Diophantine Modeling of Provability in Algebraic Logic

Andrea Formisano[1,*], Isacco Gavazzi[2] and Eugenio G. Omodeo[3]

[1]*DMIF, Dept. of Mathematics, Computer Science and Physics, University of Udine, Italy*

[3]*Graduated from the University of Trieste, Italy*

[3]*DMIG, Dept. of Mathematics, Informatics and Geosciences, University of Trieste, Italy*

Abstract

It has long been established that the set Th of theorems in an axiomatic formal theory is recursively enumerable (r.e.). Building upon the Davis-Putnam-Robinson-Matiyasevich theorem, which states that every r.e. set is Diophantine, this paper explores the complexity of representing Th through a Diophantine equation $D = 0$. We contend that a good trade-off between two primary measures of the complexity of the representation, which are the number of unknowns and the degree of the polynomial D, should aim at the transparency of the representation. Our work builds on a previous construction, notably that of M. Carl and B.Z. Moroz, who have provided a Diophantine representation of the sentences provable in the Gödel-Bernays class theory (NBG) within first-order predicate calculus. In contrast, our Diophantine representation of NBG relies on a modernized version of Schröder's algebra of relations, specifically the $\mathcal{L}^{\times}$ equational calculus proposed by A. Tarski and S. Givant. Additionally, we replace NBG's traditional axioms with an alternative axiomatization by H. Friedmann. These changes reduce the complexity of the Diophantine representation of NBG's provability, while maintaining equivalence to more classical formalizations. While we provide only preliminary insights into this novel equational axiomatization, we report on initial experiments with these axioms using the Vampire theorem prover.

Keywords

Diophantine sets, Algebraic logic, Class theory

1. Introduction

For a long time (see, e.g., [1]), it has been known that the set Th of all theorems of an axiomatic formal theory is recursively enumerable (*r.e.* for short). In light of the Davis-Putnam-Robinson-Matiyasevich theorem [2, 3], which claims that every r.e. set is Diophantine, it follows that under any effective encoding $\mathcal{N}$ of sentences by natural numbers, a polynomial $D(a, x_1, \ldots, x_M)$ with integer coefficients can be determined such that the following biimplication holds for each sentence α:

$$\alpha \in \mathsf{Th} \leftrightarrow (\exists\, x_1, \ldots, x_M \in \mathbb{N})\big(\, D(\mathcal{N}(\alpha);\; x_1, \ldots, x_M) \;=\; 0\,\big)\,. \qquad (\dagger)$$

How complex is such a set of theorems? Two complexity measures associated with a Diophantine representation (†), as well as trade-offs between the two, are discussed in [4, p. 153 ff.]:

Rank of Th: The minimum possible value of M, the number of unknowns x_i in a representation (†).

Order of Th: The minimum possible degree of D with respect to the unknowns x_i in (†).

Taken alone, the order can always be kept below 5—at the price, however, of a significant increase in the rank (see [4, pp. 3–4]). Taken alone, the rank can always be kept below 11—though at the cost of an order exceeding 10^{44} (see [5, p. 552]); ways of balancing the two measures emerge, in fact, from the study [5] on universal Diophantine equations.

A criterion for best associating a polynomial D with a theory Th is that the construction of D should be *transparent*, in the sense that it closely mirrors the process of deriving a theorem α from the axioms of Th in a specific formal system. This criterion may appear somewhat elusive, but it is well illustrated

CILC 2025: 40th Italian Conference on Computational Logic, June 25–27, 2025, Alghero, Italy

[*] Corresponding author.

andrea.formisano@uniud.it (A. Formisano); isaccogavazzi@me.com (I. Gavazzi); eomodeo@units.it (E. G. Omodeo)

https://users.dimi.uniud.it/~andrea.formisano/ (A. Formisano); https://sites.units.it/eomodeo/index.html/ (E. G. Omodeo)

0000-0002-6755-9314 (A. Formisano); 0009-0009-9086-5828 (I. Gavazzi); 0000-0003-3917-1942 (E. G. Omodeo)

by the manner in which Merlin Carl and Boris Z. Moroz [6] treated the Gödel-Bernays class theory (here referred to as NBG, after the initials of von Neumann, Bernays, and Gödel) as formalized in first-order predicate calculus (see [7, Chapter 4]).

This paper presents an emulation, by the authors, of the work of Carl and Moroz. However, instead of using first-order logic, the formalism underlying the axiomatization of NBG adopts a modernized version of Ernst Schröder's algebra of (dyadic) relations, specifically the equational logic $\mathcal{L}^{\times}$, extensively discussed by Alfred Tarski and Steven Givant in [8]. Furthermore, the axioms of the theory have been replaced by an alternative axiomatization, proposed by Harvey Friedmann in [9]. These changes have streamlined the complexity of the Diophantine representation of NBG's provability, even though the new formalization remains equivalent to more classical ones.

While only a glimpse of the novel axiomatization of NBG based on $\mathcal{L}^{\times}$ is offered, the article reports on the initial stages of experimentation with these axioms, assisted by the theorem prover Vampire (cf. https://vprover.github.io/).

2. Polynomial of a Theory Specified in a Formal System

We begin by stating our goal in general terms. Our goal is to encode a *formalized theory* using Diophantine equations. The theory is based on a symbolic language and consists of the following components:

1. A finite number of *logical* axiom schemata.

2. A finite number of *derivation rules*, each applying to at most two premises.

3. A finite set of *proper* axiom schemata.

Together with the language, the first two components define the underlying logical *calculus*, while the third specifies the theory itself.

