Gaps in Semigroups

J.L. Ramírez Alfonsín*
Université Pierre et Marie Curie, Paris 6,
Equipe Combinatoire - Case 189,
4 Place Jussieu Paris 75252 Cedex 05, France.

Abstract

In this paper we investigate the behaviour of the *gaps* in numerical semigroups. We will give an explicit formula for the i^{th} gap of a semigroup generated by $k+1$ consecutive integers (generalizing a result due to Brauer) as well as for a special semigroup of three generators. It is also proved that the number of gaps of the semigroup $< p, q >$ in the interval $[pq-(k+1)(p+q), \ldots, pq-k(p+q)]$ is equals to

$2(k+1)+\left\lfloor \frac{kq}{p} \right\rfloor + \left\lfloor \frac{kp}{q} \right\rfloor$ for each $k = 1, \ldots, \left\lfloor \frac{pq}{p+q} \right\rfloor$. We actually give two

proofs of the latter result, the first one uses the so-called *Apery sets* and the second one is an application of the well-known *Pick's theorem.*

Keywords Semigroups, gaps, Frobenius number
AMS Mathematics Subject Classification: 11B25, 11B75

1 Introduction

Let $s_1, \ldots, s_n$ be positive integers such that their greatest common divisor, denoted by $(s_1, \ldots, s_n)$, is one. Let $S =< s_1, \ldots, s_n >$ be the numerical

*e-mail: ramirez@math.jussieu.fr

semigroup[1] generated by $s_1, \ldots, s_n$. The *genus* of a numerical semigroup S is the number $N(S) = \#(\mathbb{N}^+ \cup \{0\} \setminus S)$. The positive elements of S (resp. elements of $\mathbb{N}^+ \cup \{0\} \setminus S$) are called the *non-gaps* (resp. *gaps*) of S. One motivation to study gaps comes from the important role they play in the concept of *symmetry* [3] as well as in the investigations of *Weierstrass* semigroups [5, 6, 8] and its applications to *algebraic codes* [9].

In 1882, while investigating the *partition number* function, J.J. Sylvester [15, page 134] (see also [14]) proved that if $S_{pq} =< p, q >$ with $(p, q) = 1$ then

$$N(S_{pq}) = \frac{1}{2}(p-1)(q-1) \tag{1}$$

The so-called *Frobenius number*[2] denoted by $g(S) = g(s_1, \ldots, s_n)$, is the largest integer not belonging to S ($g(S)$ is also known as the *conductor* of S). From equation (1) it can be deduced that

$$g(S_{pq}) = pq - p - q. \tag{2}$$

Finding $g(S)$ is a difficult problem from the computational point of view, in general [11]. There exist numerous bounds (and formulas for particular semigroups S) for $g(S)$ as well as generalizations and applications of it. We refer the reader to [12] for a detailed discussion on the Frobenius number.

Let us enumerate the gaps of S by increasing order $l_1 < \cdots < l_{N(S)}$. So, $l_{N(S)} = g(S)$ is both the *largest gap* of S as the $N(S)^{th}$ gap. Not surprisingly, computing the i^{th} gap of a semigroup is also difficult since it comes down to calculate the Frobenius number. Indeed, for calculating the i^{th} gap of a semigroup S we may calculate $g^{N(S)-i}(S) = g(S \cup \{g^{N(S)}(S)\} \cup \cdots \cup \{g^{N(S)-i+1}(S)\})$ where $g^{N(S)}(S) = g(S)$. There is not much known about the

[1]Recall that a *semigroup* $(S, *)$ consists of a nonempty set S and an associative binary operation $*$ on S. If, in addition, there exists an element, which is usually denoted by 0, in S such that $a * 0 = 0 * a = a$ for all $a \in S$, we say that $(S, *)$ is a *monoid*. A *numerical semigroup* is a submonoid of $(\mathbb{N}, +)$ such that the greatest common divisor of its elements is equal to one.

[2]In the introduction section of [1], A. Brauer stated that G. Frobenius mentioned, occasionally in his lectures, the problem of finding the largest natural number that is not representable as a nonnegative integer combination of $s_1, \ldots, s_n$.

behaviour of the gaps in semigroups. The main intention of this paper is to investigate the distribution of gaps in some semigroups. In the next section, we prove the following two theorems.

Theorem 1.1 *Let $a, k \geq 1$ be integers and let $S =< a, a+1, \ldots, a+k >$ be a semigroup with gaps $l_1 < \cdots < l_{N(S)}$. Let $v_m = (m+1)(a-1) - k\left(\frac{m(m+1)}{2}\right)$,*

$v_{-1} = 0$ and $r = \left\lfloor \frac{a-2}{k} \right\rfloor$. Then,

$$N(S) = v_r \text{ and } l_i = t_i(a+k) + i - v_{t_i - 1}$$

for each $i = 1, \ldots, N(S)$ where t_i is the smallest integer such that $v_{t_i} \geq i$.

