EuroComb 2005 DMTCS proc. **AE**, 2005, 317–322

On the Frobenius' Problem of three numbers

Francesc Aguiló[1†] and Alícia Miralles[1‡]

[1] *Dept. Matemàtica Aplicada IV, UPC Barcelona*

Given k natural numbers $\{a_1, ..., a_k\} \subset \mathbb{N}$ with $1 \leq a_1 < a_2 < .. < a_k$ and $\gcd(a_1, ..., a_k) = 1$, let be $R(a_1, ..., a_k) = \{\lambda_1 a_1 + \cdots + \lambda_k a_k | \; \lambda_i \in \mathbb{N}, \; i = 1 \div k\}$ and $\overline{R}(a_1, ..., a_k) = \mathbb{N} \setminus R(a_1, ..., a_k)$. It is easy to see that $|\overline{R}(a_1, ..., a_k)| < \infty$. The *Frobenius Problem* related to the set $\{a_1, ..., a_k\}$ consists on the computation of $f(a_1, ..., a_k) = \max \overline{R}(a_1, ..., a_k)$, also called the *Frobenius number*, and the cardinal $|\overline{R}(a_1, ..., a_k)|$. The solution of the Frobenius Problem is the explicit computation of the set $\overline{R}(a_1, ..., a_k)$.

In some cases it is known a sharp upper bound for the Frobenius number. When $k = 3$ this bound is known to be

$$F(N) = \max_{\substack{0<a<b<N \\ \gcd(a,b,N)=1}} f(a, b, N) = \begin{cases} 2(\lfloor N/2 \rfloor - 1)^2 - 1 & \text{if } N \equiv 0 \pmod 2, \\ 2\lfloor N/2 \rfloor (\lfloor N/2 \rfloor - 1) - 1 & \text{if } N \equiv 1 \pmod 2. \end{cases}$$

This bound is given in [4].

In this work we give a geometrical proof of this bound which allows us to give the solution of the Frobenius problem for all the sets $\{\alpha, \beta, N\}$ such that $f(\alpha, \beta, N) = F(N)$.

Keywords: Frobenius problem, L-shaped tile, Smith normal form, Minimum Distance Diagram

1 Introduction

Given a set $A = \{a_1, ..., a_k\} \subset \mathbb{N}$ of different nonnegative integer values, we say that $m \in \mathbb{N}$ is *represented* by A if $m = \lambda_1 a_1 + \cdots + \lambda_k a_k$ with $\lambda_1, .., \lambda_k \in \mathbb{N}$. If $\gcd(a_1, ..., a_k) = 1$ it is easy to verify that there are only a finite number of values which can not be represented by A. We will denote by $R(A)$ the representable values, that is $R(a_1, ..., a_k) = \{\sum_{i=1}^{k} \lambda_i a_i | \; \lambda_i \in \mathbb{N} \; \forall i = 1 \div k\}$, we also denote by $\overline{R}(A) = \mathbb{N} \setminus R(A)$, that is all the non-representable values by the set A.

Definition 1 (Frobenius Number) Given $1 \leq a_1 < ... < a_k$ with $\gcd(a_1, ..., a_k) = 1$, the Frobenius number is known to be the value $f(a_1, ..., a_k) = \max \overline{R}(a_1, ..., a_k)$.

The solution to the so called *Frobenius Problem* is the (explicit) description of the set $\overline{R}(A)$. For instance, $\overline{R}(3, 5, 7) = \{1, 2, 4\}$ and so $f(3, 5, 7) = 4$. This problem is related to the *The Money Changing Problem*, where we have coins with values $a_1, ..., a_k$ only, hence we can not give change for the values in $\overline{R}(a_1, ..., a_k)$ and we can give change for any value greater than $f(a_1, ..., a_k)$. An efficient algorithm

†Supported by the Catalan Research Council under project 2001SGR00258.

‡Supported by the Comisión de Interministerial de Ciencia y Tecnología under project MCYT-TIC2002-00155

(suitable for being implemented in a pocket calculator) to compute the Frobenius number for any k can be found in [3]. A generic closed expression of the Frobenius number is known only for the case $k = 2$, $f(a_1, a_2) = a_1a_2 - a_1 - a_2$. There is no known a closed generic expression of this number for $k \geq 3$. An exhaustive compendium of known results on the Frobenius number can be found in [6].