Let $\mathfrak{F}$ be the set of all statements of the formal language, and let $\mathsf{Th} \subseteq \mathfrak{F}$ be the set of provable theorems of the theory. We assume the availability of an effective bijection $\mathcal{N} : \mathfrak{F} \to \mathbb{N}$ that assigns a unique natural number to each statement.

By the Davis-Putnam-Robinson-Matiyasevich theorem, every recursively enumerable set is Diophantine. Since Th is recursively enumerable, there exists a Diophantine polynomial $D \coloneqq D(a; x_1, \dots, x_M)$ such that the equation $D = 0$ has solutions in the set $\mathbb{N}$ of natural numbers if and only if the parameter a belongs to $\mathcal{N}[\mathsf{Th}]$. Our objective is to explicitly construct such a polynomial D.

Although general techniques exist for this purpose, our construction will provide deeper insight into the number-theoretic devices underlying the Diophantine representation of Th.

We proceed with the following subtasks:[1]

- Constructing a Diophantine polynomial $f_{AXl} \in \mathbb{Z}[a; \vec{x_1}]$, where $\vec{x_1} = (x_1, \dots, x_{k_1})$, that admits solutions in $\mathbb{N}^{k_1}$ if and only if a is the number corresponding to one of the logical axioms.

- Constructing a Diophantine polynomial $f_{der} \in \mathbb{Z}[a, b, c; \vec{x_2}]$, where $\vec{x_2} = (x_1, \dots, x_{k_2})$, that admits solutions in $\mathbb{N}^{k_2}$ if and only if $\mathcal{N}^{-1}(a)$ is obtainable from $\mathcal{N}^{-1}(b)$ and $\mathcal{N}^{-1}(c)$ by means of one of the derivation rules.

- Constructing a Diophantine polynomial $f_{AXp} \in \mathbb{Z}[a; \vec{x_3}]$, where $\vec{x_3} = (x_1, \dots, x_{k_3})$, that admits solutions in $\mathbb{N}^{k_3}$ if and only if a is the number corresponding to one of the adopted proper axioms.

We will ensure that these three polynomials take only nonnegative integer values. This does not restrict generality, as the property or relation over $\mathbb{N}$ represented by a Diophantine parametric polynomial remains unchanged when the polynomial is squared. To smooth the presentation, we also impose that

[1] For clarity, when representing a polynomial, we sometimes separate variables using ';' to distinguish those that act as parameters from those that are viewed (even if only implicitly) as existentially bounded variables.

$k_1 = k_2 = k_3$, and denote this common value as k: in fact, we can multiply any Diophantine polynomial not involving a variable x_i by the monomial $x_i + 1$, without affecting the relation it represents.

A *proof* is a nonempty list of statements each of which is either an axiom or is derived, thanks to a derivation rule, from statements which precede it in the list. We can hence say:

$$\alpha \in \mathsf{Th} \iff (\exists\, n \in \mathbb{N})\ (\exists\, T_0, T_1, \ldots, T_n \in \mathfrak{F}) \text{ such that}$$

- $T_n = \alpha$ and
- for each $h \leqslant n$, one of the the following holds:
  - T_h is a logical axiom, i.e., there exists $\vec{x} \in \mathbb{N}^k$ such that $f_{AXl}\big(\mathcal{N}(T_h), \vec{x}\big) = 0$;
  - there exist $i, j < h$ and $\vec{x} \in \mathbb{N}^k$ such that T_h is derivable in a single step from T_i and T_j , i.e.,

    $$f_{der}\big(\mathcal{N}(T_h), \mathcal{N}(T_i), \mathcal{N}(T_j), \vec{x}\big) = 0;$$

  - T_h is a proper axiom, i.e., there exists $\vec{x} \in \mathbb{N}^k$ such that $f_{AXp}\big(\mathcal{N}(T_h), \vec{x}\big) = 0$.

We can summarize this via the following

Proposition 1. Define the *demonstrative polynomial* of the theory as:

$$f_{\mathcal{D}}(a, b, c; \vec{x}) \quad \coloneqq \quad f_{AXl}(a; \vec{x}) \cdot f_{AXp}(a; \vec{x}) \cdot f_{der}(a, b, c; \vec{x})\,.$$

Let Th be the set of all theorems of our theory. Then

$$\mathcal{N}[\mathsf{Th}] \quad = \quad \Big\{ a \in \mathbb{N} \mid (\exists\, n,\, t_0, t_1, \ldots, t_n \in \mathbb{N})\ (\forall\, h \leqslant n)\ (\exists\, i, j, i', j' \in \mathbb{N})\ (\exists\, \vec{x} \in \mathbb{N}^k)\ \Big(0 \ = \ f_{\mathcal{D}}(t_h, t_i, t_j, \vec{x}) + (h + i + j) \cdot \big((i + i' + 1 - h)^2 + (j + j' + 1 - h)^2\big) + (t_n - a)^2\Big) \Big\}.$$

Each of the three polynomials composing $f_{\mathcal{D}}$ represents an alternative condition: $f_{AXl}(a, \vec{x}) = 0$ implies that a encodes a logical axiom; $f_{AXp}(a, \vec{x}) = 0$ implies that a encodes a proper axiom; and $f_{der}(a, b, c, \vec{x}) = 0$ implies that $\mathcal{N}(a)$ is directly obtainable from $\mathcal{N}(b)$ and $\mathcal{N}(c)$ via a derivation rule. Since we are interested in the locus of zeros, multiplying these polynomials together imposes that at least one of the conditions must hold. Similarly, we often sum squares of polynomials to enforce that multiple conditions are jointly satisfied. For example, $(i + i' + 1 - h)^2 + (j + j' + 1 - h)^2$ vanishes only when $i < h$ and $j < h$; $h + i + j$ vanishes only if $h = 0$, in which case we want $i = j = 0$; and $(t_n - a)^2$ vanishes precisely when the final statement t_n coincides with the theorem a we are checking for.

