Panu Raatikainen

THE PROBLEM OF THE SIMPLEST DIOPHANTINE REPRESENTATION

1. Introduction

Gregory Chaitin's information-theoretic incompleteness result (Chaitin 1974a,b) has received extraordinary attention; it is apparently one of the most widely known recent logical results.[1] Roughly, it says that for every formalized theory there is a finite constant c such that the theory in question cannot prove any particular number to have a Kolmogorov complexity larger than c, even though there are infinitely many numbers for which this is true.

The standard interpretation of Chaitin's theorem claims that the value of the limiting constant is determined by the complexity of the theory itself, which is assumed to be a good measure of the strength of the theory. In another paper (Raatikainen 1998) I have argued that this received view is simply false. I showed that the limiting constant does not in any way reflect the power of a formalized theory, but that the values of these constants actually depend on the chosen coding of Turing machines, and are thus quite accidental. As a consequence of my close analysis, I could also provide a simple, almost trivial, proof of Chaitin's Theorem, given the standard undecidability result concerning the Halting problem (Turing 1936–1937).

After these negative observations the question occurred to me whether one could do any better. And the answer turns out to be positive. In this paper I give a strengthened form of Matiyasevich's important result that Hilbert's tenth problem is unsolvable (Matiyasevich 1970). My result stands to this result in an analogous simple relation that Chaitin's result is to the undecidability of the Halting problem, and is every bit as strong as Chaitin's theorem. The setting used here

[1] For some further discussion of this matter, see Raatikainen 1998.

Nordic Journal of Philosophical Logic, Vol. 2, No. 2, pp. 47–54.

appears to be especially simple and natural. The problem considered is a fairly straightforward mathematical one, and the limiting constants that my approach provides do not depend on any coding but are "intrinsic" to the formalized theory in question and in a sense "absolute"; however, I do not intend to make any strong philosophical claims, resembling the standard interpretation of Chaitin's Theorem, about these constants. I conclude by showing how my approach exhibits an interesting difference between intuitionistic and classical arithmetical theories.

The problem that I shall consider is the one of finding for a given finite set of numbers the simplest "Diophantine representation"[2] (a notion I define below). I shall show that this problem is not only undecidable but even undecidable in a certain quite strong sense; viz. after a finite level of complexity, it turns out to be, in a sense, completely undecidable.

2. Diophantine Sets and Hilbert's Tenth Problem

Let us first review the basic concepts and results related to the subject of Diophantine equations (cf. Davis 1973, Smorynski 1991, Matiyasevich 1993).

First, note that traditionally both positive and negative integers have been allowed as solutions, and as coefficients. The modern approach, however, concentrates more on the natural number coefficients and solutions. But the difference is logically inessential. One can get rid of the negative coefficients by transforming a Diophantine equation of the form $P(\vec{x}) = 0$ to the form $P'(\vec{x}) = P''(\vec{x})$. Moreover, there are well-known techniques for reducing the decision problem of the integer case to the non-negative one, and *vice versa* (see e.g. Davis 1973, Smorynski 1991, Matiyasevich 1993). In what follows, I shall therefore be somewhat indifferent between these two cases; everything that I say below applies equally to both theories of integers and theories of natural numbers.

Accordingly, I shall use $P(x_1, \ldots, x_n)$ ambiguously for both $P(x_1, \ldots, x_n) = 0$ and $P'(x_1, \ldots, x_n) = P''(x_1, \ldots, x_n)$, with either integer or positive number coefficients, depending on the formalized theory in question.

Moreover, traditionally, one is given an equation and asked for its solutions. However, more recently it has turned out to be fruitful to invert the problem, i.e. begin with a set of "solutions" and attempt

[2] One might naturally have called the complexity of such maximally simple Diophantine equation the *Diophantine complexity* of the set S; however, Matiyasevich (1993, ch. 8) has already started to use this label for quite another issue.

to find a corresponding equation. I shall also follow this "inverted approach" here. More precisely:

Definition 1. *An equivalence of the form*

$$a \in S \Leftrightarrow \exists x_1, \ldots, x_n[P(a, x_1, \ldots, x_n)],$$

(where $P(x_0, x_1, \ldots, x_n)$ is a Diophantine equation) is called a Diophantine representation of the set S. A set that has a Diophantine representation is called Diophantine.

