MATH. SCAND. 94 (2004), 5–12

EVERY POSITIVE INTEGER IS THE FROBENIUS NUMBER OF A NUMERICAL SEMIGROUP WITH THREE GENERATORS

J. C. ROSALES, P. A. GARCÍA-SÁNCHEZ and J. I. GARCÍA-GARCÍA*

Introduction

Let $n_1, \dots, n_p$ be positive integers with greatest common divisor (gcd for short) one. Then it is not hard to show that there are finitely many nonnegative integers that cannot be expressed as a nonnegative integer linear combination of $n_1, \dots, n_p$. The largest nonnegative integer fulfilling this condition is usually known as the *Frobenius number* of $n_1, \dots, n_p$ and it will be denoted throughout this paper by $\mathrm{F}(n_1, \dots, n_p)$. The problem of determining $\mathrm{F}(n_1, \dots, n_p)$ appears in the literature as the Frobenius coin-exchange problem (for a complete survey on this problem see [5], [6]). For $p = 2$, Sylvester proved in [7] that $\mathrm{F}(n_1, n_2) = n_1 n_2 - n_1 - n_2$. No general formula has been found so far for the case $p \geq 3$. Moreover, as Curtis shows in [1], there is no closed formula of a certain type for $p = 3$. If we focus our attention on this case, then we can think of F as a correspondence that maps three relatively prime integers n_1, n_2, n_3 to a nonnegative integer $\mathrm{F}(n_1, n_2, n_3)$. In this paper we prove that this map is surjective, that is, for every positive integer g there exist positive integers n_1, n_2 and n_3 such that $\mathrm{F}(n_1, n_2, n_3) = g$ (Theorem 1.11). One easily realizes that every odd positive integer g can be expressed as $\mathrm{F}(2, g + 2)$ (see 1.1 (i)). However no even positive integers can be expressed as the Frobenius number associated to a pair of relatively prime numbers. This follows easily from Sylvester's formula given above, since this formula can be rewritten as $\mathrm{F}(n_1, n_2) = (n_1 - 1)(n_2 - 1) - 1$ and n_1, n_2 are coprime (in fact, it is well known that every numerical semigroup generated by two elements is symmetric, see for instance [2], [4], and thus its Frobenius number must be odd). Thus in order to express any nonnegative integer as the Frobenius number of a sequence of positive integers, the sequences used should be at least of length

* The authors thank J. M. Urbano-Blanco and J. L. Ramírez Alfonsín for their comments and suggestions.

Received November 20, 2002; in revised form September 26, 2003.

three, and what we show here is that this minimum is achieved.

The main result in this paper is Theorem 1.11 and the key to prove it is Proposition 1.9. However Proposition 1.9 leaves a finite number (some thousands) of cases unattended. At first, we checked these cases by using a Haskell script (see [3]) written by J. I. García-García. Then we proceeded to find a direct proof for this fact by sieving these cases. This is performed in the results labelled from 1.1 to 1.3 and collected in Proposition 1.4. Thus Theorem 1.11 simply glues Propositions 1.4 and 1.9 together.

1. Main result

Let $n_1, \dots, n_p$ be positive integers such that $\gcd\{n_1, \dots, n_p\} = 1$. Let

$$S = \langle n_1, \dots, n_p \rangle = \{a_1 n_1 + \dots + a_p n_p \mid a_1, \dots, a_p \in \mathsf{N}\}.$$

Then S is a numerical semigroup, that is, S is closed under addition, $0 \in S$ and $\mathsf{N} \setminus S$ has finitely many elements. Note that $\mathrm{F}(n_1, \dots, n_p)$ is the largest integer not belonging to S.

For $n \in S \setminus \{0\}$, the *Apéry set* of n in S is the set

$$\mathrm{Ap}(S, n) = \{x \in S \mid x - n \notin S\}.$$

Clearly $\mathrm{Ap}(S, n) = \{0, w(1), \dots, w(n-1)\}$ where for all $i \in \{1, \dots, n-1\}$, $w(i)$ is the least integer in S congruent with i modulo n. It is well known and easy to prove that $\mathrm{F}(n_1, \dots, n_p) = (\max \mathrm{Ap}(S, n)) - n$.

LEMMA 1.1. *Let g be a positive integer.*

(i) *If g is odd, then* $\mathrm{F}(2, g+2) = g$.

(ii) *If* $3 \not| \, g$, *then* $\mathrm{F}(3, a, b) = g$, *where* $\{a, b\} = \{x \in \{g+1, g+2, g+3\} \mid 3 \not| \, x\}$.

