Kangweon-Kyungki Math. Jour. **10** (2002), No. 2, pp. 191–194

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 $\{a, a+d, \cdots, a+(i-1)d, a+(i+1)d, \cdots, a+rd\}$. 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

$$S = \{\sum_{i=0}^{r} a_i n_i | n_i \in \mathbb{N}^*\}$$

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 $F(S) = [\frac{a-2}{r}]a + (a-1)d$

Received August 21, 2002.
2000 Mathematics Subject Classification: Primary: 11D04, Secondary: 11B75, 20M14.
Key words and phrases: numerical semigroup, Frobenius number.

(See [?]), where $[q]$ be the largest integer less than or equal to q. In this paper we will compute $F(S_i)$ and find 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 $2 \le i \le r-2$ and $m \ge 2$, then $A_i^{(m)} = \{ma, ma+d, \cdots, ma+mrd\}$.
Since $S_i =< a, a+d, \cdots, a+rd > \backslash \{a+id\}$,

$$F(S_i) = \max\{F(S), a+id\}.$$

Note that $A_i^{(m)} = \{ma, ma+d, \cdots, ma+mrd\}$ for $m \ge 2$. If we choose n_0 be the smallest integer such that $n_0 r \ge a+1$, then it's easy to check that $n_0 = [\frac{a}{r}]+1$. Since $n_0 r \ge a+1$, $A_1^{(n_0)}$ contains the set $C = \{n_0 a + 2d, \cdots, n_0 a + (a+1)d\} = n_0 a + \{2d, 3d, \cdots, (a+1)d\}$. We also note that since $(a,d) = 1$ the set $C \equiv \mathbb{Z}_a \pmod a$.

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

Proof. Let $\alpha = [\frac{a}{r}]a + (a+1)d$, then since $n_0 r \ge a+1 > (n_0-1)r$ we have $\alpha = [\frac{a}{r}]a + (a+1)d > (n_0-1)a + (n_0-1)rd$. Which means that $\alpha \notin \cup_{j=0}^{n_0-1} A_1^{(j)}$. Since $(a,d) = 1$, we have $kd \not\equiv d \pmod a$ for any $k = 2, 3, \cdots, a$. So the smallest number in $\cup_{j=n_0}^{\infty} A_1^{(j)}$ that is equivalent to d modulo a is $n_0 a + (a+1)d$. But $n_0 a + (a+1)d > \alpha$, so that $\alpha \notin \cup_{j=n_0}^{\infty} A_1^{(j)}$. In conclusion we have $\alpha \notin \cup_{j=0}^{\infty} A_1^{(j)} = S_1$. Since C contains an element in each residue class modulo a, for any $p \ge 1$ there exists $\beta \in C$ such that $\alpha + p \equiv \beta \pmod a$. But we have $\beta - a \le (n_0-1)a + (a+1)d < \alpha + p$, so that $\alpha + p \ge \beta$. And since $\beta \in C \subset A_1^{(n_0)} \subset S_1$, we have $\alpha + p \in S_1$. So that $\alpha = F(S_1)$. □

Now we consider $A_{r-1}^{(m)} = \{ma, ma+d, \cdots, ma+(mr-2)d, ma+mrd\}$. 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* $a \pmod r = 1$, *then* $F(S_{r-1}) = [\frac{a}{r}]a + (a-2)d$ *when* $a > d$ *and* $F(S_{r-1}) = ([\frac{a}{r}] - 1)a + (a-1)d$ *when* $a < d$.

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

$$\begin{aligned} A_{r-1}^{(n_0-1)} &= (n_0-1)a + \{0, d, \cdots, ((n_0-1)r-2)d, (n_0-1)rd\} \\ &= (n_0-1)a + \{0, d, 2d, \cdots, (a-3)d, (a-1)d\}. \end{aligned}$$