Remark 1. Note that when $h = i = j = 0$, then $t_h = t_i = t_j$. In this case, t_0 is typically an axiom, since in most formal systems no derivation rule allows deriving a statement from itself. In the calculus $\mathcal{L}^\times$ to be discussed later, this situation may arise but poses no problem: it leads to having t_0 of the form $A = A$, which is a valid scheme. ⊣

We can encode a finite-length list of natural numbers using two numbers, ℓ and c, via the Chinese Remainder Theorem (see, e.g., [4, pp. 200–201]), as embedded in a technique due to [10]. This is formalized in the following lemma, which is well introduced in [11]:

Lemma 1. Let $(a_0, a_1, \ldots, a_n)$ be a tuple whose components a_h belong to $\mathbb{N}$. Then there exist $\ell, c \in \mathbb{N}$ such that, for each h, the component a_h can be retrieved via the rule:

$$a_h \equiv \ell \mod 1 + c \cdot (h + 1) \quad \text{and} \quad a_h < 1 + c \cdot (h + 1)\,,$$

i.e.,

$$(\exists\, q \in \mathbb{N})\big[\,(\ell - a_h) = (1 + c \cdot (h + 1)) \cdot q \ \,\&\,\ a_h \leqslant c \cdot (h + 1)\,\big]\,.$$

Accordingly, we can rewrite the specification of $\mathcal{N}[\mathsf{Th}]$ as follows:

$$\mathcal{N}[\mathsf{Th}] = \Big\{ u \mid \exists\, n, \ell, c\, \forall\, h \leqslant n\, \exists\, i, j, j', j' \exists t_1, t_2, t_3\, \exists\, \vec{x} \in \mathbb{N}^k\, \exists\, q_1, q_2, q_3, q_4, r_1, \dots, r_4$$
$$\Big(0 \;=\; ((t_1 + r_1 - c(h+1))^2 + (\ell - t_1 - q_1(c(h+1)+1))^2 + (t_2 + r_2 - c(i+1))^2 +$$
$$(\ell - t_2 - q_2(c(i+1)+1))^2 + (t_3 + r_3 - c(j+1))^2 + (\ell - t_3 - q_3(c(j+1)+1))^2 +$$
$$(n + r_4 - c(n+1))^2 + (\ell - u - q_4(c(n+1)+1))^2 +$$
$$f_{\mathcal{D}}(t_1, t_2, t_3, \vec{x}) + (h+i+j)((i+i'+1-h)^2 + (j+j'+1-h)^2)) \Big) \Big\}.$$

This can be considered a valid expression in any theory formulated in a formal language with an arbitrary set of axioms and derivation rules involving at most two premises. To translate such an expression into a purely Diophantine one, we can use various techniques of eliminating the bounded universal quantifier. Here we follow the one from [11]. We will call the polynomial obtained after this elimination the polynomial f_{Th} of the theory.

The number of variables used for the elimination is $(p+1)(m+1) + F + 1$, where

- $m = k + 15$ is the number of existentially quantified variables after the bounded universal quantification (recall $k = \max(k_1, k_2, k_3)$),
- F is the number of variables present in the polynomial that expresses factorial,
- p is the number of variables present in the polynomial that expresses the product $\prod_{w=1}^{y}(1 + bw)$.

The resulting polynomial has the maximum degree among the degree of f_{Th} and the degrees of the polynomials needed to perform the translation of factorial and the product $\prod_{w=1}^{y}(1 + bw)$. All this is immediately deducible by looking at [12, pp. 153–154].

We do not make these constants explicit because they can always be improved through more refined Diophantine formulations. Here we follow the theorems in [12, pp. 144–149], from which $F = 55$ and $p = 115$.

3. Case Study: The Polynomial of NBG, a Class Theory

The goal of this article is to find a polynomial that represents the class theory NBG. To do so, we will express the theory in algebraic (relational) form.

Our work follows the line of preceding work on the same theory, as formulated in first-order predicate calculus by [6].

Operation	[6]-V	Ours-V	[6]-D	Ours-D	[6]-A	Ours-A
Polynomial f_{AXl}	$14,953$	18	$\geqslant 160$	32		
Polynomial f_{der}	2	7	4	10		
Polynomial f_{AXp}	9	0	15	30		
Polynomial $f_{\mathcal{D}}$	$14,976$	18	$\geqslant 179$	72		
Value p					240	115
Value F					118	55
Polynomial f_{Th}	$3,639,528$	4000	$\geqslant 364$	108		

Table 1
Comparison between the complexity of the Diophantine representation of NBG achieved by Carl and Moroz in [6], and the analogous one being discussed in this paper

Table 1 presents a brief summary of the differences in expressive economy between our approach and that of [6]. In that table, we denote by V the number of variables, by D the degree, and by A the other key quantities F, p mentioned at the end of Sec. 2. The number of variables indicated is the number of existential quantifiers that occur after the bounded universal quantifier. As for our work, the previous considerations apply to the numerical relationships among the various components. For the work of [6], this holds only partially due to some technical details.

