# A VARIANT OF THE FROBENIUS PROBLEM AND GENERALIZED SUZUKI SEMIGROUPS

**Gretchen L. Matthews** [1]

*Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975, USA*

gmatthe@clemson.edu

**Rhett S. Robinson** [2]

*Department of Economics, University of North Carolina, Chapel Hill, NC 27599, USA*

rrhett@email.unc.edu

*Received: , Accepted: , Published:*

## Abstract

Given relatively prime positive integers $a_1, \ldots, a_k$, let $S$ denote the set of all linear combinations of $a_1, \ldots, a_k$ with nonnegative integral coefficients. The Frobenius problem is to determine the largest integer $g(S)$ which is not representable as such a linear combination. A related question is to determine the set $B(S)$ of integers $x$ that are representable as differences $x = s_1 - a_1 = \ldots = s_k - a_k$ for some $s_i \in S$. The construction $B(S)$ can be iterated to obtain a chain of numerical semigroups. We compare this chain to the one obtained by iterating the Lipman semigroup construction. In particular, we consider these chains for generalized Suzuki semigroups.

## 1. Introduction

Let $a_1, \ldots, a_k$ be relatively prime positive integers. Then all sufficiently large integers are representable as linear combinations of $a_1, \ldots, a_k$ with nonnegative integral coefficients. The Frobenius problem is to determine the largest nonrepresentable integer. Here, we are interested in a related problem. To describe this variant, we use the language of numerical semigroups. For a general reference on numerical semigroups, see [1], [3], [4], or [5].

Throughout, $\mathbb{N}$ denotes the set of positive integers and $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ denotes the set of nonnegative integers. A numerical semigroup is an additive submonoid of $\mathbb{N}_0$ whose complement in $\mathbb{N}_0$ is finite. Given $a_1, \ldots, a_k$ as above, the numerical semigroup generated

[1]G. L. Matthews' work was supported in part by NSF DMS-0201286.

[2]This work was performed while R. S. Robinson was a student at Clemson University

by $a_1, \ldots, a_k$ is $S = \langle a_1, \ldots, a_k \rangle$ where

$$\langle a_1, \ldots, a_k \rangle := \left\{ \sum_{i=1}^{k} x_i a_i : x_i \in \mathbb{N}_0 \right\}.$$

Since there is no loss of generality in doing so, we assume that $S$ is expressed in terms of a minimal generating set; that is,

$$a_1 < \cdots < a_k \text{ and } a_i \notin \langle a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k \rangle$$

for all $1 \leq i \leq k$. In this case, the integers $a_1, \ldots, a_k$ are called the generators of $S$, and $S$ is said to be $k$-generated. The Frobenius number of $S$, denoted $g(S)$, is the largest integer in $\mathbb{N}_0 \setminus S$. Since this paper only concerns numerical semigroups, we often use the term semigroup for short.

In this paper, we consider two semigroups that can be constructed from a given one: the dual and the Lipman semigroup. The dual of a numerical semigroup $S$ is

$$B(S) := \{x \in \mathbb{N}_0 : x + S \setminus \{0\} \subseteq S\}.$$

One can check that $B(S)$ is a numerical semigroup containing $S$. The Lipman semigroup of $S$ is defined to be

$$L(S) := \langle a_2 - a_1, a_3 - a_1, \ldots, a_k - a_1 \rangle$$

where the integers $a_1, \ldots, a_k$ form a minimal generating set of $S$. Note that $S \subseteq L(S)$. Determining the dual of $S$ is related to the Frobenius problem in that $g(S)$ is the largest element of $B(S) \setminus S$.

The dual and Lipman constructions can be iterated as in [1] to obtain two chains of numerical semigroups:

$$\begin{array}{ccccccccc} B_0(S) & \subseteq & B_1(S) & \subseteq & B_2(S) & \subseteq & \ldots & \subseteq & B_{\beta(S)}(S) := \mathbb{N}_0 \\ & & & & \text{and} & & & & \\ L_0(S) & \subseteq & L_1(S) & \subseteq & L_2(S) & \subseteq & \ldots & \subseteq & L_{\lambda(S)}(S) := \mathbb{N}_0. \end{array}$$

Because $B(S) \subseteq L(S)$, it is natural to ask which semigroups $S$ satisfy

$$B_i(S) \subseteq L_i(S) \text{ for all } i \in \mathbb{N}_0. \tag{1}$$

It was conjectured in [1] that (1) holds for all numerical semigroups $S$. While this was shown to be false in [2], it does hold for several large classes of numerical semigroups, including 2-generated semigroups [2], those generated by generalized arithmetic progressions [9], and 3-generated telescopic semigroups [10]. Here, we show that (1) holds for generalized Suzuki semigroups. This gives an infinite family of telescopic 4-generated semigroups for which (1) holds.