(iii) *If g is even and* $4 \not| \, g$, *then* $\mathrm{F}(4, g/2+2, g/2+4) = g$.

PROOF. (i) Follows from the well known formula $\mathrm{F}(a, b) = ab - a - b$.

(ii) Clearly $\langle 3, a, b \rangle = \langle 3, g+1, g+2, g+3 \rangle$. Thus

$$\mathrm{F}(3, a, b) = \mathrm{F}(3, g+1, g+2, g+3) = g.$$

(iii) Let $S = \langle 4, g/2+2, g/2+4 \rangle$. If we show that $\mathrm{Ap}(S, 4) = \{0, g/2+2, g/2+4, g+4\}$, then we are done since $\mathrm{F}(4, g/2+2, g/2+4) = (\max \mathrm{Ap}(S, 4)) - 4$. As $g/2+2$, $g/2+4$ and $g+4$ belong to S, it suffices to demonstrate that none of the integers $g/2+2-4$, $g/2+4-4$, $g+4-4$ is in S.

- If $g/2-2 \in S$, then it must be a multiple of 4 and thus $g/2$ is a multiple of 2, whence g is a multiple of 4, in contradiction with the hypothesis.
- If $g/2 \in S$, then arguing as above we obtain that g must be a multiple of 4, which is absurd.
- If $g \in S$, then $g = a_1 4 + a_2(g/2+2) + a_3(g/2+4)$ for some nonnegative integers a_1, a_2, a_3. Observe that this implies that $0 < a_2 + a_3$ (g is not a multiple of 4) and $a_2 + a_3 \leq 1$. Hence either $g = a_1 4 + (g/2+2)$ or $g = a_1 4 + (g/2+4)$. In both cases we get that $g/2$ is even, contradicting once more that g is not a multiple of 4.

PROPOSITION 1.2. *Let g be a positive integer. If there exists a positive integer m such that* $\gcd(m, g) = 1$, $m-1 \mid g$ *and* $m(m-1)(m-3) < g$, *then there exist* n_1, n_2, n_3 *such that* $\mathrm{F}(n_1, n_2, n_3) = g$.

PROOF. Let $S = \langle m, g/(m-1)+m, g+m\rangle$. We prove that

$$\mathrm{Ap}(S, m) = \left\{0, \frac{g}{m-1}+m, \ldots, (m-2)\left(\frac{g}{m-1}+m\right), g+m\right\}.$$

It is clear that if n_1 and n_2 are positive integers such that $\gcd(n_1, n_2) = 1$, then

$$\mathrm{Ap}(\langle n_1, n_2\rangle, n_1) = \{0, n_2, 2n_2, \ldots, (n_1-1)n_2\}.$$

So, by setting $n_1 = m$ and $n_2 = g/(m-1)+m$, we have that

$$\mathrm{Ap}\left(\left\langle m, \frac{g}{m-1}+m\right\rangle, m\right) = \left\{0, \frac{g}{m-1}+m, \ldots, (m-1)\left(\frac{g}{m-1}+m\right)\right\}.$$

Since $(m-2)(g/(m-1)+m) < g+m$ whenever $m(m-1)(m-3) < g$, we have that $\{0, g/(m-1)+m, \ldots, (m-2)(g/(m-1)+m)\} \subset \mathrm{Ap}(S, m)$. Note also that $(m-1)(g/(m-1)+m) \equiv g+m \pmod{m}$ and that $(m-1)(g/(m-1)+m) \geq g+m$, which means that $g+m$ must be in $\mathrm{Ap}(S, m)$. Therefore

$$\mathrm{Ap}(S, m) = \left\{0, \frac{g}{m-1}+m, \ldots, (m-2)\left(\frac{g}{m-1}+m\right), g+m\right\}.$$

Since $(m-2)(g/(m-1)+m) < g+m$, we have that $(\max \mathrm{Ap}(S, m)) - m = g+m-m = g$.

COROLLARY 1.3. *Let g be a positive integer that is not a multiple of 5, 7 or 11. Then there exist positive integers* n_1, n_2, n_3 *such that* $\mathrm{F}(n_1, n_2, n_3) = g$.

PROOF. Assume that $5 \nmid g$. From Lemma 1.1 (iii), we can assume that $4 \mid g$. By applying Proposition 1.2 it suffices to prove the statement for $g \leq 5 \times 4 \times 2 = 40$. In view of Lemma 1.1 we can also assume that $3 \mid g$. Thus the only possible values left for g are multiples of 12 less than or equal to 40, that is, $g \in \{12, 24, 36\}$. Since $\mathrm{F}(5, 8, 9) = 12$, $\mathrm{F}(5, 11, 18) = 24$ and $\mathrm{F}(5, 14, 27) = 36$, we are done.