In [1], Brauer found a formula for the Frobenius number of $k+1$ consecutive positive integers, this is given by

$$g(a, a+1, \ldots, a+k) = a\left(\left\lfloor \frac{a-2}{k} \right\rfloor + 1\right) - 1.$$

We remark that Theorem 1.1 contains Brauer's result as a particular case. Indeed, since $v_r = v_{r-1} + a - (rk+1)$ and $t_{N(S)} = r$ then

$$\begin{aligned} l_{N(S)} &= r(a+k) + N(S) - v_{r-1} = r(a+k) + v_r - (v_r + rk + 1 - a) \\ &= r(a+k) + a - 1 - kr = a(r+1) - 1 = a\left(\left\lfloor \frac{a-2}{k} \right\rfloor + 1\right) - 1. \end{aligned}$$

Theorem 1.1 yields us to consider the following question.

Question: Let $S =< a, a+d, \ldots, a+kd >$ with $d \geq 1$ and $gcd(a, d) = 1$. Is there a formula that computes the i^{th} gap of S for each $1 \leq i \leq N(S)$?

A positive answer to the above question is obtained when $i = N(S)$ since, for any integer d, it is known [13] that

$$l_{N(S)} = g(a, a+d, \ldots, a+kd) = a\left(\left\lfloor \frac{a-2}{k} \right\rfloor\right) + d(a-1). \qquad (3)$$

The following Theorem answers this question when $k = 2$ and $d = a - 1$.

Theorem 1.2 *Let $a \geq 1$ be an integer and let $S =< a, 2a-1, 3a-2 >$ be a semigroup with gaps $l_1 < \cdots < l_{N(S)}$. Let*

$$r = (r_0, r_1, \ldots, r_{3n-2}) = (0, 2n-1, 2n-2, 2n-3, 2n-3, 2n-4, 2n-5, 2n-5, 2n-6, \ldots, 2, 1, 1)$$

and

$$r' = (r'_0, r'_1, \ldots, r'_{3n-1}) = (0, 2n, 2n-1, 2n-2, 2n-2, 2n-3, 2n-4, 2n-4, 2n-5, \ldots, 2, 2, 1).$$

We set $v_m = \sum_{i=0}^{m} r_i$ and $v'_m = \sum_{i=0}^{m} r'_i$. Then,

$$N(S) = \begin{cases} \frac{3}{4}n^2 - \frac{3}{2}n + 1 & \textit{if } a = 2n,\ n \geq 1, \\ \frac{3}{4}(n^2 - 2n + 1) & \textit{if } a = 2n+1,\ n \geq 1, \end{cases}$$

and

$$l_i = \begin{cases} (t_i - 1)2n + i - v_{t_i - 1} & \textit{if } a = 2n,\ n \geq 1, \\ (t_i - 1)(2n+1) + i - v'_{t_i - 1} & \textit{if } a = 2n+1,\ n \geq 1, \end{cases}$$

where t_i is the smallest integer such that $v_{t_i} \geq i$ if $a = 2n$ (or $v'_{t_i} \geq i$ if $a = 2n + 1$).

We notice that Theorem 1.2 contains equality (3) when $k = 2$ and $d = a - 1$. Indeed, equation (3) implies that if $a = 2n$, $n \geq 1$ then

$$
\begin{aligned}
g(a, 2a-1, 3a-2) &= a\left(\left\lfloor \tfrac{a-2}{2} \right\rfloor\right) + (a-1)^2 \\
&= 2n\left(\left\lfloor \tfrac{2n-2}{2} \right\rfloor\right) + (2n-1)^2 \\
&= 2n(n-1) + (2n-1)^2 \\
&= 6n^2 - 6n + 1 = 6n(n-1) + 1
\end{aligned}
$$

and $a = 2n + 1$, $n \geq 1$ then

$$
\begin{aligned}
g(a, 2a-1, 3a-2) &= a\left(\left\lfloor \tfrac{a-2}{2} \right\rfloor\right) + (a-1)^2 \\
&= (2n+1)\left(\left\lfloor \tfrac{2n+1-2}{2} \right\rfloor\right) + (2n)^2 \\
&= (2n+1)(n-1) + 4n^2 \\
&= 6n^2 - n - 1 = n(6n-1) - 1.
\end{aligned}
$$

