COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA **16** (1) (1996) 143–147

NOTE

COMPLEXITY OF THE FROBENIUS PROBLEM

J. L. RAMÍREZ-ALFONSÍN

Received May 20, 1994
Revised October 29, 1994

Consider the Frobenius Problem: Given positive integers $a_1,\dots,a_n$ with $a_i \geq 2$ and such that their greatest common divisor is one, find the largest natural number that is not expressible as a non-negative integer combination of $a_1,\dots,a_n$. In this paper we prove that the Frobenius problem is NP-hard, under Turing reductions.

1. Introduction

Consider the *Frobenius Problem*: Given positive integers $a_1,\dots,a_n$ with $a_i \geq 2$ and such that their greatest common divisor is one, find the largest natural number that is not expressible as a non-negative integer combination of $a_1,\dots,a_n$. For the special case of $n=2$, the answer is explicity known, it is $a_1a_2-a_1-a_2$ (see Theorem 2.1). Rödseth [9], Selmer and Beyer [12], Greenberg [3] and Scarf and Shallcross [10] have developed algorithms to solve the Frobenius problem in the case $n=3$. See [5, 11] for a further literature on the general problem.

R. Kannan [6] gave a polynomial time algorithm for any fixed n. He also suggested that the problem should be NP-hard for variable n; however, no proof of this statement seems to be known [7]. Our aim is to confirm this statement.

Theorem 1.1. *The Frobenius problem is NP-hard.*

First, we briefly give some relevant aspects of computational complexity needed in this paper; for a detailed presentation see [4] and [2].

Decision Problems are problems having merely two possible answers: either *yes* or *no*. Suppose Π and Π' are two problems, a *polynomial time Turing reduction* from Π to Π' is an algorithm A which solves Π by using a hypothetical subroutine A' for solving Π', such that, if A' were a polynomial time algorithm for Π' then A would be a polynomial time algorithm for Π. We say that Π can be *Turing reduced* to Π'.

Mathematics Subject Classification (1991): 68 Q 15, 90 C 10

A problem Π is called (Turing) *NP-hard* if there is an NP-complete decision problem Π' such that Π' can be Turing reduced to Π.

2. The Proof

Let $a_1,\dots,a_n$ be positive integers with $a_i \geq 2$ and such that $\gcd(a_1,\dots,a_n)=1$. Let $F(a_1,\dots,a_n)$ be the largest natural number p such that p is not a non-negative integer combination of $a_1,\dots,a_n$. Note that the fact that $\gcd(a_1,\dots,a_n)=1$ implies that $F(a_1,\dots,a_n)$ exists.

Theorem 2.1. [1] (Brauer–Shockley)

$$F(a_1,\dots,a_n) = \max_{\ell\in\{1,2,\dots,a_n-1\}} t_\ell - a_n$$

where $t_\ell =$ *the smallest positive integer congruent to* ℓ *modulo* a_n, *that is expressible as a non-negative integer combination of* $a_1,\dots,a_{n-1}$.

Proof. Let S be any positive integer. If $S\equiv 0 \pmod{a_n}$ then S is a non-negative integer combination of a_n. If $S\equiv \ell \pmod{a_n}$ then S is a non-negative integer combination of $a_1,\dots,a_n$ if and only if $S\geq t_\ell$. ∎

We shall prove Theorem 1.1 by giving a Turing reduction from *the Integer Knapsack Problem* [IKP], which is known to be NP-complete ([8], page 376).

Input: Positive integers $b_1, \dots, b_n$ and t.

Question: Does there exist integers $x_i \geq 0$, with $1\leq i\leq n$, such that $\sum_{i=1}^{n} x_i b_i = t$?

We will prove that, by using an hypothetical subroutine A that solves the Frobenius problem, we may create an algorithm B for solving [IKP] as follows.

Let $\gcd(b_1,\dots,b_n)=r$. We may assume $r=1$, otherwise consider [IKP] with input $b_i' = \frac{b_i}{r}$, for each $i=1,\dots,n$, and $t'=\frac{t}{r}$.

Algorithm B

Find $F(b_1,\dots,b_n)$

If $t > F(b_1,\dots,b_n)$ **then**

There exist integers $x_i\geq 0$, $1\leq i\leq n$, such that $\sum_{i=1}^{n} x_i b_i = t$.

