RAIRO
INFORMATIQUE THÉORIQUE

CRISTIAN CALUDE
GHEORGHE PĂUN

Independent instances for some undecidable problems

RAIRO – Informatique théorique, tome 17, n° 1 (1983), p. 49-54.
<http://www.numdam.org/item?id=ITA_1983__17_1_49_0>

R.A.I.R.O. Informatique théorique/Theoretical Informatics
(vol. 17, n° 1, 1983, p. 49 à 54)

INDEPENDENT INSTANCES FOR SOME UNDECIDABLE PROBLEMS (*)

by Cristian CALUDE and Gheorghe PĂUN (1)

Communicated by J. BERSTEL

Abstract. — *In this note we prove the existence of effectively independent instances (with respect to an arbitrary recursively axiomatizable, consistent, intuitively true and sufficiently rich theory) for some well-known undecidable problems including the Emptiness Problem, the Finiteness Problem, the Totality Problem, the Halting Problem and the Post Correspondence Problem. Applications in the Theory of Diophantine Equations and in the Formal Language Theory will be analyzed.*

Résumé. — *Dans cette note nous prouvons l'existence, pour quelques problèmes indécidables bien connus, d'instances indépendants (relativement à une théorie récursivement axiomatisable, consistante, intuitivement vraie et suffisamment riche). Les problèmes traités comprennent le problème de la vacuité, de la finitude, de la totalité, de l'arrêt et le problème de correspondance de Post. On analyse les applications à la théorie des équations diophantiennes et des langages formels.*

0. INTRODUCTION

For many years (since the appearance of Gödel Incompleteness Theorem) mathematicians have been looking for a simple, interesting and strictly mathematical example of an independent problem. The first such examples were found by Hartmanis and Hopcroft [3] and by Paris and Harrington [6].

In the present note we shall prove the existence of independent instances (with respect to an arbitrary recursively axiomatizable, consistent, intuitively true and sufficiently rich theory) for some well-known undecidable problems including the Emptiness Problem, the Finiteness Problem, the Totality Problem, the Halting Problem and the Post Correspondence Problem. Applications in the Theory of Diophantine Equations and in the Formal Language Theory will be analyzed. All the proofs are constructive, hence concrete

(*) Received in February 1982, revised in June 1982.
(1) Department of Mathematics, University of Bucharest, Str. Academiei 14, R-70109, Bucharest, Romania.

R.A.I.R.O. Informatique théorique/Theoretical Computer Science, 0399-0540/1983/49/$ 5,00

examples can be algorithmically constructed (although the constructions seem to be quite tedious).

These results motivate the following conjecture: Every undecidable problem has a true/false (at the level of metalanguage) instance which is independent.

1. PREREQUISITES

We shall specify only some basic definitions and notations; for details the reader is referred to [8] (for Recursive Function Theory), [10] (for Formal Language Theory) and [1] (for Diophantine Equations).

Let (φ_i) be an acceptable gödelization of all unary partial recursive functions. If some φ_i is undefined for some natural number x, then we write $\varphi_i(x)=\infty$.

We denote by $\pi=(V, n, x, y)$ a Post Correspondence Problem (PCP, for short) [7], where V is a finite alphabet and x, y are n-tuples of non-empty strings over V; the empty string is denoted by λ.

All the considerations in the paper are dealing with an arbitrarily given formalized theory T, having the following four properties:

1. The theory T is recursively axiomatizable (i. e. the set of all theorems which can be inferred in T is recursively enumerable);

2. The theory T is consistent;

3. All the theorems deductible in T are intuitively true (at the level of metalanguage);

4. The theory T is rich enough to contain the recursive arithmetic.

The previous requirements are quite natural and a theory T as above is the usual framework for most of the independence studies.

A true/false (at the level of metalanguage) problem P is said to be *independent* with respect to T if neither P nor the negation of P can be proved in T.

2. RESULTS

Firstly we shall prove a general independence result.

THEOREM 1 : *Let (φ_i) be an acceptable gödelization and let T be a theory having the above four properties. Let $P(i)$ be a predicate representable in T, subject to the following two conditions:*

i) If $P(i)$ is true, then there exists an x such that $\varphi_i(x)=\infty$;

ii) If $P(i)$ is false, then there exists an y such that $\varphi_i(y) \neq \infty$.

Then we can effectively find a natural number k such that the statement $P(k)$ is true (at the level of metalanguage) and $P(k)$ is independent of T.