In this work we use the metric information given by the L-shaped tiles to solve this problem in the case $k = 3$, for all the sets attaining the upper bound given by Dixmier in [4]. Hamidoune in [5] gave all the sets that attain this bound.

2 L-shaped Tiles

L-shaped tiles have been used to study several discrete problems, mainly in Graph Theory. Roughly speaking, these tiles give metrical information when we are not working with values but with equivalence classes in some $\mathbb{Z}_N$. We give an example from Graph Theory: a *double-loop* digraph $G(N; a, b) = G(V, A)$, $\gcd(a, b, N) = 1$, is defined by

$$\begin{aligned} V &= \mathbb{Z}_N = \{0, 1, ..., N-1\}, \\ A &= \{(i, i+a \pmod N), (i, i+b \pmod N) |\, i \in V\}. \end{aligned}$$

When we want to compute the diameter of $G = G(N; a, b)$, since G is vertex symmetric, we only want to find the distance of a vertex at maximum distance from 0. Then it is known that a *Minimum Distance Diagram* (MDD) of G is a plane shape which is similar to the (capital) letter L. This L-shaped periodically tessellates the plane. These diagrams minimize the (directed) distance $d(i, j) = i + j$ in the plane. Each vertex $v \equiv ia + jb \pmod N$ is represented by a unit square (i, j) at distance $d(i, j)$ from the square $(0, 0)$ (representing the vertex 0.) The digraph $G(9; 2, 5)$ and a related L-shaped tile is depicted in Figure 1.

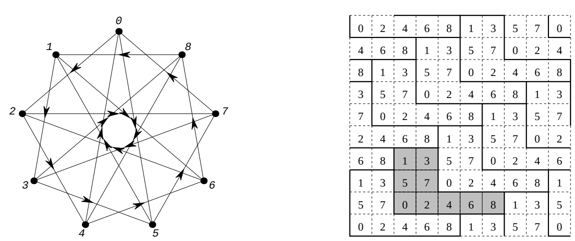

Fig. 1: $G(9; 2, 5)$ and one related plane tessellation

It can be shown that each digraph $G(N; a, b)$ has at most two different minimum distances diagrams. It has been shown that these diagrams are always L-shaped tiles. However it may be related L-shaped tiles which are not MDD. See [1] for more details. These tiles can be described by its dimensions, denoted by $L(l, h, w, y)$, as it is shown in Figure 2.

The main idea on controlling the values of $\overline{R}(a, b, N)$ is the following one:

- Think the values of $\mathbb{N}$ modulus N.
- The first time we represent an element m of some equivalent class $[m]$, then all the elements $n \geq m$ belonging to $[m]$ are also represented (adding some multiple of N).

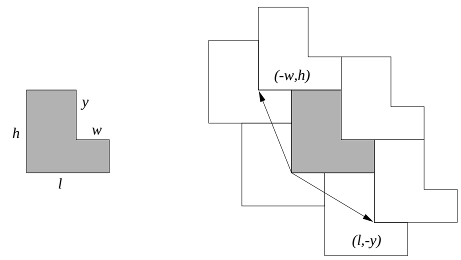

Fig. 2: Generic description of an L-shaped tile and its related tessellation

- The first time we have represented all the classes modulus N, say when we represent the value t, then we will be able to represent any value greater than t.

Here when we say the "first time", we want to mean at minimum distance from 0. Now the distance is given by $d(i,j) = ai + bj$ and each square (i,j) has been labelled by the value $ai + bj$, without doing modulus N. This distance give another kind of minimum distances diagrams. These kind of diagrams will be called *Minimum Distance Diagram of Elements* (not of equivalence classes), denoted by MDDE.

Hence, we have now two types of minimum distances diagrams: MDD and MDDE. The former controls the first time we represent the equivalent class (but possibly not the lower possible element in the class,) the latter controls the values of the elements (and also it controls the classes.) Let us see several examples which will clarify the strategy we want to take.