On other hand, by Theorem 1.2, we have that.
(a) If $a = 2n$, $n \geq 1$ then $t_{N(S)} = 3n - 2$, $N(S) = v_{3n-2}$ and $v_{3n-2} = v_{3n-3} + r_{3n-1} = v_{3n-3} + 1$. So,

$$
\begin{aligned}
l_{N(S)} &= (3n-3)2n + N(S) - v_{3n-2-1} \\
&= (3n-3)2n + v_{3n-2} - (v_{3n-2} - 1) \\
&= 6n^2 - 6n + 1 = 6n(n-1) + 1.
\end{aligned}
$$

(b) If $a = 2n + 1$, $n \geq 1$ then $t_{N(S)} = 3n - 1, N(S) = v_{3n-1}$ and $v'_{3n-1} = v'_{3n-2} + r'_{3n-1} = v'_{3n-2} + 1$. So,

$$
\begin{aligned}
l_{N(S)} &= (3n-2)(2n+1) + N(S) - v'_{3n-1-1} \\
&= (3n-2)(2n+1) + v_{3n-1} - (v'_{3n-1} - 1) \\
&= 6n^2 - 4n + 3n - 2 + 1 = n(6n+1) - 1.
\end{aligned}
$$

In this paper, we also study the gaps of semigroups with two generators.

Theorem 1.3 *Let p, q positive integers such that $g.c.d.(p,q) = 1$. Let $g_k(S_{pq})$ be the number of gaps of $S_{pq} =< p, q >$ in the interval*

$$[pq - (k+1)(p+q), \ldots, pq - k(p+q)],$$

for each $0 \le k \le \left\lfloor \frac{pq}{p+q} \right\rfloor - 1$. Then,

$$g_k(S_{pq}) = \begin{cases} 1 & \text{if } k = 0 \\ 2(k+1) + \left\lfloor \frac{kq}{p} \right\rfloor + \left\lfloor \frac{kp}{q} \right\rfloor & \text{if } 1 \le k \le \left\lfloor \frac{pq}{p+q} \right\rfloor - 1. \end{cases}$$

In Section 3, we give two proofs of Theorem 1.3, the first one uses the notions of *Apery* set and the second one the well-known *Pick's theorem.* These algebraic and geometric proofs may motivate further investigations on the study of gaps of semigroups with $n \ge 4$. We remark that Theorem 1.3 can be regarded as a generalization, to some extent, of equation (2) contained when $k = 0$ (an arithmetical and an algebraic proofs of equation (2) are given in [7] and [2] respectively).

2 Arithmetic sequences

We may now prove Theorems 1.1 and 1.2.

Proof of Theorem 1.1. Let $S_i = \{i(a+k)+1, \ldots, (i+1)a - 1\}$ for each $i = 0, \ldots, r = \left\lfloor \frac{a-2}{k} \right\rfloor$. So, $|S_i| = a - (ik+1)$. We shall prove, by induction on i, that if $s \in S_i$ then $s \notin S$. It is clear for $i = 0$ since $S_0 = \{1, \ldots, a-1\}$. Let us suppose that it is true for $i = m \le r - 1$ and let $s \in S_{m+1}$. Notice that $s \in S$ if and only if $s - (a+j) \in S$ for some $0 \le j \le k$. So, if we show that $s - (a+j) \in S_m$ for all $0 \le j \le k$ then, by the inductive hypothesis, $s \notin S$. To this end, it can be easily checked that

$$m(a+k) + 1 \le s - (a+j) = (m+1)(a+k) + l - (a+j) \le (m+1)a - 1$$

for all $1 \leq l \leq a - (k(m+1)+1)$ and all $0 \leq j \leq k$ with equality on the left-hand side when $l = 1$ and $j = k$ and equality on the right-hand side when $l = a - (k(m+1)+1)$ and $j = 0$.

Now, we claim that if $t \notin S_i$ for all $i = 0, \ldots, r = \left\lfloor \frac{a-2}{k} \right\rfloor$ then $t \in S$.

For this, we consider the sets $T_i = \{(i+1)a, \ldots, (i+1)(a+k)\}$ for each

$i = 0, \ldots, r = \left\lfloor \frac{a-2}{k} \right\rfloor$ and $T_{r+1} = \{x | x \geq (r+1)(a+k)+1\}$. We show, by induction on i, that if $t \in T_i$ for some i then $t \in S$. This is clear for $i = 0$ since $T_0 = \{a, \ldots, a+k\}$. Now, suppose that it is true for $i = m-1 \leq r-1$. Then, by inductive hypothesis, all elements in

$$T_{m-1} = \{ma, \ldots, ma + mk = m(a+k)\}$$

belong to S. So, all elements in $A = \{x + a | x \in T_{m-1}\}$ also belong to S. Moreover, all elements in $B = \{m(a+k)+a+1, m(a+k)+a+2, \ldots, m(a+k)+a+k\}$ also belong to S since $m(a+k)$ belong to T_m. Hence, all the elements in