Proof : Consider the following partial function:

$$\tau(x, i) = \begin{cases} 1, \text{ if there exists a proof in } T \text{ for } P(i), \\ \infty, \text{ otherwise.} \end{cases}$$

Clearly, τ is a partial recursive function because T is recursively axiomatizable.

We apply the $S-m-n$ Theorem; we effectively find a recursive function $s: N \to N$ such that

$$\tau(x, i) = \varphi_{s(i)}(x), \quad \text{for all} \quad i \text{ and } x.$$

Now by the Recursion Theorem there exists a natural number k such that

$$\varphi_k(x) = \varphi_{s(k)}(x), \quad \text{for all } x.$$

We shall prove that $P(k)$ has the required properties.

The statement $P(k)$ is true at the level of metalanguage. Indeed, if $P(k)$ is false, then by *ii)* there exists an x_0 such that $\varphi_k(x_0) \neq \infty$. In view of the construction of the partial recursive function τ and of property 3, we derive the relation $\tau(x, k) = \infty$, for all x. Consequently, $\varphi_k(x) = \infty$, for all x. Putting $x = x_0$ we obtain a contradiction.

Now we prove that $P(k)$ is not a theorem in T. Suppose, on the contrary, that $P(k)$ can be deduced by a proof in T. By construction we have: $\varphi_k(x) = \tau(x, k) = 1$, for all x. Again we use the property 3 of T and we deduce that $P(k)$ is true; then, by *i)* there exists an x_0 such that $\varphi_k(x_0) = \infty$. The last equality contradicts the relation $\varphi_k(x_0) = 1$.

Finally we show that the negation of $P(k)$ cannot be a theorem in T. If, on the contrary, there exists a proof in T for the negation of $P(k)$, then $P(k)$ is false (at the level of metalanguage). This contradicts the first conclusion of our proof.

In the sequel we shall examine some particular cases.

THEOREM 2 : *We can effectively find a diophantine equation $p_k = 0$ which has at least one solution and for which the statement " the equation $p_k = 0$ has a solution " is independent of T.*

Proof: Let $P(i)$ be the predicate: " For all natural x and y, $\varphi_i(x) \neq y$ ". Clearly,

we can apply the Theorem 1 and we effectively find an independent instance $P(k)$.

Please note that for all natural i, $P(i)$ is true iff the range of φ_i is empty. So, the Emptiness Problem has an independent instance. Finally, we apply the Diophantine Representation Theorem (*see* [1], [4]) and we effectively obtain the required equation.

COROLLARY 1: *The Totality Problem has an independent instance which is false at the level of metalanguage.*

Proof: Let us consider the predicate $P(i)$: " The partial recursive function φ_i is not total ". Obviously, $P(i)$ is true iff φ_i is not total. By the Theorem 1 we get the desired independent instance.

COROLLARY 2: *The Finiteness Problem has an independent instance which is true at the level of metalanguage.*

Proof: Let $P(i)$ be the predicate: " There exists x such that for all y, $y \geqslant x$, $\varphi_i(y) = \infty$ ". The predicate $P(i)$ satisfies the hypothesis of Theorem 1 and $P(i)$ is true iff the domain of φ_i is finite.

COROLLARY 3: *The Halting Problem has an infinity of true and independent instances.*

Proof: Let x_0 be a given natural number. Let $P(i)$ be the predicate: " The partial recursive function $\varphi_i(x_0) = \infty$ ". The predicate $P(i)$ satisfies the hypothesis of Theorem 1. Consequently, the statement " $\varphi_k(x_0) = \infty$ " is true and independent of T.

THEOREM 3: *There exists a PCP π for which the proposition " π has a solution " is true and independent.*

Proof: Let (φ_i) be a gödelization of Turing Machines. In view of Corollary 3, there exists a Turing Machine A_0 for which the proposition " A_0 halts on input u ", for some string u, is true and independent. For each machine A, an equivalent type-O Chomsky grammar G can be constructed. For each type-O grammar G and each string $u \neq \lambda$, a *PCP* $\pi(G, u)$ can be algorithmically constructed such that $\pi(G, u)$ has a solution iff $u \in L(G)$. Consequently, starting from Turing Machine A_0 and from an arbitrary nonempty string u, a *PCP* $\pi_0(u)$ can be algorithmically constructed such that $\pi_0(u)$ has a solution iff A_0 halts on input u. The *PCP* $\pi_0(u)$ has a solution but " $\pi_0(u)$ has a solution " is an independent proposition.