Clearly $\alpha = [\frac{a}{r}]a + (a-2)d \notin A_{r-1}^{(n_0-1)}$, and so $\alpha \notin \cup_{j=0}^{n_0-1} A_{r-1}^{(j)}$. Now since $\alpha \equiv (a-2)d \pmod a$ and $(a,d) = 1$, the smallest element in $\cup_{j=n_0}^{\infty} A_{r-1}^{(j)}$ that is equivalent to α modulo a is $n_0 a + (a-2)d$ which is larger than α. That is $\alpha \notin \cup_{j=n_0}^{\infty} A_{r-1}^{(j)}$. Now since the set $D = (n_0-1)a + \{0, d, \cdots, (a-1)d\} \equiv \mathbb{Z}_a \pmod a$, for $p \geq 1$, $\alpha + p \equiv \beta \pmod a$ for some $\beta \in D$. If $\beta \neq (n_0-1)a + (a-2)d$, since $\beta - a \leq (n_0-2)a + (a-1)d = \alpha - a + d < \alpha$, $\alpha + p \geq \beta \in A_{r-1}^{(n_0-1)} \subset S_{r-1}$. 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 $\gamma = ([\frac{a}{r}] - 1)a + (a-1)d$. If $a < d$, since $[\frac{a-2}{r}] = [\frac{a}{r}] - 1$, $F(S_{r-1}) \geq F(S) = \gamma$. If $p \geq 1$, $\gamma + p \equiv \beta \pmod a$ 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* $a \pmod r \neq 1$, *then* $F(S_{r-1}) = [\frac{a}{r}]a + (a-1)d$.

Proof. Since $(a,d) = 1$ and $a - 1 \leq n_0 r - 2$, the set $E = n_0 a + \{0, d, \cdots, (a-1)d\} \subset A_{r-1}^{(n_0)}$ is equivalent to $\mathbb{Z}_a$ modulo a. If $a \pmod r = 0$, 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 $\alpha = (n_0-1)a + (a-1)d \notin \cup_{j=0}^{n_0-1} A_{r-1}^{(j)}$. Moreover, since $(a,d) = 1$, the smallest number in $\cup_{j=n_0}^{\infty} A_{r-1}^{(j)}$ which is equal to α modulo a is $n_0 a + (a-1)d$. And since $n_0 a + (a-1)d > \alpha$, $\alpha \notin S_{r-1}$. Since $E \equiv \mathbb{Z}_a \pmod a$, for any $p \geq 1$ there exists $\beta \in E$ such that $\alpha + p \equiv \beta \pmod a$. 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 $F(S_{r-1}) = [\frac{a}{r}]a + (a-1)d$. If $a \pmod r > 1$, then $a > (n_0-1)r + 1$. So that the largest element $(n_0-1)a + (n_0-1)rd$ in the set $\cup_{j=0}^{n_0-1} A_{r-1}^{(j)}$ is smaller than $\alpha = (n_0-1)a + (a-1)d$. And since $(a,d) = 1$, the smallest element in $\cup_{j=n_0}^{\infty} A_{r-1}^{(j)}$ that is equivalent to

α modulo a is $n_0a + (a-1)d$, which is larger than α. 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 $F(S_{r-1}) = \alpha$. $\square$

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 $i = 1$, $F(S_1) = [\frac{a}{r}]a + (a+1)d > [\frac{a-2}{r}]a + (a-1)d = F(S)$.
If $2 \leq i \leq r-2$ and $r < a-1$, since $a + id < a + (a-1)d \leq [\frac{a-2}{r}]a + (a-1)d = F(S)$, $F(S_i) = F(S)$.
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 $[\frac{a}{r}] = [\frac{a-2}{r}]$. This condition is identical to $a \pmod{r} \geq 2$.
If $i = r-1$, $a \pmod{r} = 1$ and $a > d$, $F(S_{r-1}) = [\frac{a}{r}]a + (a-2)d \neq [\frac{a-2}{r}]a + (a-1)d = F(S)$.
If $i = r-1$, $a \pmod{r} = 1$ and $a < d$, $F(S_{r-1}) = ([\frac{a}{r}]-1)a + (a-1)d = [\frac{a-2}{r}]a + (a-1)d = F(S)$. $\square$

References

[1] Ritter, S. M., *The linear diophantine problem of Frobenius for subsets of arithmetic sequences,* Arch. Math. **69** (1997), 31-39.

[2] Ritter, S. M., *On a linear diophantine problem of Frobenius: Extending the basis* , J. Number Theory **69** (1998), 201-212.

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

[4] Selmer, E. S., *On the linear diophantine problem of Frobenius*, J. reine angew. Math. **293/294** (1977), 1-17.

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