THE FROBENIUS NUMBERS OF SOME NUMERICAL SEMIGROUPS

HYUNG NAE LEE AND BYUNG CHUL SONG

Abstract. Let \( S_i \) be the numerical semigroup generated by the set \( \{a, a + d, \ldots, a + (i - 1)d, a + (i + 1)d, \ldots, a + rd\} \). In this paper, we will formulate the largest nonmember, the Frobenius number, of each set \( S_i \).

1. Introduction

If the greatest common divisor of the positive integers \( a_0, a_1, \cdots, a_r \) is 1, then the set

\[
S = \{\sum_{i=0}^{r} a_in_i | n_i \in \mathbb{N}^*\}
\]

where \( \mathbb{N}^* = \mathbb{N} \cup \{0\} \), contains all the nonnegative integers except a finite set of numbers. In this case we call the set \( S \) a numerical semigroup generated by the set \( \{a_0, a_1, \cdots, a_r\} \). Denote \( S \) by \( < a_0, a_1, \cdots, a_r > \). We denote \( F(S) \) by the largest nonmember, the Frobenius number, of \( S \).

In 1956, Roberts \[?\] found \( F(S) \) for \( S =< a, a + d, \cdots, a + rd > \), when \( (a, d) = 1 \). In general if 2 numerical semigroups \( T_1 \) and \( T_2 \) are generated by 2 sets \( B_1 \) and \( B_2 \) respectively with \( B_1 \subset B_2 \), then \( F(T_1) \geq F(T_2) \). So if we add (or delete) terms into (or from) a given set \( B \) to make \( B' \), then the Frobenius number of the numerical semigroup generated by \( B' \) may be changed. Several authors \[?\], \[?\], \[?\] treated \( F(B') \) when \( B \) is a finite arithmetical progression. Throughout this paper we assume that the positive numbers \( a, d, r \) satisfy \( (a, d) = 1 \) with \( a > r \geq 3 \). Now we consider the sets \( B = \{a, a + d, \cdots, a + rd\}, B_i = B \setminus \{a + id\}, S =< B > \) and \( S_i =< B_i > \) for \( 1 \leq i \leq r - 1 \). Note that \( F(S) = \left[\frac{a-2}{r}\right]a + (a-1)d \)

Received August 21, 2002.


Key words and phrases: numerical semigroup, Frobenius number.
Let in each residue class modulo $\alpha$ we have $\alpha \equiv \alpha + t \pmod{d}$, so that $\alpha$ is defined as $\alpha = \alpha + nt$. This means that $\alpha$ is the smallest integer such that $\alpha \equiv \alpha + nt \pmod{d}$. Then clearly $S_i = \cup_{m=0}^{\infty} A_i^{(m)}$, where $A_i^{(0)} = \{0\}$.

If $2 \leq i \leq r - 2$ and $m \geq 2$, then $A_i^{(m)} = \{ma, ma + d, \cdots, ma + mrd\}$. Since $S_i = A_i^{(0)} \cup A_i^{(1)} \cup \cdots \cup A_i^{(m-1)}$, we have $\alpha \equiv \alpha + t \pmod{d}$ if and only if $\alpha + t \in A_i^{(m-1)}$ for some $m$. And since $(a, d)$ is a necessary and sufficient condition under which $F(S) = F(S_i)$.

2. Main Theorems

Let $A_i^{(m)}$ be the set of numbers with $m$ addition of elements from $B_i$, that is,

$$A_i^{(m)} = \{\sum_{j=1}^{m} \alpha_j | \alpha_j \in B_i\}.$$ 

Then clearly $S_i = \cup_{m=0}^{\infty} A_i^{(m)}$, where $A_i^{(0)} = \{0\}$.

If $2 \leq i \leq r - 2$ and $m \geq 2$, then $A_i^{(m)} = \{ma, ma + d, \cdots, ma + mrd\}$. Since $S_i = \{ma, ma + d, \cdots, ma + mrd\}$, we have $F(S_i) = \max\{F(S), a + id\}$.

Note that $A_i^{(m)} = \{ma, ma + d, \cdots, ma + mrd\}$ for $m \geq 2$. If we choose $n_0$ be the smallest integer such that $n_0r \geq a + 1$, then it's easy to check that $n_0 = \left[\frac{a}{r}\right] + 1$. Since $n_0r \geq a + 1$, $A_i^{(n_0)}$ contains the set $C = \{n_0a + 2d, \cdots, n_0a + (a+1)d\} = n_0a + \{2d, 3d, \cdots, (a+1)d\}$. We also note that since $(a, d) = 1$ the set $C \equiv Z_a \pmod{a}$.