Let $\deg(D)$ denote the degree of a generic polynomial D. Observe that $\deg(f_{\mathcal{D}}) \leqslant \deg(f_{AXl} \cdot f_{AXp} \cdot f_{der})$. Here, the inequality hints that sometimes, as we will do in the following section, it is possible to combine these three polynomials in a less expensive way than by direct multiplication. This inequality suggests that, as we will demonstrate in the following section, it is sometimes possible to combine these three polynomials more efficiently than by direct multiplication.

We can now proceed to show how to encode logical axioms, proper axioms, and derivation rules.

3.1. Encoding of the equalities of $\mathcal{L}^{\times}$, a historical relational language

We briefly recall the syntax of the relational language, which we denote by $\mathcal{L}^{\times}$. For further details, the reader may consult the standard reference [8].

The alphabet is as follows:

Definition 3.1. The alphabet of $\mathcal{L}^{\times}$ consists of:

- Two identity symbols, one for relations, one for predicates $\{\iota, =\}$
- Two binary operators, union and composition $\{\cup, \circ\}$
- Two unary operators, reflection and complement $\{{}^{\smile}, {}^{-}\}$
- The membership symbol $\{\ \epsilon\ \}$
- Parentheses $\{(,)\}$

Semantically, ϵ is interpreted as a non-empty two-argument relation.

We define, inductively, the formation rules of predicates:

Definition 3.2. The set $\overline{\mathcal{P}}$ of predicates is formed as follows:

- ι, ϵ are predicates,
- If A, B are predicates, then $A \cup B$, $A \circ B$, $A^{\smile}$, $\bar{A}$ are predicates.

However, the ultimate objects of our relational calculus are not predicates but equalities.

Definition 3.3. Let $A, B \in \overline{\mathcal{P}}$. An equality is an expression of the form $A = B$. We denote by $\mathcal{U}$ the set of such equalities.

Hence, for the language $\mathcal{L}^{\times}$, formulas $\mathfrak{F}$ are equalities $\mathcal{U}$.

Since our work concerns exclusively syntactic aspects of the language (in particular, the notion of derivation), there is no need to define the semantic of $\mathcal{L}^{\times}$.

The logical axioms are reported in section 3.2 and the notion of proof in Section 3.4. The formulation of the proper axioms requires constructs that go beyond the scope of this article and will be presented in a different work.

We can proceed to number the formulas of the language. We take this idea from Julia Robinson [13].

First, we give the definition of Cantor's bijection in Diophantine form:

Definition 3.4. We denote by c the Cantor pairing function:

$$\mathsf{c}(i, j) = g \quad \coloneqq \quad 2g = (i + j)(i + j + 1) + 2j$$

The definition of $\mathcal{N}$ proceeds in two steps, the first being inductive:

Definition 3.5. Define inductively a numbering $\mathcal{N}'$ of the formulas $P_0, P_1, \ldots$:

- $P_0 = \ \epsilon$, i.e. $\mathcal{N}'(\ \epsilon\ ) = 0$,

- $P_1 = \iota$,
- $P_{4(g+1)} = P_i \cup P_j$ with $g = \mathsf{c}(i,j)$,
- $P_{4(g+1)+1} = P_i \circ P_j$ with $g = \mathsf{c}(i,j)$,
- $P_{4g+2} = \bar{P}_g$,
- $P_{4g+3} = P_g^{\smile}$.

The map $\mathcal{N} : \mathcal{U} \to \mathbb{N}$ is defined as

$$\mathcal{N}(P_i = P_j) = \mathsf{c}(i,j).$$

We emphasize that among the many possible bijections between $\mathcal{U}$ and $\mathbb{N}$, we have chosen one that allows us to immediately reconstruct the structure of the formula it represents from a given number.

3.2. Diophantine representation of axiomatic relational laws

We present, without delay, the logical axioms:

1. $P \cup Q = Q \cup P$
2. $P \cup (Q \cup R) = (P \cup Q) \cup R$
3. $\overline{\overline{Q \cup P} \cup \overline{\bar{Q} \cup P}} = Q$
4. $P \circ (Q \circ R) = (P \circ Q) \circ R$
5. $(P \cup Q) \circ R = (P \circ R) \cup (Q \circ R)$
6. $P \circ \iota = P$
7. $P^{\smile\smile} = P$
8. $(P \cup Q)^{\smile} = Q^{\smile} \cup P^{\smile}$
9. $(P \circ Q)^{\smile} = Q^{\smile} \circ P^{\smile}$
10. $(P^{\smile} \circ \overline{P \circ Q}) \cup \overline{Q} = \overline{Q}$

These axioms are actually laws, that is, axiom schemata.

