A polynomial encoding provability in pure mathematics (outline of an explicit construction)

M. Carl B.Z. Moroz

To professor G.E. Mints on his seventieth birthday

1. Let V be an algebraic variety defined over $\mathbb{Z}$, the ring of rational integers. The study of the structure of the set $V(\mathbb{Z})$ of the integral points of such a variety is one of the major goals in number theory and arithmetic geometry. One may ask, in particular, whether $V(\mathbb{Z})$ is an empty or a finite set. It is an easy and well-known corollary of the celebrated theorem of Matiyasevich [11] that, in a given formal system, neither statement can be proved or disproved for infinitely many varieties V (cf. [11] - [13], [4, pp. 327-328], [5]). For instance, there is a hypersurface V over $\mathbb{Z}$ such that neither the assertion

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

nor its negation is provable in, say, the Zermelo-Fraenkel set theory (=:ZF).

Given a recursively enumerable subset S of the set $\mathbb{N}$ of the positive rational integers, Matiyasevich's construction allows, in principle, to write down a polynomial $P_S(t, \vec{x})$, $\vec{x} := (x_1, \ldots, x_{n(S)})$, with integral rational coefficients such that, for $a \in \mathbb{N}$, the Diophantine equation $P_S(a, \vec{x}) = 0$ is soluble in $\mathbb{Z}^{n(S)}$ if and only if $a \in S$. The set T of the (ZF-)provable mathematical theorems is recursively enumerable. Therefore, given a suitable numbering $\mathcal{N}$ of the set of the well-defined mathematical assertions, one can construct a polynomial $F(t, \vec{x})(:= P_{\mathcal{N}(T)}(t, \vec{x}))$ such that the Diophantine equation $F(a, \vec{x}) = 0$ is soluble if and only if $a \in \mathcal{N}(T)$. In this sense, the arithmetic of the affine hypersurface, defined by the equation

Received by the editors April 2012.
Communicated by A. Weiermann.
2010 *Mathematics Subject Classification :* 11D72, 11G35, 11U05, 03E55.
Key words and phrases : Matiyasevich's theorem, Diophantine coding, Gödel-Bernays set theory.

$F(t, \vec{x}) = 0$, is "exactly as difficult as the whole of mathematics" [10, p. 2]; indeed, according to Gauß, "number theory is the queen of mathematics".

In this note, we shall outline an explicit construction of a polynomial encoding provability in pure mathematics as formalized in the Gödel-Bernays axiomatic set theory; the minute details of that construction will be found in our work [2] (cf. also [1]). As a by-product, one obtains a true mathematical statement that can not be proved in the Zermelo-Fraenkel set theory and for its proof requires new "axioms, which go beyond the usual axioms for mathematics", cf. [6, p. 804]. Our arithmetic statement (1) seems to be simpler and by far more natural than the combinatorial statements presented in the work of H.M. Friedman [6] cited above.

Notation and conventions. As usual, $\mathbb{Z}$ stands for the ring of rational integers and $\mathbb{N} := \{n \mid n \in \mathbb{Z},\ n \geq 1\}$. A finite sequence of symbols is denoted by $\vec{x}$ and $L(\vec{x})$ stands for its length (we write, for instance, $\vec{x} := (y_1, \ldots, y_n)$ and $L(\vec{x}) = n$). The polynomial

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

defines a bijection

$$p\colon \mathbb{N}^2 \to \mathbb{N},\ p\colon \vec{a} \mapsto p(\vec{a}) \text{ for } \vec{a} \in \mathbb{N}^2.$$

2. Let $\mathcal{P}$ be the predicate calculus with a single binary predicate letter (and no function letters or individual constants). By Kalmár's theorem [9] (cf. also [14, p. 223]), analysis of provability in any pure predicate calculus can be reduced to studying provability in $\mathcal{P}$. Moreover, the Gödel-Bernays set theory, to be denoted by $\mathfrak{S}$, is known to be finitely axiomatisable in $\mathcal{P}$ [7], [14, Ch.4]. In our work [2], we describe a polynomial encoding provability in $\mathcal{P}$ and thereby in $\mathfrak{S}$. In what follows, we sketch briefly the construction of that polynomial.

