, \nu_7(4, u_1))), \quad (9)$$

where $u_1 := \nu_2(\nu_3(5, u_2), 4p(3, 4) - 3)$ and $u_2 := \nu_1(\nu_{10}(5, 3, 4), 4p(5, 2) - 3)$;

$$a_5 = 4p(1, 4p(2, u_1) - 1) - 1, \quad (10)$$

where $u_1 := \nu_3(3, 4p(4, \nu_2(u_2, u_3)) - 1)$, $u_2 := 4p(4, 3) - 3$,
and $u_3 := \nu_1(4p(4, 1) - 3, 4p(4, 2) - 3)$;

$$a_6 = 4p(1, \nu_3(2, u_1)) - 1, \quad (11)$$

where $u_1 := \nu_7(3, \nu_2(u_2, u_3))$, $u_2 := 4p(3, 2) - 3$, and $u_3 := 16p(3, 1) - 14$;

$$a_7 = 4p(1, \nu_3(2, u_1)) - 1, \quad (12)$$

where $u_1 := \nu_7(3, \nu_2(u_2, u_3))$, $u_2 := 4p(3, 2) - 3$, $u_3 := \nu_8(4, u_4)$, and

$$u_4 := \nu_3(5, \nu_1(\nu_{10}(5, 3, 4), 4p(5, 1) - 3));$$

$$a_8 = 4p(1, \nu_3(2, u_1)) - 1, \quad (13)$$

where $u_1 := \nu_7(3, \nu_7(4, u_2))$, $u_2 := \nu_2(u_3, 4p(3, 1) - 3)$, and

$$u_3 := \nu_3(5, \nu_1(\nu_{10}(5, 3, 4), 4p(5, 2) - 3));$$

$$a_9 = 4p(1, \nu_3(2, u_1)) - 1, \quad (14)$$

where $u_1 := \nu_7(3, \nu_7(4, \nu_7(5, u_2)))$, $u_2 := \nu_3(6, \nu_3(7, \nu_1(u_3, u_4)))$,

$$u_3 := \nu_1(\nu_{11}(6, 3, 4, 5), \nu_{11}(7, 4, 5, 3)),$$

and $u_4 := \nu_2(4p(6, 2) - 3, 4p(7, 1) - 3)$;

$$a_{10} = 4p(1, \nu_3(2, u_1)) - 1, \quad (15)$$

where $u_1 := \nu_7(3, \nu_7(4, \nu_7(5, u_2)))$, $u_2 := \nu_3(6, \nu_3(7, \nu_1(u_3, u_4)))$, $u_3 := \nu_1(\nu_{11}(6, 3, 4, 5), \nu_{11}(7, 3, 5, 4))$, and $u_4 := \nu_2(4p(6, 2) - 3, 4p(7, 1) - 3)$;

$$a_{11} = \nu_7(1, \nu_8(2, \nu_7(3, u_1))), \quad (16)$$

where $u_1 := \nu_2(4p(3, 2) - 3, \nu_8(4, u_2))$ and $u_2 := \nu_1(4p(3, 4) - 3, 4p(4, 1) - 3)$;

$$a_{12} = \nu_7(1, \nu_8(2, \nu_7(3, u_1))), \quad (17)$$

where $u_1 := \nu_2(4p(3, 2) - 3, u_2)$, $u_2 := 4p(4, u_3) - 1$,
and $u_3 := 4p(4, 3) - 3, 4p(4, 1) - 3$;

$$a_{13} = \nu_7(1, 4p(2, u_1) - 1), \quad (18)$$

where $u_1 := \nu_8(3, \nu_7(4, u_2))$, $u_2 := \nu_2(4p(4, 3) - 3, u_3)$,
and $u_3 := \nu_1(4p(4, 1) - 3, 4p(4, 2) - 3)$;

$$a_{14} = 4p(u_1, u_2), \quad (19)$$

where

$$\begin{aligned} u_1 &:= \nu_1(v_1, v_2), \quad v_1 := 4p(2, \nu_2(v_3, v_4)), \quad v_3 := 4p(2, 1) - 3, \\ u_2 &:= \nu_3(3, \nu_3(4, \nu_{10}(2, 3, 4))), \quad v_2 := \nu_7(2, \nu_7(3, \nu_7(4, v_5))), \\ u_3 &:= 4p(\nu_1(v_6, v_7), \nu_6(3, 4)), \quad v_6 := \nu_3(5, \nu_1(\nu_{10}(5, 2, 3), 4p(5, 1) - 3)), \\ u_4 &:= \nu_3(5, \nu_1(\nu_{10}(5, 2, 4), 4p(5, 1) - 3)), \end{aligned}$$