Now we study the case $7 \nmid g$ and $5 \mid g$. By using Lemma 1.1, we can assume that $3 \times 4 \times 5 = 60 \mid g$. In particular $6 \mid g$, which allows us to apply Proposition 1.2, whence arguing as above it suffices to prove the statement for $g \leq 7 \times 6 \times 4 = 168$. As g is a multiple of 60, the only possible values left for g are $g = 60$ and $g = 120$. Since $\mathrm{F}(7, 17, 33) = 60$, and $\mathrm{F}(7, 27, 73) = 120$, these two cases are also covered.

Finally, suppose that $11 \nmid g$, and that 5 and 7 divide g. By using this together with Lemma 1.1, we can assume that $3 \times 4 \times 5 \times 7 = 420 \mid g$, whence $10 \mid g$. By Proposition 1.2 we can restrict ourselves to $g \leq 11 \times 10 \times 8 = 880$. Since g is a multiple of 420, it suffices to check that the cases $g \in \{420, 840\}$. We conclude the proof by pointing out that $\mathrm{F}(8, 107, 109) = 420$ and $\mathrm{F}(9, 143, 353) = 840$.

PROPOSITION 1.4. *If g is a positive integer such that $g < 4620$, then there exist positive integers n_1, n_2, n_3 such that* $\mathrm{F}(n_1, n_2, n_3) = g$.

PROOF. Note that $3 \times 4 \times 5 \times 7 \times 11 = 4620$. Hence if $g < 4620$ there exists $p \in \{3, 4, 5, 7, 11\}$ such that $p \nmid g$. According to the value of p, by applying one of the results presented so far we conclude in any case that there exists n_1, n_2, n_3 such that $\mathrm{F}(n_1, n_2, n_3) = g$.

Given a finite set A of integers, as usual, lcm A will denote the least common multiple of them.

LEMMA 1.5. *Let g be a positive integer and let m be the least positive integer such that $m \nmid g$. Then*

(i) *m is the power of a prime,*

(ii) *if* $\gcd(m, g) = k$, *then* $\gcd(m, (g + m)/k) = 1$.

PROOF.

(i) If m is not a power of a prime, then $m = pq$ with $\gcd(p, q) = 1$ and $p \neq 1 \neq q$. As $p < m$ and $q < m$ we have that both p and q divide g, whence $m = \mathrm{lcm}\{p, q\} = pq$ also divides g, in contradiction to the hypothesis.

(ii) Assume that $g = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ for some primes $p_1, \ldots, p_r$ and positive integers $\alpha_1, \ldots, \alpha_r$. By (i), we deduce that either m is a prime not in $\{p_1, \ldots, p_r\}$ or $m = p_i^{\alpha_i + 1}$ for some $i \in \{1, \ldots, r\}$. Clearly if m is a prime not in $\{p_1, \dots, p_r\}$, then $k = \gcd(m, g) = 1$ and

$$\gcd(m, (g+m)/k) = \gcd(m, g+m) = \gcd(m, g) = 1.$$

If $m = p_i^{\alpha_i+1}$, for some $i \in \{1, \dots, r\}$, then $k = \gcd(m, g) = p_i^{\alpha_i}$ and $\gcd(m, (g+m)/k) = \gcd(p_i^{\alpha_i+1}, p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_r^{\alpha_r} + p_i) = 1.$

LEMMA 1.6. *Let $a, b, m, k, s, t \in \mathbb{N}$ be such that* $\gcd(a, m) = 1$ *and* $a + b = km$. *Then* $ta \equiv sb (\operatorname{mod} m)$ *if and only if* $t + s \equiv 0 (\operatorname{mod} m)$.

PROOF. Note that $ta \equiv sb \equiv s(km - a) \equiv -sa (\operatorname{mod} m)$, whence $ta \equiv sb (\operatorname{mod} m)$ if and only if $(t + s)a \equiv 0 (\operatorname{mod} m)$ and this is equivalent to $t + s \equiv 0 (\operatorname{mod} m)$.

LEMMA 1.7. *Let S be a numerical semigroup generated by $\{m, a, tm - a\}$ for some positive integers m, a, t such that* $\gcd(m, a) = 1$ *and $tm - a > m$. Then*

$$\operatorname{Ap}(S, m) = \{0, a, 2a, \dots, \lambda a, tm - a, 2(tm - a), \dots, \mu(tm - a)\},$$

for some λ, μ such that $\lambda + \mu = m - 1$.