We begin constructing the polynomials that represent the logical axioms of our theory. We define the auxiliary variables:

$$\begin{aligned}
&f_{fun}(p,q,r,y_1,\dots,y_5,t_1,\dots,t_9) = z^2(z-1)^2 + \\
&(2y_1 - 2\mathsf{c}(p,q))^2 + (2y_2 - 2\mathsf{c}(q,p))^2 + \\
&(2y_3 - 2\mathsf{c}(q,r))^2 + (2y_4 - 2\mathsf{c}(4(y_1+1)+z, r))^2 + \\
&(2y_5 - 2\mathsf{c}(p, 4(y_3+1)+z))^2 + +(2t_1 - 2\mathsf{c}(4q+2, p))^2 + \\
&(2t_2 - 2\mathsf{c}(4(y_1+1), r))^2 + (2t_3 - 2\mathsf{c}(p,r))^2 + \\
&(2t_4 - 2\mathsf{c}(4(t_3+1)+1, 4(y_3+1)+1))^2 + (2t_5 - 2\mathsf{c}(p,1))^2 + \\
&(2t_6 - 2\mathsf{c}(4p+3, 4(4(y_1+1)+1)+2))^2 + (2t_7 - \mathsf{c}(4(t_6+1)+1, 4q+2))^2 + \\
&(2t_8 - 2\mathsf{c}(16(y_2+1)+2, 16(t_1+1)+2))^2 + (2t_9 - 2\mathsf{c}(4q+3, 4p+3))^2
\end{aligned}$$

and we use these variables in the following polynomials:

$$\begin{aligned}
f_1^* &= 2u - 2\mathsf{c}(4(y_1+1), 4(y_2+1)) \\
f_{2,4}^* &= 2u - 2\mathsf{c}(4(y_4+1)+z, 4(y_5+1)+z) \\
f_3^* &= 2u - 2\mathsf{c}(4t_8+2, q) \\
f_5^* &= 2u - 2\mathsf{c}(4(t_2+1)+1, 4(t_4+1)) \\
f_6^* &= 2u - 2\mathsf{c}(4(t_5+1)+1, p) \\
f_7^* &= 2u - 2\mathsf{c}(4(4p+3)+3, p) \\
f_{8,9}^* &= 2u - 2\mathsf{c}(4(4(y_1+1)+z)+3, 4(t_9+1)+z) \\
f_{10}^* &= 2u - 2\mathsf{c}(4(t_7+1), 4q+2)
\end{aligned}$$

Call $f_\times^*$ the product of these, and define $f_\times = f_{fun} + f_\times^{*2}$. We have $\deg(f_\times^*) = 2 \cdot 8 = 16,\ \deg(f_\times) = (2 \cdot 8) \cdot 2 = 32$.

We can now state the following:

Proposition 2. Let $f_{AXl}(u, \vec{g_1}) = f_{\times}$, with $\vec{g_1} = (p, q, r, y_1, \dots, y_5, t_1, \dots, t_9, z)$. Then, if $U \in \mathcal{U}$ is in one of the logical-axioms schemata, there exists $\vec{g_1} \in \mathbb{N}^{18}$ such that $f_{AXl}(\mathcal{N}(U), \vec{g_1}) = 0$.

Proof. Obvious by construction.

Let us elaborate on the first axiom as an example. y_1 is the pairing of p, q via c, y_2 the pairing of q, p via c. The operation $4(y_1 + 1)$ is precisely that given in the definition of $\mathcal{N}'$ for $\cup$. Therefore, the operation $\mathsf{c}(4(y_1 + 1), 4(y_2 + 1))$ is exactly the operation performed in the definition of $\mathcal{N}$ to represent the equality of two unions with identical operands in reversed order. □

3.3. Diophantine representation of NBG's proper axioms

We must now perform the same operation for the polynomials of the proper axioms of our class theory. We have chosen to use the axioms as formulated in [9]. The choice of this axiomatization depends on the fact that it is simpler to formulate in the relational language than that of [7].

Since there are no axiom schemata, the multi-image of each axiom via $\mathcal{N}$ will be a single number.

Hence, we may refrain from explicitly writing out the individual axioms and thus the polynomial:

Lemma 2. Let $f_{\mathcal{X}} : \mathbb{N} \times \mathbb{Z} \to \mathbb{Z}$ be a polynomial, and $\mathcal{X} \in AXp$. Then

$$\mathcal{N}[\mathcal{X}] = \{u \in \mathbb{N} \mid \exists p \in \mathbb{Z} \text{ s.t. } f_{\mathcal{X}}(u, p) = u - m_{\mathcal{X}} = 0\}$$

with $m_{\mathcal{X}} \in \mathbb{N}$. Furthermore, if we let $f_{AXp} = \prod_{\mathcal{X} \in \mathrm{AXp}} f_{\mathcal{X}}$, then

$$\mathcal{N}[AXp] = \{u \in \mathbb{N} \mid \exists p \in \mathbb{Z} \text{ s.t. } f_{AXp}(u, p) = 0\}.$$

Note that in this lemma, the presence of the variable p is purely accessory.

According to our formulation of the proper axioms, $|AXp| = 15$. Again, we have chosen to remain faithful to a more transparent idea of proof rather than forcing the degree or the number of variables to be as low as possible. Using appropriate operations, we could indeed have created a single 'macroaxiom' to obtain a polynomial f_{AXp} of degree 1 instead of one of degree 30.