6	3		
8	5	2	9
0	7	4	1

16	23		
8	15	22	29
0	7	14	21

Fig. 3: Two different types of minimum distances diagrams for the set A_1

Let us consider the set $A_1 = \{7, 8, 10\}$. Two types of diagrams related to A_1, a MDD and a MDDE, are shown in the Figure 3. In this particular set A_1 these diagrams are essentially the same one (except for the additions modulus 10.) Now let us consider the MDDE. The values inside it are the first values of any equivalent class modulus 10 which can be represented by A_1. Hence the elements of the set $\overline{R}(7, 8, 10)$ are $\{1, 2, 3, 4, 5, 6, 9, 11, 12, 13, 19\}$. Note that the Frobenius number can be computed from the dimensions of the MDDE directly, without the previous computation of $\overline{R}(7, 8, 10)$: its dimensions are $L(4, 3, 2, 1)$, therefore we have

$$f(7, 8, 10) = \max\{23, 29\} - 10 = \max\{(l - w - 1)a + (h - 1)b, (l - 1)a + (h - y - 1)b\} - 10 = 19.$$

Note that this computation is true only if we work on the MDDE.

Let us consider now another example which will put some light on the possible difficulty for the direct computation of $f(a, b, N)$. Let us consider the set $A_2 = \{2, 9, 10\}$. A MDD modulus 10, the same MDD without doing modulus and the MDDE are shown respectively in Figure 4. We have $f(2, 9, 10) = 7$, computed from the MDDE. In this example, the metrical data given by the MDD can not been used for our purposes.

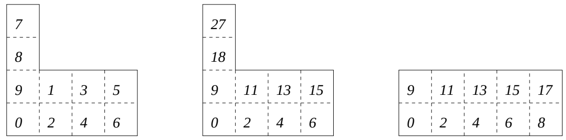

Fig. 4: Metrical data of A_2

¿From these examples we can note some important facts for a generic case: a MDD $L = L(l,h,w,y)$ related to a given set $A = \{a,b,N\}$ give the following upper bound for the Frobenius number of A

$$f(a,b,N) \leq g(L) := \max\{(l-w-1)a + (h-1)b, (l-1)a + (h-y-1)b\} - N. \tag{1}$$

The equality holds when the MDD L is a MDDE also. Fixed N, the area of the MDD L, then the value of this upper bound raises if the value $D(L)$ raises also.

3 Sharp Upper Bound

¿From the examples given in the previous section, we can note that the diameter of MDD play an important rôle in the study of the sharp upper bound $F(N)$. This section give the tools for computing this bound.

Theorem 1 (Sharp bounds for $D(L)$) Given a MDD $L = L(l,h,w,y)$, related to a set $\{a,b,N\}$ with $\gcd(a,b,N) = 1$, then $\left\lceil \sqrt{3N} \right\rceil - 2 = \text{lb}(N) \leq D(L) \leq \text{ub}(N) = \lfloor N/2 \rfloor$, where $D(L)$ is the diameter of L and these two bounds are sharp.

Given a double-loop digraph $G(N;a,b)$ and a related L-shaped tile $L(l,h,w,y)$ which periodically tessellates the plane (being MDD or not,) then the tile $L(h,l,y,w)$ is related to the digraph $G(N;b,a)$. In terms of sets and the Frobenius Problem the digraph $G(N;b,a)$ give the same metrical information (through its related MDDs) than $G(N;a,b)$. Therefore we can restrict our study to non considering these symmetrical L-shaped tiles. From now on, all the results will be stated modulus this symmetry.

Theorem 2 Let be $N = 2n$. Let L be a MDD related to the set $\{a,b,N\}$ of area N and diameter $D(L) = \text{ub}(N)$. Let be $L_1 = L(2, \text{ub}(N), 0, 1)$ and $L_2 = L(2, \text{ub}(N), 1, 0)$, related to the sets $\{N-2, N-1, N\}$ and $\{\text{ub}(N), N-1, N\}$ respectively. Then $f(a,b,N) \leq g(L_1) = g(L_2) = 2(\text{ub}(N)-1)^2 - 1$.

Theorem 3 Let be $N = 2n$. Let L be a MDDE of area N and $D(L) < \text{ub}(N)$, then $g(L) < g(L_1)$ where L_1 is the tile define in Theorem 2.

Theorem 4 Let be $N = 2n+1$. Let L be a MDD related to the set $\{a,b,N\}$ of area N and diameter $D(L) = \text{ub}(N)$. Let be $L_3 = L(2, \text{ub}(N)+1, 1, 1)$ related to the set $\{\text{ub}(N), N-1, N\}$. Then

$$f(a,b,N) \leq g(L_3) = 2\text{ub}(N)(\text{ub}(N)-1) - 1.$$

Theorem 5 Let be $N = 2n+1$. Let L be a MDDE of area N and $D(L) < \text{ub}(N)$, then $g(L) < g(L_3)$ where L_3 is the tile define in Theorem 4.