PROOF. If $x \in \operatorname{Ap}(S, m)$, then $x \in S$ and $x - m \notin S$. Hence $x = \lambda a + \mu(tm - a)$ for some nonnegative integers λ and μ. If both λ and μ are not equal to zero, then $x = (a + tm - a) + (\lambda - 1)a + (\mu - 1)(tm - a) = tm + (\lambda - 1)a + (\mu - 1)(tm - a)$, contradicting that $x \in \operatorname{Ap}(S, m)$. Hence either λ or μ are equal to zero, meaning that either x is a multiple of a or x is a multiple of $tm - a$. The rest of the proof follows by taking into account that $\operatorname{Ap}(S, m)$ has exactly $m - 1$ nonzero elements.

LEMMA 1.8. *Let S be a numerical semigroup and let n be a nonzero element of S. If s, t are elements in S such that $s + t \in \operatorname{Ap}(S, n)$, then $s, t \in \operatorname{Ap}(S, n)$.*

PROOF. Trivial.

PROPOSITION 1.9. *Let g be a positive integer, let m be the least positive integer such that $m \nmid g$ and set $k = \gcd(m, g)$. If $m(m-k)(m-k-1) < g+m$, then there exist n_1, n_2, n_3 such that $\mathrm{F}(n_1, n_2, n_3) = g$.*

PROOF. By Lemma 1.5 we know that $\gcd(m, (g+m)/k) = 1$. Let

$$S = \left\langle m, \frac{g+m}{k}, \left\lceil \frac{g+m}{k(m-k)} \right\rceil m - \frac{g+m}{k} \right\rangle.$$

From Lemma 1.7 (from the hypothesis, it can be deduced that the condition $tm - a > m$ holds) we deduce that

$$\begin{aligned}\operatorname{Ap}(S,m) = \Big\{0, \frac{g+m}{k}, \dots, \lambda\frac{g+m}{k},\\ \left\lceil\frac{g+m}{k(m-k)}\right\rceil m - \frac{g+m}{k}, \dots, \mu\left(\left\lceil\frac{g+m}{k(m-k)}\right\rceil m - \frac{g+m}{k}\right)\Big\},\end{aligned}$$

for some $\lambda, \mu \in \mathsf{N}$ such that $\lambda + \mu = m - 1$. Thus we only have to find the exact values for λ and μ.

In view of Lemma 1.6, $k\frac{g+m}{k} \in \operatorname{Ap}(S,m)$ if $k\frac{g+m}{k} \le (m-k)\big(\lceil\frac{g+m}{k(m-k)}\rceil m - \frac{g+m}{k}\big)$, and this holds since $k\frac{g+m}{k} = (m-k)\big(\frac{g+m}{k(m-k)}m - \frac{g+m}{k}\big)$. Hence $k\frac{g+m}{k} = g + m \in \operatorname{Ap}(S,m)$. By Lemma 1.8, $\big\{0, \frac{g+m}{k}, \dots, (k-1)\frac{g+m}{k}, g+m\big\} \subseteq \operatorname{Ap}(S,m)$. Using the same argument, $(m-k-1)\big(\lceil\frac{g+m}{k(m-k)}\rceil m - \frac{g+m}{k}\big) \in \operatorname{Ap}(S,m)$ if $(m-k-1)\big(\lceil\frac{g+m}{k(m-k)}\rceil m - \frac{g+m}{k}\big)$ is less than or equal to $(k+1)\frac{g+m}{k}$. But

$$\begin{aligned}(1)\quad (m-k-1)&\left(\left\lceil\frac{g+m}{k(m-k)}\right\rceil m - \frac{g+m}{k}\right)\\ &\le (m-k-1)\left(\left(\frac{g+m}{k(m-k)}+1\right)m - \frac{g+m}{k}\right)\\ &\le g+m \le (k+1)\frac{g+m}{k},\end{aligned}$$

and thus $(m-k-1)\big(\lceil\frac{g+m}{k(m-k)}\rceil m - \frac{g+m}{k}\big) \in \operatorname{Ap}(S,m)$. Applying once more Lemma 1.8, we obtain that $\big\{0, \lceil\frac{g+m}{k(m-k)}\rceil m - \frac{g+m}{k}, \dots, (m-k-1)\big(\lceil\frac{g+m}{k(m-k)}\rceil m - \frac{g+m}{k}\big)\big\} \subseteq \operatorname{Ap}(S,m)$. Since $k + (m-k-1) = m - 1$, we have that

$$\begin{aligned}\operatorname{Ap}(S,m) = \Big\{0, \frac{g+m}{k}, \dots, k\frac{g+m}{k} = g+m,\\ \left\lceil\frac{g+m}{k(m-k)}\right\rceil m - \frac{g+m}{k}, \dots, (m-k-1)\left(\left\lceil\frac{g+m}{k(m-k)}\right\rceil m - \frac{g+m}{k}\right)\Big\}.\end{aligned}$$