Compared to the axiomatization proposed by [9], ours omits one axiom that we discovered unnecessary (the union of two classes) and adds one. It is well-known (see [8]) that the relational calculus is equivalent to first-order predicate calculus with only three variables. This is an extremely important limitation of its expressiveness. It is also known, however, that there is a condition under which this limitation is overcome, providing a calculus with the same expressive power. This condition is the existence of a pair of conjugate quasi-projections, i.e. two functions $\varpi_0,\ \varpi_1$ for which $\varpi_0^{\smile}\varpi_1 = \mathbb{1}$. For some specific $\varpi_0,\ \varpi_1$, this property is our additional axiom. Having clarified this fundamental point, we can proceed by setting $AX = AXp \cup AXl$ and thus combining the obtained results:

Proposition 3. Let

$$f_{AX}(u, \vec{g_1}) = f_{fun} + \Big(f_{\times}^{*} \cdot \prod_{\mathcal{X} \in \mathrm{AXp}} f_{\mathcal{X}}\Big)^2$$

then

$$\mathcal{N}[\mathrm{AX}] = \{u \in \mathbb{N} \mid \exists \vec{g_1} \in \mathbb{N}^{18} \text{ s.t. } f_{\mathrm{AX}}(u, \vec{g_1}) = 0\}$$

and we have $\deg(f_{AX}) = (16 + 15) \cdot 2 = 62$.

Proof. Obvious by construction. □

The polynomial f_{AX} encodes the fact that a demonstration step δ_i is a logical or a proper axiom.

3.4. A Diophantine representation of $\mathcal{L}^{\times}$'s formal derivations

In this section, we codify, in Diophantine form, the notion of derivability in the relational calculus, recalled here:

Definition 3.6. A family Θ of equalities is called a *theory* if it possesses the following closure properties:

0. The logical axioms belong to Θ.
1. When two equalities $B = C$ and $B = D$ belong to Θ, then $C = D$ also belongs to Θ.
2. When B, C, D are predicates and $B = C$ belongs to Θ, the equalities $B \cup D = C \cup D$, $B \circ D = C \circ D$, $\bar{B} = \bar{C}$, and $B^{\smile} = C^{\smile}$ also belong to Θ.

The equalities that form a theory are called its theorems.

Here, we are interested in points 1 and 2.

We must encode the fact that one equality is derived from another (or from two others) by means of these rules.

Lemma 3. Let $B = C$ and $B = G$ be equalities in $\mathcal{U}$.

Given $h_1 \in \mathbb{Z}[u, u', u'', p, q, r]$, then the equality $C = G$ is derived from $B = C$ and $B = G$ by inference rule 1 if and only if

$$\exists p, q, r \ \mid \ h_1(\mathcal{N}(C = G), \mathcal{N}(B = C), \mathcal{N}(B = G), p, q, r) = 0$$

with

$$h_1(u, u', u'', p, q, r) = (2u' - 2\mathsf{c}(p, q))^2 + (2u'' - 2\mathsf{c}(p, r))^2 + (2u - \mathsf{c}(q, r))^2.$$

Let

$$h_i \in \mathbb{Z}[u, u', p, q, r, s, t], \ i = 2, \ldots, 5 \ \text{ and } \ h_i \in \mathbb{Z}[u, u', p, q], \ i = 6, 7,$$

then for each of the four inference schemata of point 2, the following holds:

An equality U with code $u = \mathcal{N}(U)$ is derived by the ith schema from $B = C$ if and only if

$$\exists p, q, r, s, t \ \mid \ h_i(u, \mathcal{N}(B = C), p, q, r, s, t) = 0, \quad i = 2, 3$$

$$\text{or } \ h_i(u, \mathcal{N}(B = C), p, q) = 0, \quad i = 4, 5$$

with h_i defined as follows:

$$\begin{array}{ll}
B \cup D = C \cup D & h_2(u, u', p, q, r, s, t) = (2u' - 2\mathsf{c}(p, q))^2 + \\
 & (2s - 2\mathsf{c}(p, r))^2 + (2t - 2\mathsf{c}(q, r))^2 + (2u - 2\mathsf{c}(4s + 4, 4t + 4))^2 \\
B \circ D = C \circ D & h_3(u, u', p, q, r, s, t) = (2u' - 2\mathsf{c}(p, q))^2 + \\
 & (2s - 2\mathsf{c}(p, r))^2 + (2t - 2\mathsf{c}(q, r))^2 + (2u - 2\mathsf{c}(4s + 5, 4t + 5))^2 \\
B^{\smile} = C^{\smile} & h_4(u, u', p, q) = (2u' - 2\mathsf{c}(p, q))^2 + (2u - 2\mathsf{c}(4p + 3, 4q + 3))^2 \\
\overline{B} = \overline{C} & h_5(u, u', p, q) = (2u' - 2\mathsf{c}(p, q))^2 + (2u - 2\mathsf{c}(4p + 2, 4q + 2))^2
\end{array}$$

Proof. Immediate by the bijectivity of $\mathcal{N}$, $\mathcal{N}'$. □

Taking care to keep variables and degree under control, we can summarize:

Proposition 4. Let

$$f_{der}(u, u', u'', \vec{g_3}) =$$
$$(2u' - 2\mathsf{c}(p, q))^2 + (2s - 2\mathsf{c}(p, r))^2 + (2t - 2\mathsf{c}(q, r))^2 + (z^2 - z)^2 +$$
$$((s - u'')^2 + (t - u)^2)\,(2u - 2\mathsf{c}(4s + 4 + z, 4t + 4 + z))^2 \cdot$$
$$\cdot (2u - 2\mathsf{c}(4p + 2 + z, 4q + 2 + z))^2$$

with $\vec{g_3} = (p, q, r, s, t, z)$. An equality U with code $u = \mathcal{N}(U)$ is derived from the equality $B = C$ (and $B = G$) by the derivation rules if and only if

$$\exists \vec{g_3} \in \mathbb{N}^6 \;\mid\; f_{der}(u, \mathcal{N}(B = C), \mathcal{N}(B = G), \vec{g_3}) = 0$$

and also $\deg(f_{der}) = 2 + 2 \cdot 2 \cdot 2 = 10$.