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 $(x\ \varepsilon\ y)$, with $\{x,\ y\} \subseteq \mathcal{X}$, is a formula; if $\mathfrak{A}$ and $\mathfrak{B}$ are formulae and $x \in \mathcal{X}$, then $\neg\, \mathfrak{A}$, $(\mathfrak{A} \supset \mathfrak{B})$, and $\forall x\, \mathfrak{A}$ are formulae.

Remark. The symbols " $\subseteq$ " and " $\in$ " have the usual meaning and should not be confused with the letters " $\supset$ ", "ε" of the language of $\mathcal{P}$. For instance, the expression $\{x,\ y\} \subseteq \mathcal{X}$ means, of course, that $x = t_i$ and $y = t_j$ for some i and j in $\mathbb{N}$.

A bijective map $\mathcal{N}\colon \mathfrak{F} \to \mathbb{N}$ is defined inductively:

$$\mathcal{N}(t_i\ \varepsilon\ t_j) = 4p(i, j) - 3$$

for $\{i,\ j\} \subseteq \mathbb{N}$ and

$$\mathcal{N}(\neg\, \mathfrak{A}) = 4\mathcal{N}(\mathfrak{A}) - 2,$$

$$\mathcal{N}(\forall t_i\ \mathfrak{A}) = 4p(i, \mathcal{N}(\mathfrak{A})) - 1,$$
$$\mathcal{N}(\mathfrak{A} \supset \mathfrak{B}) = 4p(\mathcal{N}(\mathfrak{A}), \mathcal{N}(\mathfrak{B}))$$

for $\{\mathfrak{A},\ \mathfrak{B}\} \subseteq \mathfrak{F}$ and $i \in \mathbb{N}$.

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

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

$$\mathcal{A}_2 := \{(\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{C})) \supset ((\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \mathfrak{C})) \mid \{\mathfrak{A},\ \mathfrak{B},\ \mathfrak{C}\} \subseteq \mathfrak{F}\};$$
$$\mathcal{A}_3 := \{(\neg\, \mathfrak{B} \supset \neg\, \mathfrak{A}) \supset ((\neg\, \mathfrak{B} \supset \mathfrak{A}) \supset \mathfrak{B}) \mid \{\mathfrak{A},\ \mathfrak{B}\} \subseteq \mathfrak{F}\};$$
$$\mathcal{A}_4 := \{\forall x\ (\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \forall x\ \mathfrak{B}) \mid \{\mathfrak{A},\ \mathfrak{B}\} \subseteq \mathfrak{F},\ x \in \mathcal{X} \setminus [\mathfrak{A}]_f\},$$

where $[\mathfrak{A}]_f$ stands for the set of the free variables of $\mathfrak{A}$;

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

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

where $\mathfrak{A}[x|y]$ denotes the formula obtained from $\mathfrak{A}$ when each of the *free* occurrences of the variable x in $\mathfrak{A}$ is replaced by y. The set $\mathfrak{T}$ of the theorems of $\mathcal{P}$ is defined inductively:

(i) $\cup_{j=1}^{5} \mathcal{A}_j \subseteq \mathfrak{T}$;

(ii) if $\{\mathfrak{A},\ (\mathfrak{A} \supset \mathfrak{B})\} \subseteq \mathfrak{T}$, then $\mathfrak{B} \in \mathfrak{T}$ ("modus ponens");

(iii) if $\mathfrak{A} \in \mathfrak{T}$ and $x \in \mathcal{X}$, then $\forall x\ \mathfrak{A} \in \mathfrak{T}$ ("generalisation").