Lemma 1 The MDD L_1, L_2 and L_3 defined in theorems 2 and 4 are MDDE.

Theorem 6 Given $1 \leq a < b < N$, with $\gcd(a,b,N) = 1$, we have

$$f(a,b,N) \leq F(N) = \begin{cases} 2(\mathrm{ub}(N)-1)^2 - 1 & \text{if } N = 2n, \\ 2\mathrm{ub}(N)(\mathrm{ub}(N)-1) - 1 & \text{if } N = 2n+1. \end{cases}$$

These results show that $F(N)$ is a sharp upper bound for the Frobenius number of any set of three elements. Also it is shown that all the sets attaining this bound are $A_1 = \{N-2, N-1, N\}$, $A_2 = \{\mathrm{ub}(N), N-1, N\}$ for $N = 2n$ and $A_3 = \{\mathrm{ub}(N), N-1, N\}$ for $N = 2n+1$. The former result was published by Dixmier in [4], the later by Hamidoune in [5]. In any case they did not give the solution for these three sets.

4 Solution to Distinguished Sets

¿From the previous section we know that the MDDE giving the value $F(N)$ are $L_1 = L(2, \mathrm{ub}(N), 0, 1)$ related to $A_1 = \{N-2, N-1, N\}$ and $L_2 = L(2, \mathrm{ub}(N), 1, 0)$ related to $A_2 = \{\mathrm{ub}(N), N-1, N\}$ for $N = 2n$; and $L_3 = L(2, \mathrm{ub}(N)+1, 1, 1)$ related to the set $\{\mathrm{ub}(N), N-1, N\}$ for $N = 2n+1$. Now we will give the solution of the Frobenius Problem for these three sets.

Theorem 7 If $N = 2n$, then

$$\overline{R}(N-2, N-1, N) = \begin{cases} \{2\} & \text{if } N = 4, \\ \{N-3\} \cup \displaystyle\bigcup_{j=2}^{n-1} \left[\{j(N-2)-1\} \cup \bigcup_{s=1}^{j-1} \{sN-2j-1, sN-2j\} \right] & \text{if } N \geq 6. \end{cases}$$

Theorem 8 If $N = 2n$ and $A = \{n, N-1, N\}$, then

$$\overline{R}(A) = \begin{cases} \{1\} & \text{if } N = 4, \\ \displaystyle\bigcup_{j=2}^{n-1} \bigcup_{k=1}^{\left\lfloor \frac{j(N-1)-1}{N} \right\rfloor} \{(j-k)N - j\} \cup \bigcup_{j=1}^{n-1} \bigcup_{k=1}^{\left\lfloor \frac{j(N-1)+n-1}{N} \right\rfloor} \{(j-k)N + n - j\} & \text{if } N \geq 6. \end{cases}$$

Theorem 9 If $N = 2n+1$, then for $N \geq 5$ we have

$$\overline{R}(n, N-1, N) = \bigcup_{j=2}^{n} \bigcup_{k=1}^{\left\lfloor \frac{j(N-1)-1}{N} \right\rfloor} \{(j-k)N - j\} \cup \bigcup_{j=1}^{n-1} \bigcup_{k=1}^{\left\lfloor \frac{j(N-1)+n-1}{N} \right\rfloor} \{(j-k)N + n - j\}.$$

References

[1] F. Aguiló and A. Miralles, Implementable L-shaped tiles and the POMDIG process, submitted to *Discrete Math.*

[2] M. Beck, D. Einstein and S. Zacks, Some Experimental Results on the Frobenius Problem, *Experimental Mathematics* **12**:3 (2003) 263-269

[3] S. Böcker and Z. Lipták, The Money Changing Problem revisited: Computing the Frobenius number in time $O(ka_1)$, Technical Report no. 2004-2, Universität Bielefeld, Technische Fakultät

[4] J. Dixmier, Proof of a conjecture by Erdös and Graham concerning the problem of Frobenius, *J. Number Theory*, **34** (1990) 198-209

[5] Y.O. Hamidoune, On the Diophantine Frobenius Problem, *Potugaliae Mathematica* Vol. **55** Fasc. 4 (1998) 425-449

[6] J.L. Ramírez Alfonsín, *The Diophantine Frobenius Problem*, to be published.

[7] J-C Schlage-Puchta, An Estimate for Frobenius' Diophantine Problem in Three Dimensions, *J. Integer Sequences* Vol. **8** (2005) Article 05.1.7