Since f_{der} and f_{AX} are positive, we simply multiply them to obtain $f_{\mathcal{D}}$, which then has degree $10 + 62 = 72$.

Because we are multiplying, with an appropriate renaming of variables, we can reuse those of the polynomial that has more of them (in our case f_{AX}) in the definition of the other. Hence, we have a total of 18 variables in $f_{\mathcal{D}}$.

4. Vampire-assisted Reasoning

The availability of an equational reformulation of an axiomatic set theory within Tarski-Givant relational calculus offers an interesting approach to the mechanization of reasoning in Set Theory. The approach consists of two steps. The first step requires building a prover for the equational calculus on top of an existing first-order theorem prover. Subsequently, this equational prover will be used to automate equational set-reasoning in the axiomatic theory.

The feasibility of this path has been explored in [14, 15], where the authors propose an equational re-engineering of Zermelo-Skolem-Fraenkel axiomatic system ZF and show how the first-order theorem prover Otter can serve as an inference engine for ZF.

In this section, we outline a similar approach for the case of NBG based on the state-of-the-art theorem prover Vampire.

4.1. Reasoning in the $\mathcal{L}^{\times}$ calculus

The key to enable a first-order theorem prover to perform deductions in $\mathcal{L}^{\times}$ is to consider relational equalities (e.g., the logical axioms of Section 3.2) as universally closed first-order sentences, where the predicates (namely, P, Q, R) play the role of first-order variables.

We implemented this idea by developing a hierarchy of layers on top of a core group of first-order sentences reflecting the logical axioms of $\mathcal{L}^{\times}$.

Each level extends the syntax of calculus by introducing new constructs derived from the constructs of the levels below. Then, Vampire is used to prove, starting from definitions and laws proved at lower levels, a set of laws that characterize the new constructs. For example, at the bottom level Vampire easily proved a rich collection of lemmas on the primitive operators, namely, union ($\cup$), composition ($\circ$), complementation ($^{-}$), and inversion ($^{\smile}$). At the next level we introduced the relational constants $\emptyset$, $\mathbb{1}$ and the constructs of intersection ($P \cap Q := \overline{\overline{P} \cup \overline{Q}}$), difference ($P \setminus Q := \overline{Q \cup \overline{P}}$), and Peircean sum ($P \dagger Q := \overline{\overline{P} \circ \overline{Q}}$). Vampire quickly proved several laws involving these new constructs.

We recall below only some examples of the constructs introduced, and laws demonstrated, in the subsequent levels of the hierarchy.

Inclusion. A possible definition for the notion of inclusion of relations is:

$$P \subseteq Q := Q \cup \overline{P} = \mathbb{1}.$$

Among the laws proved in this layer we mention, monotonicity and transitivity of inclusion, the so-called *cycle laws* and Dedekind law [16].

Functionality. The main derived constructs in this layer are a selector of the functional part of a relation:

$$\mathsf{fncPart}\,(P) := P \setminus (P \circ \bar{\iota})$$

and a shorthand for functionality condition:

$$\mathtt{Fnc}(P) \coloneqq P^{\smile} \circ P \;\subseteq\; \iota.$$

Among the laws proved in this level there are:

$$\begin{aligned}
&\mathsf{fncPart}\,(P)^{\smile} \circ \mathsf{fncPart}\,(P) \subseteq \iota, \\
&\mathtt{Fnc}(P) \wedge \mathtt{Fnc}(Q) \;\rightarrow\; \mathtt{Fnc}(P \circ Q)\,, \\
&\mathtt{Fnc}(P) \;\rightarrow\; P \circ (Q \cap R) = ((P \circ Q) \cap (P \circ R)).
\end{aligned}$$

Totality. This layer introduces and a shorthand for totality of relations:

$$\mathsf{Total}(P) \coloneqq P \circ \mathbb{1} \;=\; \mathbb{1}.$$

Among the related laws Vampire easily proved the implications:

$$\begin{aligned}
&\mathsf{Total}(P) \wedge \mathsf{Total}(Q) \;\rightarrow\; \mathsf{Total}(P \circ Q)\,, \qquad && \mathsf{Total}(\iota)\,, \\
&\mathsf{Total}(P \circ Q) \;\rightarrow\; \mathsf{Total}(P)\,, && P \cap P^{\smile} = \varnothing \;\rightarrow\; \mathsf{Total}\big(\overline{P}\big)\,.
\end{aligned}$$

By developing the entire hierarchy of levels, Vampire managed to prove several hundreds laws, in most cases taking fractions of a second and never going beyond a few minutes for the most difficult proofs.

4.2. Benchmarks for assisted reasoning in the equational formalization of NBG

At the top of the hierarchy described earlier, after specifying the (equational rendering of the) proper axioms of the theory of interest, one can exploit Vampire to obtain proofs of theory-specific theorems.