$$\begin{aligned} T_m &= \{(m+1)a, \ldots, (m+1)(a+k)\} = \{ma + a, \ldots, m(a+k) + a + k\} \\ &= \{ma + a, \ldots, ma + a + mk = m(a+k) + a, m(a+k) + a + 1, \ldots, m(a+k) + a + k\} \\ &= A \cup B \end{aligned}$$

belong to S. Finally, note that

$$|T_r| = |T_{\left\lfloor \frac{a-2}{k} \right\rfloor}| = \left(\left\lfloor \frac{a-2}{k} \right\rfloor + 1 \right) k + 1 \geq a.$$

So, T_r contains a consecutive elements forming a complete system modulo a, that is, T_r contain elements $t(0), \ldots, t(a-1)$ such that $t(i) \equiv i \bmod a$. It is clear if $t \in T_{r+1}$ then $t = t(i) + la$ with $l \geq 0$ integer and where $t \equiv i \bmod a$.

Thus, the set of all gaps in S is given by $\{S_i\}_{0\leq i\leq r}$. So,

$$N(S)=\sum_{i=0}^{r}|S_i|=a-(ik+1)=(r+1)(a-1)-k\left(\frac{r(r+1)}{2}\right)$$

and

$$l_i=t_i(a+k)+i-v_{t_i-1}$$

for each $i=1,\ldots,N(S)$ where t_i is the smallest integer such that $v_{t_i}\geq i$. $\square$

Example: Let $S=<8,9,10,11>$. Then, $k=3$ and $r=2$. $S_0=\{1,2,3,4,5,6,7\}$, $S_1=\{12,13,14,15\}$, $S_2=\{23\}$, $T_0=\{8,9,10,11\}$, $T_1=\{16,17,19,19,20,21,22\}$, $T_2=\{24,\ldots,33\}$ and $T_3=\{34,35,\ldots\}$.

Proof of Theorem 1.2. We consider two cases according with the parity of a.

Case A) If $a=2n$, $n\geq 1$ then $S=<2n,4n-1,6n-2>$. We consider the sets $S_i=\{(i-1)2n+1,\ldots,(i-1)2n+r_i\}$ for each $i=1,\ldots,3n-2$. We shall show, by induction on i, that if $s\in S_i$ then $s\notin S$. This can be easily checked for $i=1,2$ and 3. Let us suppose that it is true for $i=m\geq 4$ and let $s\in S_{m+1}$. Again, as in the above proof, we use the fact that $s\in S$ if and only if $s-l\in S$ with either $l=2n$ or $l=4n-1$ or $l=6n-2$. We then show that $s-l\in S_j$, for some $1\leq j\leq m$ when either $l=2n$ or $l=4n-1$ or $l=6n-2$ and thus, by the inductive hypothesis, $s-l\notin S$ (and therefore $s\notin S$).

Remark 2.1 *(a) If $r_{m+1}=r_m$ then $r_{m-1}=r_{m+1}+1$ and $r_{m-2}=r_{m+1}+2$.*
(b) If $r_{m+1}<r_m$ then $r_m=r_{m+1}+1$ and either $r_{m-1}=r_{m+1}+1$ and $r_{m-2}=r_{m+1}+2$ or $r_{m-1}=r_{m+1}+2$ and $r_{m-2}=r_{m+1}+2$.
From (a) and (b) we have that $r_{m+1}\leq r_m$, $r_{m+1}+1\leq r_{m-1}$ and $r_{m+1}+2=r_{m-2}$.

We now check three cases.

(1) If $l=2n$ then $s-l=m(2n)+j-2n=(m-1)2n+j$ with $1\leq j\leq r_{m+1}$. So, $s-l\in S_m$ since, by the above remark, $1\leq j\leq r_{m+1}\leq r_m$.

(2) If $l = 4n-1$ then $s - l = m(2n) + j - (4n-1) = (m-2)2n + j + 1$ with $1 \leq j \leq r_{m+1}$. So, $s - l \in S_{m-1}$ since, by the above remark, $1 \leq j+1 \leq r_{m+1} + 1 \leq r_{m-1}$.

(3) If $l = 6n-2$ then $s - l = m(2n) + j - (6n-2) = (m-3)2n + j + 2$ with $1 \leq j \leq r_{m+1}$. So, $s - l \in S_{m-2}$ since, by the above remark, $1 \leq j+2 \leq r_{m+1} + 2 = r_{m-2}$.

