NUMERICAL SEMIGROUPS OF TWO GENERATORS

Antoine Mhanna

NUMERICAL SEMIGROUPS OF TWO GENERATORS

ANTOINE MHANNA[1]*

ABSTRACT. This paper will represent in a simple way some known facts about semigroups especially when the number of minimal generators equals two or in general semigroups with at least two minimal generators. The originality of this exposition is that it is a straight application of a remark written by Sylvester itself.

1. Introduction

As the title indicates we shall revisit numerical semigroups S having at most two minimal generators. However in contrast to other research analogies we shall consider general semigroups *i.e.* letting $a_1, \cdots, a_n$ be n positive integers with $gcd(a_1, \cdots, a_n) = m$, the set $S' := \left\{ \sum_{i=1}^{s} \lambda_i a_i, s \in \mathbb{N}, \lambda_i \geq 0, \text{for all } i \right\}$ is called the semigroup S' and $a_1, \cdots, a_n$ are called the generators of S'. $a_1, \cdots, a_n$ are minimal generators if we cannot take out a generator a_i without changing the set S', in this case we denote S' by $\langle a_1, \cdots, a_n \rangle$. If $m = 1$ the semigroup S' becomes a numerical semigroup and is denoted hereafter by S. We will see (Lemma 1) that for such semigroups there exist a point $F(S)$ known as the Frobenius number for which every $n > F(S)$, $n \in S$. The set of points $E := \{y \leq F(S), y \in S\}$ is also called set of green points. The cardinality of E is denoted by $|E|$. Wilf's Conjecture stats that for a given $S = \langle a_1, \cdots, a_n \rangle$, we have:

$$n.|E| \geq F(S) + 1.$$

I will be giving a proof that is due to Sylvester, nevertheless no literature exist (to my knowledge) that explicit what Sylvester has to say concerning semigroups with two minimal generators.

Remark. Notice that $a_1 a_2 = \lambda_1 a_1 + \lambda_2 a_2$ is impossible for any $\lambda_1, \lambda_2 \in \mathbb{N}$ both different from 0 and a_1 and a_2 are coprime *i.e* $gcd(a_1, a_2) = 1$. We will suppose hereafter that $a_1 < a_2$.

2. Two minimal generators

Definition. Let a_1 and a_2 be positive integers with $gcd(a_1, a_2) = 1$. The set of positive numbers x of the form $x = \alpha a_i - \beta a_{3-i}$, $i = 1$ or 2 with $0 < \alpha < a_{3-i}$ and $0 < \beta < a_i$ is called the non-coumpound set (this will be clarified next) and is denoted by NC. The set of numbers x of the form $x = \alpha a_1 + \beta a_2$ with $\alpha > 0$, $\beta > 0$ and $x < a_1 a_2$ is called the coumpound set and is denoted by C.

Date: 2016
* Corresponding author.
2010 *Mathematics Subject Classification.* 11D07; 11A99.
Key words and phrases. Numerical Semigroups, Frobenius Number, Bezout's theorem.

The next theorem was just a line in a brief illustration remarked by Sylvester, (see [1] on p. 134).

Theorem 1. *For $S = \langle a_1, a_2 \rangle$, we have $x \in NC$ if and only if $0 < x < a_1a_2$ and $x \notin S$.*

Proof. Clearly if we subtract from a_1a_2 such number x the result is a positive number y, $(y \in S)$. Suppose $x \in S$, $x < a_1a_2$, $x = aa_1 + ba_2 = \alpha a_i - \beta a_{3-i}$ for some positive numbers a, b but this contradicts the fact that $\alpha < a_{3-i}$ and $\beta < a_i$. $|NC| = \dfrac{(a_1-1)(a_2-1)}{2}$. Take the numbers less than a_1a_2 having neither a_1 nor a_2 as a divisor, there are $(a_1-1)(a_2-1)$ such numbers, arrange them as couples summing a_1a_2 -this is possible see Remark 1- if $x \in NC$, $a_1a_2 - x = y \in S$, and if $y \in C$, $(a_1a_2 - y) = x \notin S$, that means that $x \in NC$. Finally $|NC| = \dfrac{(a_1-1)(a_2-1)}{2}$ and $|NC| + |C| = (a_1-1)(a_2-1)$. □

We have proven that $|NC| = |C| = \dfrac{(a_1-1)(a_2-1)}{2}$. The number $F(S) = (a_1-1)(a_2-1) - 1$ doesn't belong to S, indeed since $a_1a_2 - F(S)$ is coumpound, the nearest (smaller) non counpound number is precisely $y = F(S) - a_1$, but again the difference between $F(S)$ and y is a_1 and $F(S)+a_1 \in S$ so all $n > F(S)$ do belong to S. In other words $|E| = (a_1-1)(a_2-1) - \dfrac{(a_1-1)(a_2-1)}{2} = \dfrac{(a_1-1)(a_2-1)}{2}$ and $2.|E| = F(S) + 1$.