To give a Diophantine description of the predicate "$\mathfrak{A}$ is an axiom of $\mathcal{P}$", we construct a polynomial $g_i(u, \vec{x})$ for $1 \leq i \leq 5$ such that $g_i(u, \vec{x}) \in \mathbb{Z}[u, \vec{x}]$ and

$$\mathcal{N}(\mathcal{A}_i) = \{u \mid u \in \mathbb{N},\ (\exists\, \vec{b} \in \mathbb{N}^{L(\vec{x})}) g_i(u, \vec{b}) = 0\},\ 1 \leq i \leq 5.$$

It can be easily seen [2] that we may let

$$g_1(u, \vec{x}) := u - 4p(x_1, 4p(x_2, x_1))$$

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

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

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

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

with $\vec{x} := (x_1, x_2)$. In order to construct the polynomials $g_4(u, \vec{x})$ and $g_5(u, \vec{y})$, one employs techniques of Diophantine coding developed in the works on Hilbert's tenth problem (cf. [3], [13], and references therein). This construction is the technical heart of our works [1] and [2]. The detailed description of those polynomials is beyond the scope of this note; let us mention, however, that

$$g_4(u, \vec{x}) \in \mathbb{Z}[u, \vec{x}] \text{ with } L(\vec{x}) = 8878$$

and

$$g_5(u,\vec{y}) \in \mathbb{Z}[u,\vec{y}] \text{ with } L(\vec{y}) = 17873.$$

Let

$$G_1(\vec{u};x) := x(u_3 - 4p(u_2,u_1))$$

with $\vec{u} := (u_1,u_2,u_3)$ and let

$$G_2(\vec{u};x) := u_1 - 4p(x,u_2) + 1$$

with $\vec{u} := (u_1,u_2)$. Let

$$u_i := \mathcal{N}(\mathfrak{A}_i),\ \mathfrak{A}_i \in \mathfrak{F},\ 1 \le i \le 3.$$

It can be easily proved [2] that the formula $\mathfrak{A}_1$ follows from the formulae $\mathfrak{A}_2$ and $\mathfrak{A}_3$ by the rule "modus ponens" (respectively from the formula $\mathfrak{A}_2$ by the rule "generalisation") if and only if $(\exists\ b \in \mathbb{N})G_1(\vec{u};b) = 0$ (respectively $(\exists\ b \in \mathbb{N})G_2(\vec{u};b) = 0$). Applying techniques of Diophantine coding again, we construct a polynomial $f(t,\vec{x})$ such that $f(t,\vec{x}) \in \mathbb{Z}[t,\vec{x}]$ and

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

with $L(\vec{x}) = 4n,\ n := 3639528$ [2, Corollary 3]. The polynomial $f(t,\vec{x})$ is explicitly expressible in terms of the polynomials $G_1, G_2, g_1, g_2, g_3, g_4$, and g_5 (see [2]).

3. Let us say a few words about "Diophantine coding", the term coined in the works on Hilbert's tenth problem (see [13, Chapter 5], for example) and alluded to in the previous section. A "Diophantine code" of an enumerable subset S of the set $\mathbb{N}$ of natural numbers is a polynomial $P_S(t,\vec{x})$ such that

$$P_S(t,\vec{x}) \in \mathbb{Z}[t,\vec{x}],\ \vec{x} := (x_1,\ldots,x_{n(S)}),$$

and

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

The techniques, used to construct Diophantine codes, may be illustrated by the following examples. The Lagrange four squares theorem leads to the representation

$$\mathbb{N} := \{1 + \sum_{k=1}^{4} x_k^2 \mid \vec{x} \in \mathbb{Z}^4,\ \vec{x} := (x_1,x_2,x_3,x_4)\},$$

allowing us to replace a Diophantine equation in $\mathbb{N}$ by an equivalent one in $\mathbb{Z}$; on the other hand, a Diophantine equation in $\mathbb{Z}$ can be replaced by an equivalent Diophantine equation in $\mathbb{N}$ simply by expressing an integer as a difference of two natural numbers, cf. [13, §1.3]. As another example, let us consider the set $\mathbb{P}$ of the prime numbers. Let $p \in \mathbb{N}$; by definition, $p \in \mathbb{P}$ if and only if

$$p > 1\ \&\ (\forall x \in \mathbb{N}, x \le p)(\forall y \in \mathbb{N}, y \le p)\ p = xy \Rightarrow (x-1)(y-1) = 0. \qquad (2)$$