Else

Find $F(\bar b_1,\dots,\bar b_n,\bar b_{n+1})$ where $\bar b_i = 2b_i$ for each $i=1,\dots,n$ and $\bar b_{n+1} = 2F(b_1,\dots,b_n)+1$ (note that $\gcd(\bar b_1,\dots,\bar b_{n+1}) = 1$ since $\gcd(\bar b_1,\dots,\bar b_n) = 2$ and $\bar b_{n+1} \equiv 1 \pmod 2$) Find $F(\bar b_1,\dots,\bar b_n,\bar b_{n+1},\bar b_{n+2})$ where $\bar b_{n+2} = F(\bar b_1,\dots,\bar b_{n+1}) - 2t$.

We need the following proposition before proving Theorem 1.1.

Proposition 2.2. *Let b_i for each $i=1,\dots,n$, and $\bar{b}_i$ for each $i=1,\dots,n+1$ be as in algorithm* **B**. *Then $F(\bar{b}_1,\dots,\bar{b}_{n+1})=4F(b_1,\dots,b_n)+1$.*

Proof. Let g be an integer such that $g>4F(b_1,\dots,b_n)+1$. Let $g'=g-\ell\bar{b}_{n+1}$ where $\ell\equiv g \pmod 2$. If $\ell=0$ then $g'=g>4F(b_1,\dots,b_n)+1>2F(b_1,\dots,b_n)$. Otherwise, if $\ell=1$ then

$$g'=g-\bar{b}_{n+1}>4F(b_1,\dots,b_n)+1-(2F(b_1,\dots,b_n)+1)=2F(b_1,\dots,b_n).$$

Hence, $g'>2F(b_1,\dots,b_n)$ and since $g'\equiv 0 \pmod 2$ then g' is expressible as a non-negative integer combination of $\bar{b}_1,\dots,\bar{b}_n$. Therefore, g is also expressible as a non-negative integer combination of $\bar{b}_1,\dots,\bar{b}_{n+1}$.

We prove now by contradiction that $4F(b_1,\dots,b_n)+1$ is not expressible as a non-negative integer combination of $\bar{b}_1,\dots,\bar{b}_{n+1}$.

Suppose there exist integers $x_i\geq 0$, $1\leq i\leq n+1$, such that $\sum_{i=1}^{n+1} x_i\bar{b}_i = 4F(b_1,\dots,b_n)+1$. Since $4F(b_1,\dots,b_n)+1\not\equiv 0 \pmod 2$ then $x_{n+1}\geq 1$.

On the other hand, if $x_{n+1}\geq 2$ then $x_{n+1}\bar{b}_{n+1}>4F(b_1,\dots,b_n)+1$ so $x_{n+1}\leq 1$. Therefore $x_{n+1}=1$, thus

$$\sum_{i=1}^{n} x_i\bar{b}_i+\bar{b}_{n+1}=4F(b_1,\dots,b_n)+1$$

and

$$\sum_{i=1}^{n} x_i\bar{b}_i=2F(b_1,\dots,b_n)$$

then

$$\sum_{i=1}^{n} x_i b_i=F(b_1,\dots,b_n), \qquad \text{which is impossible.}$$

Hence, $4F(b_1,\dots,b_n)+1$ is the largest natural number that is not expressible as a non-negative integer combination of $\bar{b}_1,\dots,\bar{b}_{n+1}$. ∎

We may prove now Theorem 1.1.

Proof of theorem 1.1. Let $t<F(b_1,\dots,b_n)$. We claim that there exist integers $x_i\geq 0$, with $1\leq i\leq n$, such that $\sum_{i=1}^{n} x_i b_i=t$ if and only if $F(\bar{b}_1,\dots,\bar{b}_{n+2})<F(\bar{b}_1,\dots,\bar{b}_{n+1})$.

Assume that there exist integers $x_i \geq 0$, $1 \leq i \leq n$, such that $\sum_{i=1}^{n} x_i b_i = t$. So, $\sum_{i=1}^{n} x_i \bar{b}_i = 2t$ and since $\bar{b}_{n+2} = F(\bar{b}_1, \ldots, \bar{b}_{n+1}) - 2t$ then

$$F(\bar{b}_1, \ldots, \bar{b}_{n+1}) = \sum_{i=1}^{n+2} x_i \bar{b}_i.$$

Hence, $F(\bar{b}_1, \ldots, \bar{b}_{n+2}) < F(\bar{b}_1, \ldots, \bar{b}_{n+1})$.