(In this paper, I consider solely *sets* of numbers; however, it is obvious how to generalize everything presented here for arbitrary n-tuples and relations.)

The epoch-making work of Yuri Matiyasevich (1970) based on earlier work by Julia Robinson, Martin Davis and Hilary Putnam (for history, see Davis 1973, Matiyasevich 1993) established the following results:

Theorem 1. *A set is Diophantine, i.e. has a Diophantine representation, iff it is recursively enumerable.*

Theorem 2. *Hilbert's tenth problem is unsolvable: there is no algorithm for testing Diophantine equations for possession of solutions.*

Theorem 3. *Corresponding to any given axiomatization of number theory there is a Diophantine equation which has no solutions, but such that this fact cannot be proved within the given axiomatization.*

3. The Problem of Simplest Diophantine Representation

Let me now turn to the proper subject of this paper.

To begin with, I assume that a formalized language of arithmetic $\mathcal{L}$, that has a *finite* stock of basic symbols, has been fixed. Obviously, this is assumed to include the standard logical symbols, a constant symbol (e.g. '$\bar{0}$') for 0, the successor symbol (e.g. 'S' or '$'$'), and two function symbols (e.g. '$\times$' and '$+$') for addition and multiplication.

Next, I take the *complexity*, or *simplicity*, of a Diophantine equation to be the number of basic symbols occurring in it.[3] Now recall that

[3] There are, of course, alternative possibilities, but note that for my purposes here the degree of equation would not be suitable, because every Diophantine set has degree ≤ 4 (Skolem 1934); whatever measure is chosen, it is essential that it is not bounded. It is apparently necessary to take the size of the coefficients into account; for it is possible to reduce the degree of an equation by, so to say, coding more and more information to the coefficients.

the modern "inverted" approach to the subject begins with a set of "solutions" and attempts to find a corresponding equation. Now it is indeed a very short and natural step to add that given a set of "solutions" one would like to find a maximally simple equation. And this will be our problem. To make it exactly defined, let us formulate it as follows:

"Given a finite set of numbers S, what is the *simplest* (in terms of the number of basic symbols it contains) Diophantine equation $P(x_0, x_1, \ldots, x_n)$, such that $a \in S \Leftrightarrow \exists x_1, \ldots, x_n[P(a, x_1, \ldots, x_n)]$, i.e. $P(x_0, x_1, \ldots, x_n)$ provides a Diophantine representation of the set S ?"

Obviously, because of Theorem 1, every finite set has a Diophantine representation; moreover, among Diophantine equations, there must be a minimal complexity such that there is an equation with this complexity that represents a given set, and that no simpler equation does. Of course, a set may have more than one equally simple Diophantine representation; nevertheless, there may always be only finitely many such equations. We may agree that in such a case any one of the simplest equations will do; or, alternatively, we may further define an "alphabetical" ordering of the basic symbols, and agree that given a set of equations of the same complexity, by "the simplest" one means the first equation in the alphabetical order. However, such fine details do not really matter in what follows.

I shall now show how the problem of the simplest Diophantine representation behaves logically.

Let us assume that we have fixed, in the language $\mathcal{L}$, a recursively axiomatizable theory $\mathcal{T}$. Imagine then that one tries to proceed as follows. With a given set of numbers S, one tries to test Diophantine equations in their order of size, beginning from the simplest, whether they provide a Diophantine representation of S or not. As long as it is possible to determine such facts in $\mathcal{T}$, it is possible to apply this method successfully.

However, it follows from the above-mentioned results of Matiyasevich that in any formal system of arithmetic $\mathcal{T}$ one will eventually meet an equation P^* such that P^* does not provide a Diophantine representation of any set S (i.e. has no solutions), but one cannot prove this fact in $\mathcal{T}$. Let the complexity of the simplest such equation P^* in our chosen theory $\mathcal{T}$ be c.

