An extension of the Frobenius coin-exchange problem [1]

MATTHIAS BECK AND SINAI ROBINS[2]

Dedicated to the memory of Robert F. Riley

1 Introduction

Given a set of positive integers $A = \{a_1, \ldots, a_d\}$ with $\gcd(a_1, \ldots, a_d) = 1$, we call an integer n *representable* if there exist nonnegative integers $m_1, \ldots, m_d$ such that

$$n = m_1 a_1 + \cdots + m_d a_d \ .$$

The *linear diophantine problem of Frobenius* asks for the largest integer which is not representable. We call this largest integer the *Frobenius number* $g(a_1, \ldots, a_d)$.

One fact which makes this problem attractive is that it can be easily described, for example, in terms of coins of denominations $a_1, \ldots, a_d$; the Frobenius number is the largest amount of money which cannot be formed using these coins.

The following "folklore" theorem has long been known (probably at least since Sylvester [9]).

Theorem 1. *$g(a, b) = ab - a - b$.*

For $d \geq 3$, the quest for general formulas has so far been unsuccessful. For the case $d = 2$, Sylvester [9] proved the following result.

Theorem 2 (Sylvester). *For $A = \{a, b\}$, exactly half of the integers between 1 and $(a-1)(b-1)$ are representable.*

Here we introduce and study a more general problem, a natural extension of the Frobenius problem.

Definition 1. *We say that n is* k-representable *if n can be represented in the form*

$$n = m_1 a_1 + \cdots + m_d a_d$$

(where $m_1, \ldots, m_d$ are again nonnegative integers) in exactly k ways.

In terms of coins, we can exchange the n pennies in exactly k different ways in terms of the given coin denominations. It is not hard to convince ourselves that—because the numbers in A are relatively prime—eventually every integer can be represented in more than k ways, for any k. Our extension of the Frobenius number is captured by the following definition:

---

[1]Revised version of 11/11/2002.

[2]The second author is supported by the NSA Young Investigator Grant MSPR-OOY-196.

Definition 2. *$g_k(a_1, \ldots, a_d)$ is the smallest integer beyond which every integer is represented more than k times.*

This is a natural generalization of the concept of the Frobenius number, as

$$g(a_1, \ldots, a_d) = g_0(a_1, \ldots, a_d) .$$

As to be expected, the study of g_k is extremely complicated for $d \geq 3$, due to a certain non-linearity of a function $p_A(n)$ that is defined below. In this paper we completely analyze the case $d = 2$, that is, $A = \{a, b\}$, and present the following results.

Theorem 3. $g_k(a, b) = (k + 1)ab - a - b$.
Theorem 4. *Given $k \geq 2$, the smallest k-representable integer is $ab(k - 1)$.*
Theorem 5. *There are exactly $ab - 1$ integers which are uniquely representable. Given $k \geq 2$, there are exactly ab k-representable integers.*

Theorem 3 is a direct generalization of Theorem 1. (Theorem 4 is meaningless for $k = 0$ and trivial for $k = 1$: the smallest representable integer is $\min(a, b)$). Theorem 5 extends Theorem 2 for all $k > 0$.

Quite recently, Jeff Shallit and Ming-Wei Wang found this notion of k-representability useful as a device for studying the complexity of finite automata [8]. In another interesting application, Basil Gordon [4] has recently used this notion in his theory of 'piecewise linear recurrences'.

2 Proofs

One approach to the Frobenius problem and its generalizations is through the study of the *restricted partition function*

$$p_A(n) = \# \left\{ (m_1, \ldots, m_d) \in \mathbb{Z}^d : \text{ all } m_j \geq 0, \ m_1 a_1 + \cdots + m_d a_d = n \right\} ,$$

the number of partitions of n using only the elements of A as parts. In view of this function, $g_k(a_1, \ldots, a_d)$ is the smallest integer such that for every $n > g_k(a_1, \ldots, a_d)$ we have $p_A(n) > k$.

The basic idea behind our proofs is to view p_A as

$$p_A(n) = \# \left\{ (m_1, \ldots, m_d) \in \mathbb{Z}^d : \text{ all } m_j \geq 0, \ m_1 a_1 + \cdots + m_{d-1} a_{d-1} = n - m_d a_d \right\} ,$$

from which one obtains the recursion formula

$$p_{\{a_1, \ldots, a_d\}}(n) = \sum_{m \geq 0} p_{\{a_1, \ldots, a_{d-1}\}}(n - m a_d) . \tag{1}$$

For the following, it will be useful to introduce the function

$$q_A(n) = \# \left\{ (m_1, \ldots, m_d) \in \mathbb{Z}^d : \text{ all } m_j > 0, \ m_1 a_1 + \cdots + m_d a_d = n \right\},$$

which counts those partitions of n which uses only parts from A, where we additionally demand that each part gets used at least once. The functions p_A and q_A are intimitely related through

$$q_A(n) = p_A(n - a_1 - \cdots - a_d) \ . \tag{2}$$

The recursion formula for q_A, corresponding to (1), is

$$q_{\{a_1,\ldots,a_d\}}(n) = \sum_{m>0} q_{\{a_1,\ldots,a_{d-1}\}}(n - ma_d) \ . \tag{3}$$

Proof of Theorem 3. For $d = 2$, (3) simplifies to

$$q_{\{a,b\}}(n) = \sum_{m>0} q_{\{a\}}(n - mb) \ . \tag{4}$$

Now

$$q_{\{a\}}(n) = \begin{cases} 1 & \text{if } a|n \text{ and } n > 0 \\ 0 & \text{otherwise.} \end{cases}$$