Now, we claim that if $t \notin S_i$ for all $i = 1, \ldots, 3n-2$ then $t \in S$. For this, we consider the set $T_i = \{(i-1)2n + r_i + 1, \ldots, i2n\})$ for each $i = 1, \ldots, 3n-2$ and $T_{3n-1} = \{(3n-2)2n + 1, \ldots, (3n-2)2n + 2n\}$. We show, by induction on i, that if $t \in T_i$ for some i then $s \in S$. This is clear for $i = 1, 2$ and 3. Indeed, the elements in $T_1 = \{2n\}$, $T_2 = \{4n-1, 4n = 2(2n)\}$ and $T_3 = \{6n-2, 6n-1 = 4n-1+2n, 6n = 3(2n)\}$ all belong to S. Now, we suppose that it is true for $i = m$ with $4 \leq m \leq 3n-3$ and notice that $T_j = (j-1)2n + s$ where $r_j + 1 \leq s \leq 2n$ for each $1 \leq j \leq 3n-2$. Let $t \in T_{m+1}$. If $s = 2n$ then $t = (m+1-1)2n + 2n = (m+1)2n$ that clearly belongs to S (t is a multiple of $2n$) and if $s = 2n-1$ then $t = (m+1-1)2n + 2n - 1 = (m+1)2n - 1 = 4n - 1 + (m-1)2n$ that also belongs to S (t is a combination of elements $4n-1$ and $2n$). Let us suppose now that $r_{m+1} + 1 \leq s < 2n-1$. We have three subcases according to the above remark (we recall that $t \in S$ if and only if $t_l \in S$ where $l = 2n$ or $4n-1$ or $6n-2$).

(1) If $r_{m+1} = r_m$ then $t - l = m(2n) + s - 2n = (m-1)2n + s$ with $r_{m+1} + 1 \leq s \leq 2n$. But, $t - l \in S_m$ since $r_m + 1 = r_{m+1} + 1 \leq s \leq 2n$. Thus, by the inductive hypothesis, $t - l \in S$ and therefore $t \in S$.

(2) If $r_m = r_{m+1} + 1$, $r_{m-1} = r_{m+1} + 1$ and $r_{m-2} = r_{m+1} + 2$ then $t - l = m(2n) + s - (4n-1) = (m-2)2n + s + 1$ with $r_{m+1} + 1 \leq s < 2n-1$. But, $t - l \in S_{m-1}$ since $r_{m-1} + 1 = r_{m+1} + 2 \leq s + 1 \leq 2n$. Thus, by the inductive hypothesis, $t - l \in S$ and therefore $t \in S$.

(3) If $r_m = r_{m+1} + 1$, $r_{m-1} = r_{m+1} + 2$ and $r_{m-2} = r_{m+1} + 2$ then $t - l = m(2n) + j - (6n-2) = (m-3)2n + s + 2$ with with $r_{m+1} + 1 \leq s < 2n-1$. But, $t - l \in S_{m-2}$ since $r_{m-1} + 1 = r_{m+1} + 3 \leq s + 2 \leq 2n$. Thus, by the inductive hypothesis, $t - l \in S$ and therefore $t \in S$.

For the case $i = 3n-1$ we have that $T_{3n-1} = (3n-2)2n + j$ with $j = 1, \ldots, 2n$. So, if $t \in T_{3n-1}$ then $t = (3n-2)2n + j = (3n-3)2n + j + 2n$ and since

$(3n-2)2n+j$ belongs to T_{3n-2} then $t \in S$. Since the elements in T_{3n-1} are consecutive and $|T_{3n-1}| = a$ then they form a complete system modulo a, that is, T_{3n-1} contain elements $t(0), \ldots, t(a-1)$ such that $t(i) \equiv i \bmod a$. From this, it is clear that if $t > \max\{T_{3n-1}\}$ then $t = t(i) + la$ with $l \geq 0$ integer and where $t \equiv i \bmod a$.

Thus, the sets S_i are the gaps in S (increasingly ordered) and

$$N(S) = v_{3n-2} = \sum_{i=0}^{3n-2} r_i = \frac{3}{4}n^2 - \frac{3}{2}n + 1.$$

In order to find the i^{th}-gap of S we first find out to which set S_j the gap l_i belongs to. The latter is done by computing the smallest integer t_i such that $v_{t_i} \geq i$ obtaining that $l_i \in S_{t_i}$. And thus, l_i is given by $(t_i - 1)2n + j$ with $j = i - v_{t_i - 1}$.

Case B) If $a = 2n+1$, $n \geq 1$ then $S =< 2n+1, 4n+1, 6n+1 >$. This case is analogous as the first one by considering the sets $S'_i = \{(i-1)(2n+1)+1, \ldots, (i-1)(2n+1)+r'_i\}$ for each $i = 1, \ldots, 3n-1$ and $T'_j = \{(j-1)(2n+1)+r'_j+1, \ldots, j(2n+1)\}$ with $j = 1, \ldots, 3n-2$.

