THE JOURNAL OF SYMBOLIC LOGIC
Volume 68, Number 1, March 2003

SOME STRONGLY UNDECIDABLE NATURAL ARITHMETICAL PROBLEMS, WITH AN APPLICATION TO INTUITIONISTIC THEORIES

PANU RAATIKAINEN

§1. Introduction. Although Church and Turing presented their path-breaking undecidability results immediately after their explication of effective decidability in 1936, it has been generally felt that these results do not have any direct bearing on ordinary mathematics but only contribute to logic, metamathematics and the theory of computability. Therefore it was such a celebrated achievement when Yuri Matiyasevich in 1970 demonstrated that the problem of the solvability of Diophantine equations is undecidable. His work was building essentially on the earlier work by Julia Robinson, Martin Davis and Hilary Putnam (1961), who had showed that the problem of solvability of exponential Diophantine equations is undecidable. One should note, however, that although it was only Matiyasevich's result which finally solved Hilbert's tenth problem, already the earlier result had provided a perfectly natural problem of ordinary number theory which is undecidable.[1]

Nevertheless, both the set of Diophantine equations with solutions and the set of exponential Diophantine equations with solutions are still semi-decidable, that is, recursively enumerable (i.e., Σ_1^0); if an equation in fact has a solution, this can be eventually verified. More generally, they are — as are their complements, the sets of equations with no solutions, which are Π_1^0 — also Trial and Error decidable (Putnam [1965]), or decidable in the limit (Shoenfield [1959]), for every Δ_2^0 set is (and conversely). This last-mentioned natural "liberalized" notion of decidability has begun more recently to play an essential role e.g., in so-called Formal Learning Theory (see e.g., Osherson, Stob, and Weinstein [1986], Kelly [1996]).[2]

Later, the researchers in Diophantine decision problems have studied various problems related to the cardinality of solutions (see Davis [1972], Davis, Putnam, and Robinson [1976], Smoryński [1977]; cf. Davis [1973], [1977], Matiyasevich [1993], Smoryński [1991]). But to date the strongest results explicitly presented in

Received November 26, 2001; accepted August 20, 2002.

[1] It should be added that these were not the first problems from ordinary mathematics which were shown to be undecidable. There were, for example, various problems related to the theory of groups which had been shown to be undecidable already earlier. For a good overview, see Davis [1977]. However, the problems of Matiyasevich and Robinson, Davis and Putnam were arguably unique in their simplicity and elementary nature, and in any case the first natural undecidable problems from ordinary arithmetic.

[2] Note also that by Post's Theorem, every Δ_2^0 set is recursive in some Σ_1^0 or some Π_1^0 set, and consequently, is recursive in a Σ_1^0 complete set such as the Halting set K_0. This also confirms my view that no Δ_2^0 set is "strongly undecidable" but "decidable in a weak sense" (being decidable relative to a semi-decidable set), and that in order to be really "strongly undecidable" a set must be beyond Δ_2^0.

0022-4812/03/6801-0012/$1.50

the literature are that neither the set of equations with only finitely many solutions nor the set of equations with infinitely many solutions are recursively enumerable (see e.g., Smoryński [1991, p. 240–241]). However, this does not rule out that they might still be Trial and Error decidable (i.e., Δ_2^0). Davis, Putnam, and Robinson [1976] conjecture that the infinity case for ordinary Diophantine equations is not (more exactly, they conjecture that it has the degree $0''$), but this case remains open.[3]

Now it is of course easy, in terms of Turing machines, jumps etc., to present problems that are not even Trial and Error decidable. But it seems to me that there would be some interest in presenting explicitly a natural problem from elementary arithmetic which is so strongly undecidable that it is not even Trial and Error decidable (in other words, not decidable in the limit). The aim of this little note is to present such a problem (or rather, a couple of problems).[4] Actually, this can be achieved quite easily by combining a few known results. Although for a specialist, this could be pointed out in few lines, I think the phenomenon may have a wider interest, and therefore in what follows, I shall go into the issue in more detail and try to make the treatment relatively self-contained.

§2. Some theoretical prerequisites.

DEFINITION 1. A Diophantine equation is an equation of the form $P(x_1, \ldots, x_n) = P'(x_1, \ldots, x_n)$, where P and P' are polynomials with integer coefficients. An exponential Diophantine equation is an equation of the form $P(x_1, \ldots, x_n) = P'(x_1, \ldots, x_n)$, where P and P' are expressions constructed from variables and particular natural numbers using addition, multiplication and also exponentiation.

DEFINITION 2. A system of indices is called acceptable if it is possible to go effectively from the standard coding system to the system and vice versa (see Rogers [1958], [1967]).

DEFINITION 3. Let us denote the partial recursive function with (in the standard coding) the code e by f_e, and the recursively enumerable set that is the domain of f_e by W_e.