Let

$$h(\vec{u}) := (u_1 - 1 - u_4)^2 + (u_1 - u_2u_3 - u_5)^2(u_2 - 1)^2(u_3 - 1)^2,\ \vec{u} := (u_1,\ldots,u_5);$$

formula (2) is easily seen be equivalent to the following one:

$$(\forall x \in \mathbb{N}, x \leq p)(\forall y \in \mathbb{N}, y \leq p)(\exists\, \vec{z} \in \mathbb{N}^2)h(p, x, y, z_1, z_2) = 0, \tag{3}$$

with $\vec{z} := (z_1, z_2)$. The Diophantine code $P_{\mathbb{P}}(t, \vec{x})$ of the set $\mathbb{P}$ of the prime numbers can be constructed from formula (3) by repeated application of the bounded quantifier theorem [3, §5], [4, §4], one of the main tools used in Diophantine coding. Another important tool is the sequence number theorem [3, p. 237], allowing, for instance, to produce a polynomial $P_g(t_1, t_2, \vec{x})$ with integral rational coefficients, which encodes the graph of the function

$$g : \mathbb{N} \to \mathbb{N},\ g : y \mapsto \prod_{k=1}^{y}(1 + k^2),\ y \in \mathbb{N},$$

so that

$$(\exists\, \vec{b} \in \mathbb{Z}^{L(\vec{b})})P_g(z, g(y), \vec{b}) = 0 \Leftrightarrow z = g(y)$$

for $\{z,\ y\} \subseteq \mathbb{N}$, cf. [3, p. 257]. The other tools of Diophantine coding are borrowed from elementary number theory.

4. Let $\mathfrak{T}_0$ stand for the set of the theorems of the Gödel-Bernays axiomatic set theory $\mathfrak{S}$ and let $\mathfrak{A}$ be the conjunction of the proper (non-logical) axioms of $\mathfrak{S}$ in the language of $\mathcal{P}$ [14], [2]. By definition, $\mathfrak{B} \in \mathfrak{T}_0$ if and only if the formula $(\mathfrak{A} \supset \mathfrak{B})$ belongs to $\mathfrak{T}$, the set of the theorems of $\mathcal{P}$. If the theory $\mathfrak{S}$ is consistent, that is if $\mathfrak{T}_0 \neq \mathfrak{F}$, then the formula $(t_1\ \varepsilon\ t_1)$ is not in $\mathfrak{T}_0$. Let

$$m := \mathcal{N}(\mathfrak{A} \supset (t_1\ \varepsilon\ t_1)),$$

let $F(\vec{x}) := f(m, \vec{x})$, and let V be the hypersurface defined by the equation $F(\vec{x}) = 0$, then

$$(\exists\, \vec{b} \in \mathbb{Z}^{4n})F(\vec{b}) = 0 \Leftrightarrow \mathfrak{T}_0 = \mathfrak{F}.$$

Therefore if the Gödel-Bernays axiomatic set theory $\mathfrak{S}$ is consistent, then the statement $V(\mathbb{Z}) = \emptyset$ is true but can not be proved in $\mathfrak{S}$.