**Theorem 2.1.** $F(S_1) = \left[\frac{a}{r}\right]a + (a + 1)d$.

**Proof.** Let $\alpha = \left\lfloor\frac{a}{r}\right\rfloor a + (a + 1)d$, then since $n_0r \geq a + 1 > (n_0 - 1)r$ we have $\alpha = \left\lfloor\frac{a}{r}\right\rfloor a + (a + 1)d > (n_0 - 1)a + (n_0 - 1)rd$. Which means that $\alpha \notin \cup_{j=0}^{n_0-1} A_i^{(j)}$. Since $(a, d) = 1$, we have $kd \equiv d \pmod{a}$ for any $k = 2, 3, \cdots, a$. So the smallest number in $\cup_{j=0}^{\infty} A_i^{(j)}$ that is equivalent to $d$ modulo $a$ is $n_0a + (a+1)d$. But $n_0a + (a+1)d > \alpha$, so that $\alpha \notin \cup_{j=n_0}^{\infty} A_i^{(j)}$. In conclusion we have $\alpha \notin \cup_{j=n_0}^{\infty} A_i^{(j)} = S_1$. Since $C$ contains an element in each residue class modulo $a$, for any $p \geq 1$ there exists $\beta \in C$ such that $\alpha + p \equiv \beta \pmod{a}$. But we have $\beta - a \leq (n_0 - 1)a + (a+1)d < \alpha + p$, so that $\alpha + p \geq \beta$. And since $\beta \in C \subset A_i^{(n_0)} \subset S_1$, we have $\alpha + p \in S_1$. So that $\alpha = F(S_1)$. \hfill $\Box$

Now we consider $A_i^{(m)} = \{ma, ma + d, \cdots, ma + (mr - 2)d, ma + mrd\}$. And let $n_0$ be the same as above. We denote the residue of $n$ modulo $t$ by $n \pmod{t}$.
THEOREM 2.2. If $a \ (\text{mod } r) = 1$, then $F(S_{r-1}) = \left[\frac{a}{r}\right]a + (a - 2)d$ when $a > d$ and $F(S_{r-1}) = (\left[\frac{a}{r}\right] - 1)a + (a - 1)d$ when $a < d$.

Proof. If $a > d$, since $a = (n_0 - 1)r + 1$, we have

$$A_{r-1}^{(n_0-1)} = (n_0 - 1)a + \{0, d, \cdots, ((n_0 - 1)r - 2)d, (n_0 - 1)r d\}$$

$$= (n_0 - 1)a + \{0, d, 2d, \cdots, (a - 3)d, (a - 1)d\}.$$

Clearly $\alpha = \left[\frac{a}{r}\right]a + (a - 2)d \notin A_{r-1}^{(n_0-1)}$, and so $\alpha \notin \bigcup_{j=0}^{n_0-1} A_{r-1}^{(j)}$. Now since $\alpha \equiv (a - 2)d \ (\text{mod } a)$ and $(a, d) = 1$, the smallest element in $\bigcup_{j=n_0}^{\infty} A_{r-1}^{(j)}$ that is equivalent to $\alpha$ modulo $a$ is $n_0a + (a - 2)d$ which is larger than $\alpha$. That is $\alpha \notin \bigcup_{j=n_0}^{\infty} A_{r-1}^{(j)}$. Now since the set $D = (n_0 - 1)a + \{0, d, \cdots, (a - 1)d\} \equiv \mathbb{Z}_{a} \ (\text{mod } a)$, for $p \geq 1$, $\alpha + p \equiv \beta \ (\text{mod } a)$ for some $\beta \in D$. If $\beta \neq (n_0 - 1)a + (a - 2)d$, since $\beta - a \leq (n_0 - 2)a + (a - 1)d = a - a + 1 = \alpha$, $\alpha + p \geq \beta \in A_{r-1}^{(n_0-1)} \subset S_{r-1}$. If $\beta = (n_0 - 1)a + (a - 2)d = \alpha$, since $\alpha + p > \beta$, $\alpha + p \geq \beta + a \in A_{r-1}^{(n_0)} \subset S_{r-1}$. So $\alpha + p \in S_{r-1}$. Thus

$$F(S_{r-1}) = \alpha.$$ Let $\gamma = \left[\frac{a}{r}\right]a + (a - 1)d$. If $a < d$, since $\left[\frac{a-2}{r}\right] = \left[\frac{a}{r}\right] - 1$, $F(S_{r-1}) \geq F(S) = \gamma$. If $p \geq 1$, $\gamma + p \equiv \beta \ (\text{mod } a)$ for some $\beta \in D$. If $\beta \neq (n_0 - 1)a + (a - 1)d$, since $\beta \leq (n_0 - 1)a + (a - 2)d = \gamma + a - d < \gamma + p$, we have $\gamma + p \geq \beta + a \in A_{r-1}^{(n_0)} \subset S_{r-1}$. If $\beta = (n_0 - 1)a + (a - 1)d$, since $\beta - a = \gamma < \gamma + p$, $\gamma + p \geq \beta \in A_{r-1}^{(n_0-1)} \subset S_{r-1}$. So $\gamma + p \in S_{r-1}$. Thus

$$F(S_{r-1}) = \gamma.$$ □

THEOREM 2.3. If $a \ (\text{mod } r) \neq 1$, then $F(S_{r-1}) = \left[\frac{a}{r}\right]a + (a - 1)d$.