Again, in this case, the sets S'_i are the gaps in S (increasingly ordered). So,

$$N(S) = v'_{3n-1} = \sum_{i=0}^{3n-1} r'_i = \tfrac{3}{4}(n^2 - 2n + 1) \text{ and } l_i = (i-1)(2n+1) + i - v'_{t_i - 1}.$$

$\square$

Example: Let $S =< 7, 13, 19 >$. Then, $n = 3$ and $r' = (0, 6, 5, 4, 4, 3, 2, 2, 1)$. $S_1 = \{1,2,3,4,5,6\}$, $S_2 = \{8,9,10,11,12\}$, $S_3 = \{15,16,17,18\}$, $S_4 = \{22,23,24,25\}$, $S_5 = \{29,30,31\}$, $S_6 = \{36,37\}$, $S_7 = \{43,44\}$, $S_8 = \{50\}$, $T_1 = \{7\}$, $T_2 = \{13,14\}$, $T_3 = \{19,20,21\}$, $T_4 = \{26,27,28\}$, $T_5 = \{32,33,34,35\}$, $T_6 = \{38,39,40,41,42\}$ and $T_7 = \{45,46,47,48,49\}$.

3 Gaps in $< p, q >$

The *Apéry* set of element a, $a \in S \setminus \{0\}$ is defined as $Ap(S,a) = \{s \in S | s - a \notin S\}$. It is known that the set $Ap(S,a)$ is a complete system modulo a, that is, $Ap(S,a) = \{0 = w(0), \dots, w(a-1)\}$ where $w(i)$ is the least element in S congruent with i modulo a. Let p, q positive integers such that $g.c.d.(p,q) = 1$. The semigroup $S_{pq} =< p, q >$ is *symmetric*, that is, for any integer $x \in [0, \dots, g(S_{pq})]$, $x \in S_{pq}$ if and only if $g(S_{pq}) - x \notin S_{pq}$.

Proof of Theorem 1.3. As S_{pq} is symmetric then for each $k = 0, \dots, \left\lfloor \frac{pq}{p+q} \right\rfloor - 1$ there exists a one-to-one correspondence between the sets

$$\{x \in \mathbb{N} | x \notin S_{pq} \text{ and } pq - (k+1)(p+q) \leq x \leq pq - k(p+q)\}$$

and

$$\{x \in S_{pq} | (k-1)(p+q) \leq x \leq k(p+q)\}.$$

Let $Ap(S_{pq}, p+q) = \{w(0), \dots, w(p+q-1)\}$ where $w(i)$ is the least element in S_{pq} congruent with i modulo $p+q$. Then, for each $i \in \{0, \dots, p+q-1\}$ we have that $(k-1)(p+q) + i \in S_{pq}$ if and only if $(k-1)(p+q) + i \geq w(i)$. Hence,

$$|\{x \in S_{pq} | (k-1)(p+q) \leq x \leq k(p+q)\}| = |\{w \in Ap(S_{pq}, p+q) | w < k(p+q)\}| + 1 \tag{4}$$

Since $g.c.d.(p,q) = 1$ then $Ap(S_{pq}, p+q) = \{0, p, 2p, \dots, (q-1)p, q, 2q, \dots, (p-1)q, pq\}$. Besides, $tq < k(p+q)$ if and only if $t < k + kp/q$ or equivalently, $t \leq k + \lfloor kp/q \rfloor$. Analogously, $tp < k(p+q)$ if and only if $t \leq k + \lfloor kq/p \rfloor$. Therefore,

$$\{w \in Ap(S_{pq}, p+q) | w < k(p+q)\} = \{0, p, \dots, (k + \lfloor kq/p \rfloor)p, q, \dots, (k + \lfloor kp/q \rfloor)q\}$$

and

$$|\{0, p, \dots, (k + \lfloor kq/p \rfloor)p, q, \dots, (k + \lfloor kp/q \rfloor)q\}| = 1 + k + \lfloor kq/p \rfloor + k + \lfloor kp/q \rfloor.$$

Thus, by equation (4),

$$|\{x \in S_{pq} | (k-1)(p+q) \leq x \leq k(p+q)\}| = 2(k+1) + \left\lfloor \frac{kq}{p} \right\rfloor + \left\lfloor \frac{kp}{q} \right\rfloor$$

and the result follows by the above bijection. □

Pick's theorem [10] is considered as one of the gems of elementary mathematics. It asserts that the area of a *simplest lattice polygon*[3] S, denoted by $A(S)$, is given by $I(S) + B(S)/2 - 1$ where $I(S)$ and $B(S)$ are the number of lattice points in the interior of S and in the boundary of S respectively; see [16] for a short proof of Pick's theorem.