5. The polynomials $f(t, \vec{x})$ and $F(\vec{x})$ are rather complicated. Although one does not expect a polynomial, encoding provability in pure mathematics, be too simple, it is not known how complicated it *must* be. Let $P(z, \vec{y})$ be an universal polynomial (the reader may consult references [8], [13, Ch. 4], and the literature cited in those works for different constructions of an universal polynomial) and let $\mathcal{M}$ be the numbering of the ring of polynomials with integral rational coefficients used in the construction of the polynomial $P(z, \vec{y})$. The Diophantine equation $f(t, \vec{x}) = 0$ (respectively $F(\vec{x}) = 0$) is soluble in $\mathbb{Z}$ if and only if the equation $P(\mathcal{M}(f), \vec{y}) = 0$ (respectively $P(\mathcal{M}(F), \vec{y}) = 0$) is. It is clear, however, that the integers $\mathcal{M}(f)$ and $\mathcal{M}(F)$ are at least as "complicated" as the polynomials $f(t, \vec{x})$ and $F(\vec{x})$.

Is it possible to construct a polynomial encoding provability in $\mathcal{P}$ and/or in $\mathfrak{S}$, which can be written down in a few lines ?

6. It should be observed that we have only used the techniques developed in the course of the proof of Matiyasevich's theorem, but not the theorem itself. Since no algorithm can possibly decide provability in the Gödel-Bernays set theory, Matiyasevich's theorem follows from our results.

Acknowledgement. We are grateful to Professor Yu.V. Matiyasevich and to Professor G.E. Mints for several useful conversations, relating to the problems discussed in this note. We are indebted to the referee for a few helpful remarks and comments.

References

[1] M. Carl, Formale Mathematik und diophantische Gleichungen, Diplomarbeit, Universität Bonn, 2007 (unpublished).

[2] M. Carl and B.Z. Moroz, On a Diophantine representation of the predicate of provability, Zapiski Nauchnykh Seminarov POMI, 407 (2012), 77-104.

[3] M. Davis, Hilbert's tenth problem is unsolvable, The American Mathematical Monthly, 80 (1973), 233 - 269.

[4] M. Davis, Yu. Matijasevič, and Ju. Robinson, Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution, *Proceedings of Symposia in Pure Maths,* 28 (1976), 323-378.

[5] V.H. Dyson, J.P. Jones, and J.C. Shepherdson, Some Diophantine forms of Gödel's theorem, *Archiv für Mathematische Logik und Grundlagenforschung,* 22 (1982), no. 1-2, 51-60.

[6] H.M. Friedman, Finite functions and the necessary use of large cardinals, *Annals of Mathematics,* 148 (1998), 803-893.

[7] K. Gödel, The consistency of the axiom of choice and of the generalized continuum hypothesis with the axioms of set theory, Princeton University Press, 1940.

[8] J.P. Jones, Universal Diophantine equation, *Journal of Symbolic Logic*, 47 (1982), 549-571.

[9] L. Kalmár, Zurückführung des Entscheidungsproblems auf den Fall von Formeln mit einer einzigen binären Funktionsvariablen, Compositio Mathematica, 4 (1936), 137 - 144.

[10] Yu.I. Manin, Brouwer memorial lecture, *Nieuw Arch. Wisk.*(4), 6 (1988), no. 1-2, 1-6.

[11] Yu.V. Matiyasevich, Enumerable sets are Diophantine, *Doklady AN SSSR,* 191:2 (1970), 279-282 (translated in: *Soviet Math. Doklady,* 11 (1970), 354-358).

[12] Yu.V. Matiyasevich, Diophantine representation of enumerable predicates, *Izvestiya AN SSSR. Seriya Matematicheskaya*, 35:1 (1971), 3-30 (translated in: *Mathematics of the USSR. Izvestiya,* 15(1) (1971), 1-28).

[13] Yu.V. Matiyasevich, *Hilbert's Tenth Problem,* Moskva, Nauka, 1993 (translated in: *Hilbert's Tenth Problem,* The MIT Press, 1993).

[14] E. Mendelson, *Introduction to Mathematical Logic,* Chapman & Hall/CRM, 2001.

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

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