Since $\gcd(a,b) = 1$, the sum in (4) is larger than k if we have $(k+1)a$ summands or more. There are $\left\lfloor \frac{n-1}{b} \right\rfloor$ summands in (4). Hence for any $n > (k+1)ab$, $q_{\{a,b\}}(n) > k$. On the other hand, it is easy to see that $q_{\{a,b\}}((k+1)ab) = k$. Via (2), this translates into

$$p_{\{a,b\}}(n) > k \quad \text{if} \quad n > (k+1)ab - a - b$$
$$p_{\{a,b\}}((k+1)ab - a - b) = k \qquad \square$$

Proof of Theorem 4. We play a similar game as in the previous proof, now starting with (1), which gives for $d = 2$

$$p_{\{a,b\}}(n) = \sum_{m\geq 0} p_{\{a\}}(n - mb) \ . \tag{5}$$

Now

$$p_{\{a\}}(n) = \begin{cases} 1 & \text{if } a|n \text{ and } n \geq 0 \\ 0 & \text{otherwise,} \end{cases}$$

and since $\gcd(a,b) = 1$, multiples of ab give 'peaks' for the sum in (5) in the sense that

$$p_{\{a,b\}}(kab) > p_{\{a,b\}}(n) \quad \text{for all } n < kab \ .$$

The proof is finished by the straightforward observation that

$$p_{\{a,b\}}(kab) = k + 1 \ . \qquad \square$$

Proof of Theorem 5. First, in the interval $[1, ab]$, there are, by Theorems 2 and 4,

$$ab - \frac{(a-1)(b-1)}{2} - 1$$

1-representable integers. Because of the almost periodic behavior of the partition function

$$p_{\{a,b\}}(n+ab) = p_{\{a,b\}}(n) + 1 \ , \tag{6}$$

which follows directly from (5) and the fact that a and b are relatively prime, we see that there are

$$\frac{(a-1)(b-1)}{2}$$

1-representable integers above ab. For $k \geq 2$, the statement follows by similar reasoning. □

3 Final remarks

For two relatively prime positive integers a and b, Popoviciu [6] proved the following formula, which seems to be not widely known:[3]

$$p_{\{a,b\}}(n) = \frac{n}{ab} - \left\{ \frac{b^{-1}n}{a} \right\} - \left\{ \frac{a^{-1}n}{b} \right\} + 1 \ .$$

Here $\{x\} = x - \lfloor x \rfloor$ denotes the fractional part of x, $a^{-1}a \equiv 1(\mathrm{mod}\ b)$, and $b^{-1}b \equiv 1(\mathrm{mod}\ a)$. Popoviciu's formula can be used to derive other proofs of Theorems 3, 4, and 5.

We note that for all $d > 2$, generalized Dedekind sums [3] appear in the formulas for $p_A(n)$, which increases the complexity of the problem. The full details of these connections to Dedekind sums can be found in [2].

We conclude with a few remarks regarding extensions of the above theorems to $d > 2$. Although no 'nice' formula similar to the one appearing in Theorem 1 is known for $d > 2$, there has been a huge effort devoted to giving bounds and algorithms for the Frobenius number [1]. Secondly, we remark that Theorem 2 does not extend in general; however, [5] gives necessary and sufficient conditions on the a_j's under which Theorem 2 does extend. The almost periodic behavior (6) of the partition function extends easily to higher dimensions [2]. We leave the reader with the following "exercise":

Unsolved problems. *Extend Theorems 3, 4, and 5 to* $d \geq 3$.

Acknowledgements. The authors are grateful to Mel Nathanson and Herb Wilf for helpful remarks and references on partition functions, and to Olivier Bordellès for pointing out the reference [6].

References

[1] J. L. Ramirez Alfonsin, *The diophantine Frobenius problem*, Report No. 00893, Forschungsinstitut für diskrete Mathematik, Universität Bonn, 2000.

[3] Popoviciu's formula has been resurrected at least twice [7, 10].

[2] Matthias Beck, Ricardo Diaz, and Sinai Robins, *The Frobenius problem, rational polytopes, and Fourier–Dedekind sums*, J. Number Theory **96** (2002), 1–21.

[3] Ira M. Gessel, *Generating functions and generalized Dedekind sums*, Electron. J. Combin. **4** (1997), no. 2, Research Paper 11, approx. 17 pp. (electronic), The Wilf Festschrift (Philadelphia, PA, 1996). MR 98f:11032

[4] Basil Gordon, *Piecewise linear recurrences*, to appear.

[5] Albert Nijenhuis and Herbert S. Wilf, *Representations of integers by linear forms in nonnegative integers.*, J. Number Theory **4** (1972), 98–106. MR 44 #5274

[6] Tiberiu Popoviciu, *Asupra unei probleme de patitie a numerelor*, Acad. Republicii Populare Romane, Filiala Cluj, Studii si cercetari stiintifice **4** (1953), 7–58.

[7] Sinan Sertoz, *On the number of solutions of the Diophantine equation of Frobenius*, Diskret. Mat. **10** (1998), no. 2, 62–71. MR 2000a:11049

[8] Jeffrey Shallit and Ming-Wei Wang, *Automatic complexity of strings*, J. Autom. Lang. Comb. **6** (2001), no. 4, 537–554, 2nd Workshop on Descriptional Complexity of Automata, Grammars and Related Structures (London, ON, 2000). MR 1 897 300

[9] J. J. Sylvester, *Mathematical questions with their solutions*, Educational Times **41** (1884), 171–178.

[10] Amitabha Tripathi, *The number of solutions to $ax + by = n$*, Fibonacci Quart. **38** (2000), no. 4, 290–293. MR 2001d:11036

Department of Mathematical Sciences
Binghamton University (SUNY)
Binghamton, NY 13902-6000
matthias@math.binghamton.edu

Department of Mathematics
Temple University
Philadelphia, PA 19122
srobins@math.temple.edu