Second proof of Theorem 1.3. Let P be the lattice polygon with vertices $(q-1,-1), (-1,p-1), (q,0)$ and $(0,p)$. Notice that there are no other lattice points on the boundary of P and that the set of lattice points inside P, denoted by $I(P)$, are all in the first quadrant. The equation of the line connecting the the first (resp. the last) two points is given by $px + qy = pq - p - q$ (resp. by $px + qy = pq$). Let T_1 and T_2 be the triangles formed by points $(q,0), (0,p), (-1,p-1)$ and $(-1,p-1), (q-1,-1), (q,0)$ respectively. Since

$$A(T_1) = \frac{1}{2}\begin{vmatrix} q & 0 & 1 \\ 0 & p & 1 \\ -1 & p-1 & 1 \end{vmatrix} = \frac{1}{2}(q+p) = \frac{1}{2}\begin{vmatrix} -1 & p-1 & 1 \\ q-1 & -1 & 1 \\ q & 0 & 1 \end{vmatrix} = A(T_2)$$

then $A(P) = A(T_1) + A(T_2) = p + q$ and, by Pick's theorem, we have that $|I(P)| = p + q - 1$. We claim that line $px + qy = pq - p - q + i$ contains

[3] We call a polygon simple if its boundary is a simple closed curve. A *lattice polygon* is a polygon where its vertices have integer coordinates.

exactly one point in $I(P)$ for each $i=1,\dots,p+q-1$. Suppose that there exists $1\le j\le p+q-1$ such that the line $px+qy=pq-p-q+j$ contains two points of $I(P)$, that is, $px_1+qy_1=pq-p-q+j=px_2+qy_2$ for some $0\le x_1,x_2<q$, $x_1\ne x_2$ and $0\le y_1,y_2<q$, $y_1\ne y_2$. But then, $(x_1-x_2)p=(y_2-y_1)q$ and since $(p,q)=1$ then $(x_1-x_2)=sq\ge q$ which is impossible. So each line $px+qy=pq-p-q+i$ contains at most one point of $I(P)$. Moreover, each line $px+qy=pq-p-q+i$ has at least one point of $I(P)$ otherwise, by the pigeon hole principle, it would exists a line $px+qy=pq-p-q+j$ for some $1\le j\le p+q-1$ containing two points of $I(P)$, which is a contradiction. Notice that, since all lines $px+qy=n\ge pq$ clearly have at least one lattice point in the first quadrant then $pq-p-q$ is the largest value for which $px+qy=pq-p-q$ does not have solution on the nonnegative integers. Thus $F_0(S_{pq})=1$.

Let k^* be the largest integer such that $pq-k^*(p+q)\ge 0$. Let Q_k be the polygon formed by the points $(q-k,-k),(q-(k+1),-(k+1)),(-k,p-k)$ and $(-(k+1),p-(k+1))$. Notice that $Q_0=P$, that Q_k is just a translation of Q_0 and that Q_{k^*-1} does not contains points $(-x,-y)$, $x,y>0$ (by definition of k^*). Let r_k^1 (resp. r_k^2) be the intersection of the line $px+qy=pq-k(p+q)$ with the x-axis (resp. with the y-axis) for each $k=0,\dots,k^*$. Let Q_k^1 (resp. Q_k^2), $k=0,\dots,k^*-1$ be the (not necessarily lattice) polygon formed by the points $(r_k^1,0),(r_{k+1}^1,0),(q-k,-k)$ and $(q-(k+1),-(k+1))$ (resp. formed by the points $(0,r_k^2),(0,r_{k+1}^2),(-k,p-k)$ and $(-(k+1),p-(k+1))$). We notice that Q_k^1 (resp. Q_k^2) is the piece of Q_k that lies below the x-axis (resp. on the left-hand side of the y-axis). Since each line $px+qy=pq-(p+q)+j$, $1\le j\le p+q-1$ has a unique solution with nonnegative integers (x,y) then the translated line $px+qy=pq-k(p+q)+j$ (lying in Q_k) does not have solution with nonnegative integers if the corresponding translation of (x,y) lies either in Q_k^1 or Q_k^2. Hence, $F_k(S_{pq})=I(Q_k^1)+I(Q_k^2)+2$ for each $k=1,\dots,k^*-1$ (the term 2 counts the gaps corresponding to the inexistence of solutions for $px+qy=pq-k(p+q)$ and $px+qy=pq-(k+1)(p+q)$). We calculate $I(Q_k^1)$ and $I(Q_k^2)$ for each $k=1,\dots,k^*-1$. To this end, we first observe that the number of integer points lying on the interval $[(\lceil r_k^1\rceil,0),\dots,(q,0)[=[(q-k-\lfloor\frac{kq}{p}\rfloor,0),\dots,(q,0)[$ (resp. lying on the interval