[3]It is striking how extremely close Davis, Putnam, and Robinson [1976] come to state explicitly the key observation of this paper, but they somehow just leave it dangling. First, they do make (in p. 372) quite explicit the relation between the possible existence of finite-fold definitions for ordinary Diophantine equations (which is an open problem) and the degree of unsolvability of the problem of determining whether a Diophantine equation has infinitely many solutions. But because they here consider only ordinary Diophantine equations, and not exponential Diophantine equations, they are only able to make the conjecture mentioned. But second, only a few pages earlier, they did state explicitly the then recent result by Matiyasevich, our Fact 3, that every recursively enumerable set has a singlefold exponential Diophantine representation. It would have been indeed a small step to state explicitly the conclusion at stake here. Thus the fact must have been at the time quite obvious to Davis, Matiyasevich and Robinson – but it was never stated explicitly. And surprisingly, there is simply no hint of it in the later literature, not even in quite comprehensive accounts of the field such as the books (Smoryński [1991]) or (Matiyasevich [1993]). So the fact remains that no-one has never explicitly presented, in this field, a problem which goes beyond Δ_2^0.

[4]I do not intend to claim that the problems I consider in this paper are the first problems from ordinary mathematics which have been proved to be beyond Δ_2^0. One should mention in particular Lempp's proof that the problem whether a finitely presented group is a torsion-free group is Π_2^0 complete (Lempp [1997]). Nevertheless, I think that the present problems are so far the most natural and elementary ones, and that because they are related to elementary arithmetic, they may be quite useful in various applications, e.g., in foundational considerations, such as my own application to the intuitionistic theories.

FACT 1. Both Diophantine and exponential Diophantine equations provide an acceptable indexing for recursively enumerable sets (see e.g., Smoryński [1977], [1991]).

FACT 2.

(i) The infinity problem: the set $\{n : W_n \text{ is infinite}\}$ is Π^0_2 complete;
(ii) the finiteness problem: the set $\{n : W_n \text{ is finite}\}$ is Σ^0_2 complete (see Rogers [1967, p. 326]).

At this point, it might be tempting to conclude from these two facts alone that the set of Diophantine equations with infinitely many solutions is similarly Π^0_2 complete. However, this does not follow, for it may happen that a finite set S has a Diophantine representation by an equation $P(x, y)$ such that $\exists y P(x, y) \Leftrightarrow x \in S$, but that the equation is yet satisfied by infinitely many sequences of parameters y. Therefore, there is no direct correspondence between the infinity or finiteness of a recursively enumerable set and the infinity or finiteness of solutions of an equation that provides a representation for the set.

However, for exponential Diophantine equations a stronger property, which enables us to avoid the above problem, is known to hold (Matiyasevich [1974]):

DEFINITION 4. An exponential Diophantine representation $\exists x P(x, y)$ for a recursively enumerable relation $R(y)$ is called a singlefold representation if $(\exists! x) P(x, y) \Leftrightarrow R(y)$. ('$\exists!$' means 'there is exactly one'; x and y are sequences of variables.)

FACT 3. Every recursively enumerable set has a singlefold exponential Diophantine representation (Matiyasevich [1974]).

It is not known whether a similar fact holds for the ordinary Diophantine equations; this is the reason why I consider in this paper only exponential Diophantine equations.

Finally, it can be seen easily that:

FACT 4. The exponential Diophantine equations which provide a singlefold representation for all recursively enumerable sets also provide an acceptable indexing for recursively enumerable sets.

In other words, it is possible to go effectively from a standard code of a recursively enumerable set to an exponential Diophantine equation which singlefoldly represents the set, and back.

§3. The main observation. Now Facts 2–4 easily give the desired results:

THEOREM 1.

(i) *The set of exponential Diophantine equations with infinitely many solutions is* Π^0_2 *complete.*
(ii) *The set of exponential Diophantine equations with only finitely many solutions is* Σ^0_2 *complete.*

PROOF. By the form of their definitions, these sets are Π^0_2 and Σ^0_2, respectively. By Facts 3 and 4, the set of Diophantine equations which provide a singlefold representation for recursively enumerable sets with infinitely (finitely) many solutions is Π^0_2

complete (Σ_2^0 complete). If one could know (from an oracle) in general the exponential Diophantine equations with infinitely many solutions, one could also indicate in particular which ones of the equations that provide a singlefold representation for a recursively enumerable set have infinitely many solutions. Therefore, the general case is also Π_2^0 complete (and similarly for finiteness and Σ_2^0 completeness.) ⊣

And thus we have achieved a couple of problems of the desired sort, formulated strictly in terms of ordinary number theory, which are strongly undecidable in the sense that they are neither semi-decidable nor co-semi-decidable, and not even Trial and Error decidable or decidable in the limit.