By (1), we have that $\max \operatorname{Ap}(S,m) = g + m$ and therefore

$$\mathrm{F}\left(m, \frac{g+m}{k}, \left\lceil\frac{g+m}{k(m-k)}\right\rceil m - \frac{g+m}{k}\right) = g + m - m = g.$$

Lemma 1.10. *Let g be a positive integer and let m be the least positive integer such that $m \not| g$. If $m \ge 13$, then $m(m-1)(m-2) < g$.*

PROOF. Since g is a multiple of $m-4$, $m-3$, $m-2$ and $m-1$, we have that

$$g \geq \operatorname{lcm}\{m-1, m-2, m-3, m-4\}.$$

Assume that $p_1 = 2 < p_2 = 3 < p_3 < \cdots < p_r$ are primes such that

$$\operatorname{lcm}\{m-1, m-2, m-3, m-4\} = p_1^{e_1} \cdots p_r^{e_r}$$

and

$$(m-1)(m-2)(m-3)(m-4) = p_1^{f_1} \cdots p_r^{f_r}$$

for some nonnegative integers $e_1, \ldots, e_r, f_1, \ldots, f_r$. If p is a prime greater than 4 then it can divide at most one element in $\{m-1, m-2, m-3, m-4\}$ and thus from the definition of lcm we deduce that $e_i = f_i$ for $i \geq 3$. Note also that in the set $\{m-1, m-2, m-3, m-4\}$ there are always two even numbers and one of them is divisible by 4. This means that $e_1 = f_1 - 1$. Moreover, there are at most two elements in $\{m-1, m-2, m-3, m-4\}$ that can be divided by 3 (and at most one of them is divisible by 9). This leads to either $e_2 = f_2$ or $e_2 = f_2 - 1$. In any case

$$\operatorname{lcm}\{(m-1), (m-2), (m-3), (m-4)\} \geq ((m-1)(m-2)(m-3)(m-4))/6.$$

Now, $((m-1)(m-2)(m-3)(m-4))/6 > m(m-1)(m-2)$ if and only if $6m < (m-3)(m-4)$, or equivalently $m^2 - 13m + 12 = (m-1)(m-12) > 0$. This in particular implies that $g > m(m-1)(m-2)$ for $m \geq 13$.

THEOREM 1.11. *Let g be a positive integer. Then there exist positive integers n_1, n_2, n_3 such that*

$$\mathrm{F}(n_1, n_2, n_3) = g.$$

PROOF. Let m be the least positive integer such that $m \nmid g$. If $m(m-1)(m-2) < g$, by Proposition 1.9 we deduce that there exist n_1, n_2, n_3 for which $\mathrm{F}(n_1, n_2, n_3) = g$. If to the contrary $m(m-1)(m-2) \geq g$, then by Lemma 1.10, $m \leq 12$ and thus $g \leq 12 \times 11 \times 10 = 1320 < 4620$. From Proposition 1.4 we obtain the desired result.

REFERENCES

1. Curtis, F., *On formulas for the Frobenius number of a numerical semigroup*, Math. Scand. 67 (1990), 190–192.
2. Fröberg, R., Gottlieb, C., and Häggkvist, R., *On numerical semigroups*, Semigroup Forum 35 (1987), 63–83.
3. www.haskell.org
4. Herzog, J., *Generators and relations of abelian semigroups and semigroup rings*, Manuscripta Math. 3 (1970), 175–193.

5. Ramírez Alfonsín, J. L., *The Diophantine Frobenius problem*, Forschungsintitut für Diskrete Mathematik, Bonn, Report N0. 00893 (43 pages, 2000).
6. Ramírez Alfonsín, J. L., *The Diophantine Frobenius problem*, manuscript 180 pages (2003), submitted.
7. Sylvester, J. J., *Mathematical questions with their solutions*, Educational Times 41 (1884), 21.

DEPARTAMENTO DE ÁLGEBRA
UNIVERSIDAD DE GRANADA
E-18071 GRANADA
SPAIN
E-mail: jrosales@ugr.es, pedro@ugr.es, jigg@ugr.es