It remains an open question to characterize those $S$ for which $B_i(S) \subseteq L_i(S)$ for all $i \in \mathbb{N}_0$; in particular, we do not know if (1) holds in the following cases: $S$ is 3-generated; $S$ is symmetric; and $S$ is telescopic. The smallest known counterexample to (1) is 4-generated but is not symmetric.

## 2. Generalized Suzuki semigroups

Given positive integers $p$ and $n$, let

$$S(p,n) = \langle a, b, c, d \rangle$$

where

$$\begin{aligned} a &= p^{2n+1}, \\ b &= p^{2n+1} + p^n, \\ c &= p^{2n+1} + p^{n+1}, \text{ and} \\ d &= p^{2n+1} + p^{n+1} + 1. \end{aligned}$$

If $p = 2$, then $S(p,n)$ is the Weierstrass semigroup of the point at infinity on the curve $X$ defined by

$$y^{p^{2n+1}} - y = x^{p^n}(x^{p^{2n+1}} - x)$$

over $\mathbb{F}_{p^{2n+1}}$ [6]. Because the automorphism group of $X$ is a Suzuki group (see [7], [11], [12]), $S(p,n)$ is sometimes called a generalized Suzuki semigroup.

We now consider some basic properties of generalized Suzuki semigroups.

**Definition 1** *Given a numerical semigroup $S$ with generators $a_1, \ldots, a_k$ (not necessarily in increasing order), let $d_i = gcd(a_1, \ldots, a_i)$ and $S_i = \left\langle \frac{a_1}{d_i}, \ldots, \frac{a_i}{d_i} \right\rangle$ for $1 \le i \le k$. Then $S$ is said to be **telescopic** if and only if $\frac{a_i}{d_i} \in S_{i-1}$ for all $i$, $2 \le i \le k$.*

**Proposition 2** *For all positive integers $p$ and $n$, $S(p,n)$ is telescopic.*

*Proof.* To see that a generalized Suzuki semigroup is telescopic, we must rearrange the generators. In particular, we express $S(p,n)$ as

$$S(p,n) = \left\langle p^{2n+1}, p^{2n+1} + p^{n+1}, p^{2n+1} + p^n, p^{2n+1} + p^{n+1} + 1 \right\rangle.$$

Then

$$d_1 = p^{2n+1}, \quad d_2 = p^{n+1}, \quad d_3 = p^n, \quad \text{and} \quad d_4 = 1.$$

It follows immediately that

$$\begin{aligned} &\tfrac{a_2}{d_2} \in \mathbb{N}_0 = \langle 1 \rangle = S_1, \\ &\tfrac{a_3}{d_3} = p^{n+1} + 1 = (p-1)p^n + (p^n + 1) \in \langle p^n, p^n + 1 \rangle = S_2, \text{and} \\ &\tfrac{a_4}{d_4} = p^{2n+1} + p^{n+1} + 1 = p^n\left(p^{n+1}\right) + \left(p^{n+1} + 1\right) \in \langle p^{n+1}, p^{n+1} + 1, p^{n+1} + p \rangle = S_3. \end{aligned}$$

Therefore $S(p,n)$ is telescopic. □

Recall that a semigroup $S$ is symmetric if and only if there is a bijection

$$\begin{array}{rccc} \phi: & S \cap \{0, \ldots, g\} & \to & \mathbb{N}_0 \setminus S \\ & s & \mapsto & g - s \end{array}$$

where $g := g(S)$ denotes the Frobenius number of $S$.