Now assume that S is any finite set such that the complexity of the Diophantine equation P that is in fact the simplest one that provides a Diophantine representation of S is greater than c. Then it is impossible to determine, in the fixed theory $\mathcal{T}$, what the complexity of the simplest such equation is. For, one should be able to prove in $\mathcal{T}$ both that the equation P, that in fact is the simplest equation providing a Diophantine representation of S, really represents S, and that no equation simpler than P is such. But it is not possible to prove in $\mathcal{T}$ that P^*, which is simpler than P, is not such an equation (although, actually it is not).

Note, moreover, that there are only finitely many finite sets that have a Diophantine representation by an equation having complexity less than c, and that the above phenomena hold for all other ("for almost all", as one often says instead of "all but finitely many") finite sets. That is:

Theorem 4. *Corresponding to any axiomatization of number theory there is a finite constant c, such that one cannot, in that formal system, determine for any finite set S the minimal Diophantine equation that provides a Diophantine representation of S, if the complexity of such equation is larger than c.*

Discussion. As noted in the introduction, one can now readily see that, the limiting constant obtained by my above setting is not in any way dependent on any arbitrary coding, or Gödel numbering. Moreover, although it is relative to the fixed formal language, its relativity is fairly modest, because I have used as my mean of representation Diophantine equations whose form is, by definition, quite invariant. On the other hand, it may still happen, as was the case with Chaitin's theorem (see Raatikainen 1998), that theories with considerably different strength have the same limiting constant. This, of course, makes it impossible to use any such constants as a measure of the strength of formalized theories.

4. On Classical and Intuitionistic Theories

The present approach reveals an interesting difference between classical and intuitionistic theories. Namely, the simple fact that, for any natural number n, there exists a finite set S (in fact, infinitely many sets) such that the simplest equation providing a Diophantine representation of S is more complex than n, *can easily be proved* in most classical theories of arithmetic, e.g. in PA (although not, understandably, in Q or PRA); however, it follows from the above unprovability result that it is impossible to prove this simple fact in any standard intuitionistic theory; more exactly, in any theory having the property of *explicit definability for numbers* (EDN). I shall exemplify this phenomenon with Heyting Arithmetic HA.

I abbreviate the relation "the minimal Diophantine equation representing the set x has the complexity y" as "$d(x) = y$". Also, I shall write "$d(x) > y$" for "$d(x) = z \wedge z > y$". These can readily be seen to be Σ^0_2 relations. The fact that I am interested in here has the form $\forall x \exists y(d(y) > x)$, and is hence a Π^0_3 sentence. As one can prove it in PA, one can also, by ∀E, prove $\exists y(d(y) > \bar{n})$, for any n, in PA. "$\exists y(d(y) > \bar{n})$" is again a Σ^0_2 sentence. I claim that this cannot, in general (i.e. for all n), be proved in HA, or any standard intuitionistic theory.

For assume that we could prove $\forall x \exists y(d(y) > x)$ in HA. Then we could, by ∀E, prove $\exists y(d(y) > \bar{n})$, even for some n larger than c (for HA) in Theorem 4. But by the property EDN (i.e. HA $\vdash \exists x A(x) \Rightarrow$ HA $\vdash A(\bar{n})$, for some numeral $\bar{n}$), we could then prove $(d(\bar{m}) > \bar{n})$, for some numeral $\bar{m}$. But this we have seen to be impossible, by Theorem 4. Hence we have shown:

Theorem 5. *$\exists y(d(y) > \bar{n})$ is provable, for any n, in* PA*, but not in* HA.

As noted above, the same unprovability phenomenon occurs in various other intuitionistic arithmetical theories. In fact, in their up-todate authoritative survey of intuitionism, Troelstra and van Dalen state that *all* well-known intuitionistic formalisms containing arithmetic have the property of explicit definability for numbers (Troelstra and van Dalen 1988, vol. I, p. 139; cf. Vol II 10.5.3–5, Troelstra 1973, 1.11.2 (p. 91 ff.)). Accordingly, it is impossible to prove the above-mentioned fact in any such theory.