and

$$\begin{aligned} u_5 &:= \nu_7(2, \nu_8(3, \nu_7(4, v_8))), \quad v_8 := \nu_2(4p(4, 3) - 3, v_9), \\ u_6 &:= \nu_8(5, \nu_1(v_{10}, 4p(5, 2) - 3)), \quad v_{10} := \nu_3(6, \nu_1(\nu_{10}(6, 5, 4), 4p(6, 1) - 3)); \\ u_7 &:= \nu_8(2, \nu_1(u_1, u_2)), \end{aligned} \quad (20)$$

where

$$\begin{aligned} u_1 &:= \nu_3(4, \nu_1(4p(4, 2) - 3, \nu_5(4))), \quad u_2 := \nu_7(3, 4p(4p(3, 2) - 3, u_3)), \\ u_3 &:= \nu_3(4, \nu_1(4p(4, 2) - 3, 4p(5, u_4) - 1)), \end{aligned}$$

and

$$u_4 := \nu_2(4p(5, 4) - 3, \nu_0(\nu_6(5, 3), \nu_9(5, 3, 3))).$$

Acknowledgement. We are indebted to Professor Yu. V. Matiyasevich for a private communication [13], relating to this work, and for his remarks on a preliminary version of our paper.

REFERENCES

1. M. Carl, *Formale Mathematik und diophantische Gleichungen*. Diplomarbeit, Universität Bonn, 2007.
2. M. Davis, *Hilbert's tenth problem is unsolvable*. — *The American Mathematical Monthly* **80** (1973), 233–269.
3. M. Davis, Yu. Matijasevič, Ju. Robinson, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution*. — *Proceedings of Symposia in Pure Maths* **28** (1976), 323–378.
4. V. H. Dyson, J. P. Jones, J. C. Shepherdson, *Some Diophantine forms of Gödel's theorem*. — *Archiv für Mathematische Logik und Grundlagenforschung* **22** (1982), no. 1-2, 51–60.
5. H. M. Friedman, *Finite functions and the necessary use of large cardinals*. — *Ann. Math.* **148** (1998), 803–893.
6. K. Gödel, *The consistency of the axiom of choice and of the generalised continuum hypothesis with the axioms of set theory*. Princeton University Press, 1940.

7. J. P. Jones, *Universal Diophantine equation*. — J. Symb. Logic **47** (1982), 549–571.
8. L. Kalmár, *Zurückführung des Entscheidungsproblems auf den Fall von Formeln mit einer einzigen binären Funktionsvariablen*. — Compositio Mathematica **4** (1936), 137–144.
9. Yu. I. Manin, *Brouwer memorial lecture*. — Nieuw Arch. Wisk. (4) **6** (1988), no. 1–2, 1–6.
10. Yu. V. Matiyasevich, *Enumerable sets are Diophantine*. — Dokl. Akad. Nauk SSSR **191**, No. 2 (1970), 279–282.
11. Yu. V. Matiyasevich, *Diophantine representation of enumerable predicates*. — Izv. Akad. Nauk SSSR. Ser. Mat. **35**, No. 1 (1971), 3–30.
12. Yu. V. Matiyasevich, *Hilbert's Tenth Problem*. Nauka, Moskva, 1993.
13. Yu. V. Matiyasevich, *An e-mail letter to the second author*. March 2005.
14. E. Mendelson, *Introduction to Mathematical Logic*. Chapman&Hall/CRM, 2001.

Fachbereich Mathematik und Statistik,
Universität Konstanz, Universitätsstrasse 10,
D-78457 Konstanz, GERMANY
E-mail: merlin.carl@uni-konstanz.de

Поступило 5 ноября 2012 г.

Max-Planck-Institut für Mathematik,
Vivatsgasse 7, D-53111 Bonn, GERMANY
E-mail: moroz@mpim-bonn.mpg.de