As mentioned in the previous section, the proof framework we are developing has achieved good results in proving several theorems of relational calculus.

Extending the framework to support automated theorem-proving in NBG involves the addition of layers that introduce set-theoretic notions and include equational re-formulations of the proper axioms of NBG. While the relational translation of the axiomatic system proposed by Harvey Friedmann in [9] has been largely completed, its application to the proof of non-trivial theorems remains a work in progress.

The system was preliminarily tested by obtaining some apparently simple proofs. For example, Vampire quickly obtained a proof of the equivalence of different formulations of the *Extensionality* axiom, or that from the *Infinity* axiom the existence of a set immediately follows (namely, that $\mathbb{1} \circ \; \epsilon \; \circ \mathbb{1} = \mathbb{1}$ holds).

As future work, we intend to validate the approach based on the equational formulation of NBG and powered by the theorem prover Vampire by tackling some harder problems of increasing difficulty. The goals that will be the first object of this activity include automated proofs of the following claims:

- An empty class exists (our formulation of NBG does not explicitly include the emptyset axiom)
- For any given set x there exists a class whose sole element is x
- Any class that is a singleton is a set
- Any class that has exactly two elements is a set
- There exists a universal class

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] S. C. Kleene, Introduction to Metamathematics, North-Holland, 1952. 550 pp., reprinted Ishi Press, 2009.

[2] M. Davis, H. Putnam, J. Robinson, The decision problem for exponential Diophantine equations, Ann. of Math., Second Series 74 (1961) 425–436.

[3] J. V. Matijasevič, Enumerable sets are Diophantine, Soviet Mathematics. Doklady 11 (1970) 354–358. (Translated from [17]).

[4] Y. V. Matiyasevich, Hilbert's tenth problem, The MIT Press, Cambridge (MA) and London, 1993. Translated from [18].

[5] J. P. Jones, Universal Diophantine equation, The Journal of Symbolic Logic 47 (1982) 549–571.

[6] M. Carl, B. Z. Moroz, On a diophantine representation of the predicate of provability, Journal of Mathematical Sciences 199 (2014) 36–52. URL: https://api.semanticscholar.org/CorpusID:34618563.

[7] E. Mendelson, Introduction to Mathematical Logic, 4^{th} ed., Chapman & Hall, 1997.

[8] A. Tarski, S. Givant, A formalization of Set Theory without variables, volume 41 of *Colloquium Publications*, American Mathematical Society, 1987.

[9] H. M. Friedman, Simplified axioms for class theory, 2020. https://bpb-us-w2.wpmucdn.com/u.osu.edu/dist/1/1952/files/2020/09/NBGAxioms091520.pdf.

[10] K. Gödel, Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I, Monatsh. Math. und Physik 38 (1931) 173–198. "On formally undecidable propositions of Principia Mathematica and related systems I" in Solomon Feferman, ed., 1986. Kurt Gödel Collected works, Vol. I. Oxford University Press: 144-195.

[11] M. Davis, Hilbert's tenth problem is unsolvable, Amer. Math. Monthly 80 (1973) 233–269. Reprinted with corrections in the Dover edition of *Computability and Unsolvability* [19, pp. 199–235].

[12] M. R. Murty, B. Fodden, Hilbert's tenth problem. An Introduction to Logic, Number Theory, and Computability, volume 88 of *Student mathematical library*, American Mathematical Society, Providence, RI, 2019.

[13] J. Robinson, Diophantine decision problems, in: W. J. LeVeque (Ed.), Studies in Number Theory, volume 6 of *Studies in Mathematics*, Mathematical Association of America, 1969, pp. 76–116.

[14] A. Formisano, E. G. Omodeo, An equational re-engineering of set theories, in: R. Caferra, G. Salzer (Eds.), Automated Deduction in Classical and Non-Classical Logics, Selected Papers, volume 1761 of *Lecture Notes in Computer Science*, Springer, 1998, pp. 175–190. URL: https://doi.org/10.1007/3-540-46508-1_12. doi:10.1007/3-540-46508-1_12.

[15] A. Formisano, E. G. Omodeo, M. Temperini, Layered map reasoning: An experimental approach put to trial on sets, in: A. Dovier, M. C. Meo, A. Omicini (Eds.), Declarative Programming - Selected Papers from AGP 2000, volume 48 of *ENTCS*, Elsevier, 2001, pp. 1–28. doi:10.1016/S1571-0661(04)00147-1.

[16] G. Schmidt, T. Ströhlein, Relations and Graphs, Discrete Mathematics for Computer Scientists, EATCS-Monographs on Theoretical Computer Science, Springer-Verlag, 1993.

[17] Y. V. Matiyasevich, Diofantovost' perechislimykh mnozhestv, Doklady Akademii Nauk SSSR 191 (1970) 279–282. (Russian. Available in English translation as [3]; translation reprinted in [20, pp. 269–273]).

[18] Y. V. Matiyasevich, Desyataya Problema Gilberta, Fizmatlit, Moscow, 1993. Several translation available, as indicated at URL: http://logic.pdmi.ras.ru/~yumat/H10Pbook/.

[19] M. Davis, Computability and Unsolvability, McGraw-Hill, New York, 1958. Reprinted with an additional appendix, Dover 1983.

[20] G. E. Sacks (Ed.), Mathematical Logic in the 20th Century, Singapore University Press, Singapore; World Scientific Publishing Co., Inc., River Edge, NJ, 2003.