Note, on the other hand, that PA is conservative over HA for all Π^0_2 sentences. Gödel (1933) established the conservativity for negative arithmetic sentences (which are either atomic or in their build-up use only the logical connectives $\rightarrow, \wedge, \forall$), and Kreisel (1958) extended it to Π^0_2 sentences. Finally, Friedman (1978) gave a uniform method for establishing the conservativeness of various classical theories over their intuitionistic counterparts for Π^0_2 sentences (cf. Leivant 1985, Troelstra and van Dalen 1988).

Hence we have here a sentence with the minimal quantificational complexity in terms of arithmetical hierarchy for which this is possible (i.e. Σ^0_2) that is classically but not intuitionistically provable. Now it is, of course, well known that classical theories are *not* conservative over their intuitionistic counterparts for the class of Σ^0_2 sentences. Nevertheless, we have here a concrete and, I think, natural arithmetic fact, constructed not by using some arithmetized metamathematical concepts, self-reference and paradoxes,[4] and not by using some strong, e.g. impredicative, set existence principles, that is unprovable in all well-known intuitionistic theories.

Note, on the other hand, that the limiting constant of a formalized arithmetical theory is the *same* whether it uses intuitionistic or classical logic. This is because its value is determined by certain unprovable Π^0_1 sentence, which is, by the above conservativity property, common for them. However, the *truth* of the infinitely many unprovable sentences (e.g. "$d(\bar{m}) = \bar{n}$", for any $n > c$) obtained here makes sense only in the classical case.

Department of Philosophy
University of Helsinki, Finland

References

Chaitin, Gregory J. 1974a. Information-theoretic computational complexity. *IEEE Transactions on Information Theory IT-20*, pp. 10–15.

Chaitin, Gregory J. 1974b. Information-theoretic limitations of formal systems. *Journal of the ACM*, vol. 21, pp. 403–424.

Davis, Martin. 1973. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, vol. 80, no. 3, pp. 233–269.

Friedman, Harvey. 1978. Classically and intuitionistically provably recursive functions. In Müller and Scott (eds.), *Higher Set Theory, Lecture Notes in Mathematics 669*, pp. 21–27. Springer-Verlag, Berlin.

Gödel, Kurt. 1933. Zur intuitionistischen Arithmetik und Zahlentheorie. In *Ergebnisse eines mathematischen Kolloquiums,* Heft 4, pp. 34–38.

Kreisel, Georg. 1958. Mathematical significance of consistency proofs. *Journal of Symbolic Logic 23*, pp. 155–182.

Leivant, Daniel. 1985. Syntactic translations and provably recursive functions. *Journal of Symbolic Logic*, vol. 50, pp. 682–688.

[4] Strictly speaking, one has to grant that the complexity of a Diophantine equation *is* a metamathematical property; still, I would argue that it is a fairly harmless and elementary one, compared to, say, the notions of provability and consistency, which are more often used for such unprovability results.

Matiyasevich, Yuri V. 1970. Diofantovost' perechislimykh mnozhestv. *Doklady Akademii Nauk SSSR*, vol. 191, no. 2, pp. 297–282 (Russian). (English translation, Enumerable sets are Diophantine, *Soviet Mathematics Doklady*, vol. 11, no. 2, pp. 354–358).

Matiyasevich, Yuri V. 1993. *Hilbert's Tenth Problem.* M.I.T. Press, Cambridge, Mass.

Raatikainen, Panu. 1998. On interpreting Chaitin's incompleteness theorem. *Journal of Philosophical Logic.* Forthcoming.

Skolem, Thoralf. 1934. Über die Nicht-charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschließlich Zahlenvariablen. *Fundamenta mathematicae*, vol. 23, pp. 150–161.

Smorynski, Craig. 1991. *Logical Number Theory I.* Springer-Verlag, Berlin.

Troelstra, Anne S. 1973. *Metamathematical Investigations of Intuitionistic Arithmetic and Analysis.* Springer-Verlag, Berlin.

Troelstra, Anne S. and van Dalen, Dirk. 1988. *Constructivism in Mathematics: An Introduction*, vol. I–II. North Holland, Amsterdam.

Turing, Alan M. 1936–1937. On computable numbers, with an application to the Entscheidungsproblem. In *Proceedings of the London Mathematical Society,* ser. 2, vol. 42, pp. 230–265. Correction, ibid. 43, pp. 544–546.