Conversely, assume $F(\bar{b}_1, \ldots, \bar{b}_{n+2}) < F(\bar{b}_1, \ldots, \bar{b}_{n+1})$. By Proposition 2.2 we have,

$$F(\bar{b}_1, \ldots, \bar{b}_{n+1}) = 4F(b_1, \ldots, b_n) + 1 = \sum_{i=1}^{n+2} x_i \bar{b}_i$$

for some integers $x_i \geq 0$, with $1 \leq i \leq n+2$.

Since $F(\bar{b}_1, \ldots, \bar{b}_{n+1})$ is not expressible as a non-negative integer combination of $\bar{b}_1, \ldots, \bar{b}_{n+1}$ then $x_{n+2} \geq 1$.

On the other hand, from

$$x_{n+2} \bar{b}_{n+2} = x_{n+2}(F(\bar{b}_1, \ldots, \bar{b}_{n+1}) - 2t)$$

and

$$2t < 2F(b_1, \ldots, b_n) < \frac{4F(b_1, \ldots, b_n) + 1}{2}$$

we have

$$\begin{aligned} x_{n+2} \bar{b}_{n+2} &> x_{n+2} \left(4F(b_1, \ldots, b_n) + 1 - \left(\frac{4F(b_1, \ldots, b_n) + 1}{2} \right) \right) \\ &= x_{n+2} \left(\frac{4F(b_1, \ldots, b_n) + 1}{2} \right). \end{aligned}$$

Thus, if $x_{n+2} \geq 2$ then $x_{n+2} \bar{b}_{n+2} > 4F(b_1, \ldots, b_n) + 1$ so $x_{n+2} \leq 1$. Therefore $x_{n+2} = 1$, so

$$4F(b_1, \ldots, b_n) + 1 = \sum_{i=1}^{n+1} x_i \bar{b}_i + \bar{b}_{n+2}$$

and

$$4F(b_1, \ldots, b_n) + 1 = \sum_{i=1}^{n+1} x_i \bar{b}_i + F(\bar{b}_1, \ldots, \bar{b}_{n+1}) - 2t$$

then

$$2t = \sum_{i=1}^{n+1} x_i \bar{b}_i.$$

Finally, $\bar{b}_{n+1}=2F(b_1,\dots,b_n)+1>2t$ leads to $x_{n+1}=0$. Therefore,

$$2t=\sum_{i=1}^{n} x_i\bar{b}_i$$

and $t=\sum_{i=1}^{n} x_ib_i$. ∎

References

[1] A. Brauer and J. E. Shockley: On a Problem of Frobenius, *Journal für reine und angewandte Mathematik*, **211** (1962), 399–408.

[2] M. R. Garey and D. S. Johnson: *Computers and Intractability: A Guide to the Theory of NP-completeness*, W. H. Freeman and Company, N.Y., 1979.

[3] H. Greenberg: Solution to a linear diophantine equation for nonnegative integers, *Journal of Algorithms*, **9** (1988), 343–353.

[4] M.Grötschel, L.Lovász and A.Schrijver: *Geometric Algorithms and Combinatorial Optimization*, Springer-Verlag, 1988.

[5] M. Hujter and B.Vizvári: The exact solution to the Frobenius Problem with three variables, *Journal of the Ramanujan Math.Soc.*, **2** (1987), 117–143.

[6] R. Kannan: Lattice Translates of a Polytope and the Frobenius problem, *Combinatorica*, **12** (2), (1992), 161–177.

[7] R. Kannan: private communication, 1994.

[8] C. H. Papadimitriou and K.Steiglitz: *Combinatorial Optimization: Algorithms and Complexity*, Prentice-Hall, Inc., 1982.

[9] O. J. Rödseth: On a linear diophantine problem of Frobenius, *Journal für reine und angewandte Mathematik*, **301** (1968), 171–178.

[10] H. E. Scarf and D.Shallcross: The Frobenius problem and maximal lattice three bodies, Manuscript, (1989).

[11] E. S. Selmer: On the linear diophantine problem of Frobenius, *Journal für reine und angewandte Mathematik*, **293/294** (1977), 1–17.

[12] E. S. Selmer and O.Beyer: On the linear diophantine problem of Frobenius in three variables, *Journal für reine und angewandte Mathematik*, **301** (1978), 161–170.

J. L. Ramírez-Alfonsín

Universidad Nacional Autónoma de México
Instituto de Matemáticas
Area de la Investigación Científica
Circuito Exterior, Ciudad Universitaria,
México D.F. 04510
JLRA@SERVIDOR.DGSCA.UNAM.MX