Proof. Since $(a, d) = 1$ and $a - 1 \leq n_0r - 2$, the set $E = n_0a + \{0, d, \cdots, (a - 1)d\} \subset A_{r-1}^{(n_0)}$ is equivalent to $\mathbb{Z}_{a}$ modulo $a$. If $a \ (\text{mod } r) = 0$, then $a = (n_0 - 1)r$. So $A_{r-1}^{(n_0-1)} = (n_0 - 1)a + \{0, d, \cdots, (a - 2)d, ad\}$ and $\alpha = (n_0 - 1)a + (a - 1)d \notin \bigcup_{j=0}^{n_0-1} A_{r-1}^{(j)}$. Moreover, since $\alpha = 1$, the smallest number in $\bigcup_{j=n_0}^{\infty} A_{r-1}^{(j)}$ which is equal to $\alpha$ modulo $a$ is $n_0a + (a - 1)d$. And since $n_0a + (a - 1)d < \alpha$, $\alpha \notin S_{r-1}$. Since $E \equiv \mathbb{Z}_{a} \ (\text{mod } a)$, for any $p \geq 1$ there exists $\beta \in E$ such that $\alpha + p \equiv \beta \ (\text{mod } a)$. But $\beta - a \leq (n_0 - 1)a + (a - 1)d < \alpha + p$. So that $\alpha + p \geq \beta \in S_{r-1}$. So $\alpha + p \in S_{r-1}$. We have $F(S_{r-1}) = \left[\frac{a}{r}\right]a + (a - 1)d$. If $a \ (\text{mod } r) > 1$, then $a > (n_0 - 1)r + 1$. So that the largest element $(n_0 - 1)a + (n_0 - 1)rd$ in the set $\bigcup_{j=0}^{n_0-1} A_{r-1}^{(j)}$ is smaller than $\alpha = (n_0 - 1)a + (a - 1)d$. And since $(a, d) = 1$, the smallest element in $\bigcup_{j=n_0}^{\infty} A_{r-1}^{(j)}$ that is equivalent to
\[ \alpha \text{ modulo } a = n_0a + (a - 1)d, \text{ which is larger than } \alpha. \] Finally for any \( p \geq 1 \) there exists \( \beta \in E \) such that \( \alpha + p \equiv \beta \pmod{a} \). Similar to the above, \( \alpha + p \geq \beta \in S_{r-1} \), which implies \( F(S_{r-1}) = \alpha \).

**Corollary 2.4.** Two Frobenius numbers \( F(S_i) \) and \( F(S) \) are different if and only if \( i = 1 \) or \( r = a - 1 \) and \( id > ad - a - d \) or \( i = r - 1 \) and \( a \pmod{r} = 0 \) or \( i = r - 1, a > d \) and \( a \pmod{r} = 1 \).

**Proof.** If \( i = 1 \), \( F(S_i) = \left[ \frac{a}{r} \right] a + (a + 1)d > \left[ \frac{a+2}{r} \right] a + (a - 1)d = F(S) \).

If \( 2 \leq i \leq r - 2 \) and \( r < a - 1 \), since \( a + id < a + (a - 1)d \leq \left[ \frac{a+2}{r} \right] a + (a - 1)d = F(S), F(S_i) = F(S) \).

If \( 2 \leq i \leq r - 2 \) and \( r = a - 1 \), \( F(S_i) = F(S) \) is equivalent to \( a + id \leq (a - 1)d \).

If \( i = r - 1 \) and \( a \pmod{r} \neq 1 \), by Theorem 2.3., \( F(S_i) = F(S) \) is equivalent to \( \left[ \frac{a}{r} \right] = \left[ \frac{a-2}{r} \right] \). This condition is identical to \( a \pmod{r} \geq 2 \).

If \( i = r - 1, a \pmod{r} = 1 \) and \( a > d \), \( F(S_{r-1}) = \left[ \frac{a}{r} \right] a + (a - 2)d \neq \left[ \frac{a-2}{r} \right] a + (a - 1)d = F(S) \).

If \( i = r - 1, a \pmod{r} = 1 \) and \( a < d \), \( F(S_{r-1}) = \left( \left[ \frac{a}{r} \right] - 1 \right) a + (a - 1)d = \left[ \frac{a-2}{r} \right] a + (a - 1)d = F(S) \).

---

References


Daein High School
47-3 Kongchondong, Seo Gu
Inchon, Korea

*E-mail:* galois@dreamwiz.com

Department of Mathematics
Kangnung National University
210-702 Kangnung Kangweondo, KOREA

*E-mail:* bcsong@knusun.kangnung.ac.kr