§4. On intuitionistic and classical theories. Although there is certainly an important philosophical difference between classical and intuitionistic mathematics, it is not at all easy to provide elementary mathematical statements which are provable only classically but not intuitionistically. For example, if a Diophantine equation has a solution, this can be proved both in classical and intuitionistic arithmetic. One cannot always prove, in a chosen axiomatic theory, that a Diophantine equation has no solution even if this is true, but one can prove this for exactly the same equations in a theory independently of whether one uses intuitionistic or classical logic. This is explained by the remarkable conservativity phenomenon established by Harvey Friedman in 1978.

FACT 5 (Friedman [1978]). PA is conservative over HA for Π_2^0-sentences. The same holds for various classical theories of arithmetic, analysis, type theory and set theory, over their intuitionistic counterparts.

However, the conservativity does not hold for Σ_2^0 sentences. Recall then that we have seen that the set of exponential Diophantine equations with only finitely many solutions is Σ_2^0 complete. As the set of true Σ_2^0 sentences is also Σ_2^0 complete, these two sets can be reduced to each other, and it follows that:

THEOREM 2. *There are exponential Diophantine equations with only finitely many solutions such that this fact can be established only in a theory with classical logic, but not in the corresponding theory using intuitionistic logic.*

Here we then have a natural, elementary arithmetical property which makes a difference between intuitionistic and classical theories.[5]

Acknowledgements. I am very grateful to Martin Davis for his valuable and encouraging comments on an earlier version of this paper. Moreover, I am indebted to Andreas Blass for his highly useful comments and suggestions.

REFERENCES

M. DAVIS [1972], *On the number of solutions of Diophantine equations*, ***Proceedings of the American Mathematical Society***, vol. 35, pp. 552–554.

M. DAVIS [1973], *Hilbert's tenth problem is unsolvable*, ***The American Mathematical Monthly***, vol. 80, pp. 233–269.

[5]It may appear that complications of some sort may arise because there are various notions of "finiteness" in intuitionistic mathematics, all equivalent classically but not intuitionistically. However, the set whose finiteness is at stake here, viz. the set of solutions of an exponential Diophantine equation, is decidable, and hence the situation should be quite unproblematic even from the intuitionistic prespective.

M. Davis [1977], *Unsolvable problems*, ***Handbook of mathematical logic*** (J. Barwise, editor), North-Holland, Amsterdam, pp. 567–594.

M. Davis, H. Putnam, and J. Robinson [1961], *The decision problem for exponential diophantine equations*, ***Annals of Mathematics, Second Series***, vol. 74, pp. 425–436.

M. Davis, H. Putnam, and J. Robinson [1976], *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution*, ***Proceedings of Symposia in Pure Mathematics***, vol. 28, pp. 323–378.

Harvey Friedman [1978], *Classically and intuitionistically provably recursive functions*, ***Higher set theory*** (Müller and Scott, editors), Springer-Verlag, Berlin, Lecture Notes in Mathematics 669, pp. 21–27.

K. Kelly [1996], ***The logic of reliable inquiry***, Oxford University Press, New York.

S. Lempp [1997], *The computational complexity of torsion-freeness of finitely presented groups*, ***Bulletin of the Australian Mathematical Society***, vol. 56, pp. 273–277.

Y. Matiyasevich [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).

Y. Matiyasevich [1974], *Sushchestvovanie neeffektiviziruemikh otsenok v teorii ekzponentsial'no diofantovikh*, ***Zapiski Naucnyh Seminarov Leningradskogo Otdelenija Matematiceskogo Instituta im. V. A. Steklova, Academii Nauk SSSR***, vol. 40, pp. 77–93.

Y. Matiyasevich [1993], ***Hilbert's tenth problem***, M.I.T. Press, Cambridge, MA.

D. Osherson, M. Stob, and S. Weinstein [1986], ***Systems that learn***, M.I.T. Press, Cambridge.

H. Putnam [1965], *Trial and error predicates and the solution to a problem of Mostowski*, this Journal, vol. 30, pp. 49–57.

H. Rogers, Jr. [1958], *Gödel numberings of partial recursive functions*, this Journal, vol. 23, pp. 331–341.

H. Rogers, Jr. [1967], ***Theory of recursive functions and effective computability***, McGraw-Hill, New York.

J. R. Shoenfield [1959], *On degrees of unsolvability*, ***Annals of Mathematics***, vol. 69, pp. 644–653.

C. Smoryński [1977], *A note on the number of zeros of polynomials and exponential polynomials*, this Journal, vol. 42, pp. 99–106.

C. Smoryński [1991], ***Logical number theory. I***, Springer-Verlag, Berlin.

HELSINKI COLLEGIUM FOR ADVANCED STUDIES,
P.O.BOX 4,
FIN-00014 UNIVERISTY OF HELSINKI, FINLAND
E-mail: panu.raatikainen@helsinki.fi