COROLLARY 4: *All the undecidable problems in Formal Language Theory*

which are consequences of Post Correspondence Problem have independent instances.

Here are some basic decision problems which are known to be unsolvable:

1) Is $L(G)$ empty, finite or infinite for an arbitrary type-1 grammar G?

2) Is $L(G_1) \cap L(G_2)$ empty, finite, infinite, regular, or context-free for arbitrary context-free grammars G_1, G_2?

3) Is $V^* - L(G)$ empty, finite, infinite, regular, or context-free for an arbitrary context-free grammar G?

4) Is $L(G_1)$ included or equal to $L(G_2)$ for arbitrary context-free grammars G_1, G_2?

5) Is G or $L(G)$ ambiguous for an arbitrary context-free grammar G?

For a class $\mathcal{G}$ of generative devices involving context-free rules, we denote by $\mathcal{L}(\mathcal{G})$ the family of languages generated by λ-free grammars in $\mathcal{G}$ and by $\mathcal{L}_\lambda(\mathcal{G})$ the family of languages generated by arbitrary grammars in $\mathcal{G}$.

COROLLARY 5: *If $\mathcal{G}$ is a class of grammars such that $\mathcal{L}_\lambda(\mathcal{G})$ equals the family of recursively enumerable languages and $\mathcal{L}(\mathcal{G})$ is closed under intersection by regular sets, then there exists a λ-free grammar G in $\mathcal{G}$ for which the proposition " $L(G)$ is nonempty " is true and independent.*

Proof: Let A_0 be a Turing Machine for which the halting problem is independent on the input λ. Let $G_0 \in \mathcal{G}$ be a grammar for which $L(A_0) = L(G_0)$. Let a be a new symbol; we replace each rule $X \to \lambda$ in G_0 by $X \to a$. Denote by G_1 the obtained grammar. Clearly, G_1 is λ-free and $\lambda \in L(G_0) = L(A_0)$ iff $L(G_1) \cap \{a\}^*$ is nonempty. As $\mathcal{L}(\mathcal{G})$ is closed under intersection with regular sets, it follows that $L(G_1) \cap \{a\}^*$ can be generated by a λ-free grammar G_2 in $\mathcal{G}$. The grammar G_2 is the desired one.

There are many classes $\mathcal{G}$ of grammars fulfilling the conditions in above corollary. For example, the programmed grammars of [9] (with appearance checking), the scattered context grammars of [2], the simple matrix grammars with leftish derivation [5] are such classes of grammars.

We want to emphasize the two open problems suggested at the begining of this note:

Q_1. (CONJECTURE): *All the undecidable problems contain an instance which is true/false and independent.*

Q_2. *Find (as simple as possible) concrete examples of independent problems for known undecidable problems (for instance, for the above problems in Formal Language Theory).*

REFERENCES

1. M. DAVIS, Yu. MATIJASEVIČ and J. ROBINSON, *Hilbert's Tenth Problem. Diophantine Equations: Positive Aspects of a Negative Solution*, Proc. Symposia Pure Math., vol. 28, 1976, p. 223-378.
2. S. GREIBACH and J. HOPCROFT, *Scattered Context Grammars*, J. Comput. Systems Sci., vol. 3, 1969, p. 233-247.
3. J. HARTMANIS and J. HOPCROFT, *Independence Results in Computer Science*, ACM SIGACT News, vol. 8, 1976, p. 13-24.
4. Yu. MATIJASEVIČ, *Enumerable Sets Are Diophantine*. Dokl. Akad. Nauk SSSR, vol. 191, 1970, p. 279-282.
5. H. A. MAURER, *Simple Matrix Languages with a Leftmost Restriction*, Inform. Control, vol., 23, 1973, p. 128-139.
6. J. PARIS and L. HARRINGTON, *A Mathematical Incompleteness in Peano Arithmetic*, in J. Barwise (ed.), Handbook of Mathematical Logic, North-Holland, Amsterdam, 1977, p. 1133-1142.
7. E. POST, *A Variant of a Recursively Unsolvable Problem*, Bull. AMS, vol. 52, 1946, p. 264-268.
8. H. ROGERS Jr., *Theory of Recursive Functions and Effective Computability*, McGraw-Hill, New York, 1967.
9. D. ROSENKRANTZ, *Programmed Grammars and Classes of Formal Languages*, J. of ACM, vol. 16, 1969, p. 107-131.
10. A. SALOMAA, *Formal Languages*, Academic Press, New York, London, 1973.