$[(0,p),\dots,(0,\lceil r_k^2\rceil)[=[(0,p),\dots,(0,p-k-\lfloor\frac{kp}{q}\rfloor)[$) is equals to $k+\left\lfloor\frac{kq}{p}\right\rfloor$ (resp.

equals to $k+\left\lfloor \frac{kp}{q}\right\rfloor$). Let Δ_k^1 and Δ_k^2 the number of integer points lying on

the intervals $[(r_{k+1}^1,0),\ldots,(r_k^1,0)[$ and $[(0,r_{k+1}^2),\ldots,(0,r_k^2)[$ respectively for each $k=1,\ldots,k^*-1$. Then,

$$\begin{aligned} I(Q_k^1) &= \sum_{i=0}^{k-1}\Delta_i^1 = \sum_{i=0}^{k-1}\left((i+1)+\left\lfloor\frac{(i+1)q}{p}\right\rfloor - \left(i+\left\lfloor\frac{iq}{p}\right\rfloor\right)\right) \\ &= \sum_{i=0}^{k-1}\left(1+\left\lfloor\frac{(i+1)q}{p}\right\rfloor - \left\lfloor\frac{iq}{p}\right\rfloor\right) = k+\left\lfloor\frac{kq}{p}\right\rfloor. \end{aligned}$$

Similarly, $I(Q_k^2)=k+\left\lfloor\frac{kp}{q}\right\rfloor$, $k=1,\ldots,k^*-1$ and the result follows. $\square$

We end this section with the following question. Let $\rho_i(S)=\rho_i$ be the i^{th} non-gap of S and let $M(i)$ be the number of gaps smaller than ρ_i.

Question 3.1 *Is $M(i)$ computable in polynomial time?*

References

[1] A. Brauer, On a problem of partitions, *Amer. Journal of Math.* **64** (1942), 299-312.

[2] T.C. Brown and P.J. Shiue, A remark related to the Frobenius problem, *The Fibonacci Quarterly* **31**(1) (1993), 32-36.

[3] R. Frőberg, C. Gottlieb and R. Hăggkvist, On numerical semigroups, *Semigroup Forum* **35** (1987), 63-83.

[4] R. Kannan, Lattice translates of a polytope and the Frobenius problem, *Combinatorica* **12**(2) (1992), 161-177.

[5] J. Komeda, Non-Weierstrass numerical semigroups, *Semigroup Forum* **57** (1998), 157-185.

[6] J. Komeda, Remarks on non-Weierstrass numerical semigroups, *Algebras and Combinatorics. An International Congress, ICAC'97, Hong Kong* (eds. K.-P. Shum, E.J. Taft and Z.-X. Wan), Springer-Verlag (1999), 313-319.

[7] M. Nijenhuis and H.S. Wilf, Representation of integers by linear forms in nonnegative integers, *J. Number Theory* **4** (1972), 98-106.

[8] G. Oliveira, Weierstrass semigroups and the canonical ideal of non-trigonial curves, *Manuscripta Math.* **71** (1991), 431-450.

[9] R. Pellikaan and F. Torres, On Weierstrass semigroups and the redundancy of improved geometric Goppa codes, *IEEE Transactions on Information Theory* **45**(7) (1999), 2512-2519.

[10] G. Pick, Geometrisches zur Zahlenlehre, *Sitzungsber. Lotos (Prague)* **19** (1899), 311-319.

[11] J.L. Ramírez Alfonsín, Complexity of the Frobenius problem, *Combinatorica* **16**(1) (1996), 143-147.

[12] J.L. Ramírez Alfonsín, The diophantine Frobenius problem, *Forschungsinstitut für Diskrete Mathematik, Bonn*, Report No.00893 (2000), (43 pages).

[13] J.B. Roberts, Note on linear forms, *Proc. Amer. Math. Soc.* **7** (1956), 465-469.

[14] J.J. Sylvester, Problem 7382, *Educational Times* **37** (1884), 26; reprinted in: Mathematical questions with their solution, *Educational Times* (with additional papers and solutions) **41** (1884), 21.

[15] J.J. Sylvester, On subinvariants, i.e. semi-invariants to binary quantities of an unlimited order, *Amer. J. Math.* **5** (1882), 119-136.

[16] D.E. Varberg, Pick's theorem revisited, *Amer. Math. Monthly* **92** (1985), 584-587.