**Lemma 3** *[8, Lemma 6.5] If $S = \langle a_1, \ldots, a_k \rangle$ is telescopic (where $a_1, \ldots, a_k$ may not be in increasing order), then*

1. *the Frobenius number of $S$ is $g(S) = \sum_{i=1}^{k} \left( \frac{d_{i-1}}{d_i} - 1 \right) a_i$ where $d_0 = 0$; and*
2. *$S$ is symmetric.*

Applying Proposition 3, one can see that the Frobenius number of $S(p,n)$ is

$$g\left(S\left(p,n\right)\right) = p^{2n+1}\left(2p^n + p - 2\right) - p^{n+1} - 1.$$

## 3. Chains of semigroups

We begin this section with a discussion of two chains of semigroups that can be formed from a numerical semigroup $S$. To obtain the chain of duals, set $B_0(S) := S$ and define $B_i(S) := B\left(B_{i-1}(S)\right)$ for all $i \in \mathbb{N}$. To obtain the chain of Lipman semigroups, set $L_0(S) := S$ and define $L_i(S) := L\left(L_{i-1}(S)\right)$ for all $i \in \mathbb{N}$. Each chain is finite since $\mathbb{N}_0 \setminus S$ is finite. It is also easy to verify that $B_1(S) \subseteq L_1(S)$ since $x \in B_1(S)$ implies $x + a_1 \in S$, where $a_1$ is the smallest nonzero element of $S$. This gives

$$\begin{array}{ccccccccc} B_0(S) & \subseteq & B_1(S) & \subseteq & B_2(S) & \subseteq & \ldots & \subseteq & B_{\beta(S)}(S) \\ || & & \cap & & & & & & || \\ L_0(S) & \subseteq & L_1(S) & \subseteq & L_2(S) & \subseteq & \ldots & \subseteq & L_{\lambda(S)}(S) \end{array}$$

for any numerical semigroup $S$. In this section we will show that $B_i\left(S(p,n)\right) \subseteq L_i\left(S(p,n)\right)$ for all $i \in \mathbb{N}_0$. To do this, we first determine the chain of Lipman semigroups.

**Lemma 4** *If $S = S(p,n)$, then*

$$L_i(S) = \langle p^n, p^n(p - i + 1) + 1 \rangle$$

*for $1 \leq i \leq p$, and*

$$L_{p+1}(S) = \mathbb{N}_0.$$

*Proof.* By definition, $L_1(S) = \langle p^{2n+1}, p^n, p^{n+1}, p^{n+1} + 1 \rangle = \langle p^n, p^{n+1} + 1 \rangle$. Viewing $L_1(S)$ as $L_1(S) = \langle p^n, p^n(p - 1 + 1) + 1 \rangle$, it is easy to see that $L_i(S) = \langle p^n, p^n(p - i + 1) + 1 \rangle$ for $1 \leq i \leq p$. Taking $i = p + 1$ gives $L_{p+1} = \langle p^n, 1 \rangle = \mathbb{N}$. □

In light of Lemma 4, to prove that $B_i(S(p,n)) \subseteq L_i(S(p,n))$ for all $i \in \mathbb{N}_0$, it suffices to show that $B_i(S(p,n)) \subseteq L_i(S(p,n))$ for $2 \leq i \leq p$. The following result describes $B_i(S(p,n))$ for $i$ in this range.

**Lemma 5** *If $S = S(p,n)$ and $g = g(S)$, then*

$$B_{i+1}(S) \setminus B_i(S) = \left\{ g - \sum_{j=1}^{i} \alpha_j : \alpha_j \in \{a,b,c,d\} \right\}.$$

*for all $i$, $0 \leq i < p$.*

*Proof.* Set $B_i := B_i(S)$ for all $i \in \mathbb{N}_0$. According to Lemma 3, $S$ is symmetric. This implies $B_1 = S \cup \{g\}$ [1, Lemma I.1.8]. Thus, $B_1 \setminus S = \{g\}$, and the result holds for $i = 1$. We now proceed by induction on $i$.

Assume $B_i \setminus B_{i-1} = \{g - (\alpha_1 + \cdots + \alpha_{i-1}) : \alpha_j \in \{a,b,c,d\} \text{ for } 1 \leq j \leq i-1\}$. Define $C := \{g - (\alpha_1 + \cdots + \alpha_i) : \alpha_j \in \{a,b,c,d\} \text{ for } 1 \leq j \leq i\}$. We will show that $B_{i+1} \setminus B_i = C$.

First, we will prove that $B_{i+1} \setminus B_i \subseteq C$. Suppose $x \in B_{i+1} \setminus B_i$. This implies $x + B_i \subseteq B_i$ but $x + B_{i-1} \nsubseteq B_{i-1}$. Hence, there exists $y \in B_{i-1}$ such that $x + y \in B_i \setminus B_{i-1}$. By the induction hypothesis, $x + y = g - (\alpha_1 + \ldots + \alpha_{i-1})$ with $\alpha_j \in \{a,b,c,d\}$ for $1 \leq j \leq i-1$.