Now we can characterize all the numbers that aren't in $S := \langle a_1, a_2 \rangle$.

Proposition 1. The set NC is the set $\{F(S) - y, y \in S, y < F(S)\}$

Proof. A direct application of previous arguments. □

Some topics related to the above discussion are in [2], [3] and [4]. Interested reader can see [5] and the references therein for an extensive reading on numerical semigroups.

2.1. **Bezout Theorem.** The following lemma generalizes Sylvester's idea to semigroups:

Lemma 1. *Let $S' = \langle a_1, \cdots, a_n \rangle$ with $gcd(a_1, \cdots, a_n) = m$ then there is an integer α_0 such that for all $\alpha \geq \alpha_0$, $\alpha m \in S$. In particular when $m = 1$, S' becomes S and we have the existence of $F(S)$ the Frobenius number.*

Proof. Start by $n = 2$, the semigroup $\left\langle \dfrac{a_1}{m}, \dfrac{a_2}{m} \right\rangle$ is a numerical semigroup so called S, any number $x > F(S)$ do belong to S multiplying x by m we get the result. First we deal with $m = 1$, (any semigroup S' can be transformed in a numerical semigroup by dividing each minimal generator by m) say $S = \langle a_1, a_2, a_3 \rangle$ and $m_2 = gcd(a_1, a_2) > 1$ we already know that m_2^j is in $\langle a_1, a_2 \rangle$ for some large j but since $m = 1$; $\langle m_2^j, a_3 \rangle$ is a numerical semigroup and the statement follows. By induction if $m_{n-1} = gcd(a_1, \cdots, a_{n-1}) > 1$ then $r := z^i$ is in the semigroup $\langle a_1, \cdots, a_{n-1} \rangle$ for sufficiently large i; z is formed by factors that are common to all a_i' s with $1 \leq i \leq n-1$. Having $m = 1$, $S_1 = \langle r, a_n \rangle$ is a numerical semigroup and for all $x > F(S_1)$, $x \in S_1$; x multiplied by m will be in S'. When $m_{n-1} = 1$ we can remove minimal generators until $m_h = gcd(a_1, \cdots, a_h) > 1$ and the same proof can be applied here. □

Theorem 2. *Let $S' = \langle a_1, \cdots, a_n \rangle$ with $gcd(a_1, \cdots, a_n) = m$ then there exists at least one $n-$ tuple $\lambda = (\lambda_1, \cdots, \lambda_n) \in \mathbb{Z}^n$ such that* $\displaystyle\sum_{i=1}^{n} \lambda_i a_i = m$

Proof. By Lemma 1, take any $\beta \geq \alpha_0$ so that $(\beta + 1)m - \beta m = m$ $\square$

References

[1] J. J. Sylvester. *Excursus on rational fractions and partitions.* Amer J. Math. **5**: p. 119-136, 1882.

[2] T. C. Brown, P. J.-S. Shiue, *A Remark Related to the Frobenius Prob- lem*, Fibonacci Quarterly, **31** (1), p. 32-36, 1993.

[3] Ö. J. Rödseth, *A note on T.C. Brown and P.J.-S. Shiues paper: A remark related to the Frobenius problem*, Fibonacci Quarterly, **32** (5), p. 407-408, 1994.

[4] H. J.H. Tuenter , *The Frobenius problem, sums of powers of integers, and recurrences for the Bernoulli numbers*, Journal of Number Theory, **117** (2), p. 376-386, 2006.

[5] J. C. Rosales, P. A. García-Sánchez, *Numerical semigroups*, Developments in Mathematics, **20**, Springer, New York, 2009.

[1] Kfardebian-Beirut, Lebanon
E-mail address: tmhanat@yahoo.com