We claim that $y \in \{a,b,c,d\}$. Suppose not; that is, suppose $y = s + t$ where $s, t \in B_{i-1} \setminus \{0\}$. Then $x + s = g - (\alpha_1 + \cdots + \alpha_{i-1}) - t \in B_i$. Then, since $t \in B_{i-1} \setminus \{0\}$, $x + y = x + s + t \in B_{i-1}$, which is a contradiction. Thus, $y$ is a generator of $B_{i-1}$ and so

$$y \in \{a,b,c,d\} \cup \{g - (\alpha_1 + \cdots + \alpha_{i-2}) : \alpha_j \in \{a,b,c,d\} \text{ for } 1 \leq j \leq i-2\}.$$

Suppose $y = g - (\beta_1 + \cdots + \beta_{i-2})$ where $\beta_j \in \{a,b,c,d\}$ for all $1 \leq j \leq i-2$. Then $x = g - (\alpha_1 + \cdots + \alpha_{i-1}) - g + (\beta_1 + \cdots + \beta_{i-2})$ and so $x \leq (i-2)d - (i-1)a = (i-2)(d-a) - a$. Since $i \leq p$, we have that $x \leq (p-2)(d-a) - a = -p^{2n+1} + p^{n+2} - 2p^{n+1} - 2 < 0$ which is a contradiction. This proves the claim that $y \in \{a,b,c,d\}$. Therefore, we have that $x = g - (\alpha_1 + \ldots + \alpha_{i-1}) - y \in C$, and so $B_{i+1} \setminus B_i \subseteq C$.

Next we will show that $C \subseteq B_{i+1} \setminus B_i$. By the induction hypothesis, $C \cap B_i = \emptyset$. Hence, it suffices to show that $C \subseteq B_{i+1}$. To do this, we will see that $x + y \in B_i$ for all $x \in C$ and $y \in B_i \setminus \{0\}$ by taking the sum of the smallest elements in $C$ and $B_i \setminus \{0\}$ and showing that this is greater than the Frobenius number of $B_i$. Note that the smallest element of $C$ is $g - id$. We claim that the smallest nonzero element of $B_i$ is $a$.

Suppose there exists $z \in B_i \setminus \{0\}$ such that $z < a$. By the induction hypothesis, this yields

$$a > z \geq g - (i-1)d \geq g - (p-1)d \geq p^{2n+1} + p^{2n+1}(2p^n - 2) - p^{n+2} - p \geq a,$$

and so $a$ is the smallest nonzero element of $B_i$.

Now, we must determine the Frobenius number of $B_i$. To do this, we will use the fact that for any numerical semigroup $T$, $g(B(T)) = g(T) - \mu(T)$, where $\mu(T)$ denotes the least nonzero element of $T$ [1, Proposition I.1.11]. It follows that

$$g(B_i) = g - ia$$

since $a$ is the smallest element of $B_j$ other than 0 for all $1 \leq j \leq i$.

Suppose now that $x \in C$ and $y \in B_i \setminus \{0\}$. Then

$$x+y \geq g-id+a = g-ia-i\left(p^{n+1}+1\right)+p^{2n+1} \geq g-ia+p^{2n+1}-p^{n+2}+p^{n+1}-p+1 > g-ia$$

since $p^{2n+1}-p^{n+2}+p^{n+1}-p = p\left(p^n\left(p^n-p+1\right)-1\right) > 0$; that is, $x+y > g(B_i)$. Thus, $x \in B_{i+1}$ and so $C \subseteq B_{i+1} \setminus B_i$. Therefore,

$$B_{i+1} \setminus B_i = \left\{ g - \sum_{j=1}^{i} \alpha_j : \alpha_j \in \{a,b,c,d\} \right\}.$$

for all $i$, $0 \leq i < p$. □

**Theorem 6** *If $S = S(p,n)$, then*

$$B_i(S) \subseteq L_i(S)$$

*for all $i \geq 0$.*

*Proof.* Since $B_0(S) = S = L_0(S)$, $B_1(S) \subseteq L_1(S)$, and $L_{p+1}(S) = \mathbb{N}_0$, it suffices to show that

$$B_i(S) \subseteq L_i(S)$$

for all $2 \leq i \leq p$. To do this, we will prove that

$$B_p(S) \subseteq L_1(S).$$

According to Lemma 4, $L_1(S) = \langle p^n, p^{n+1}+1 \rangle$. Since $L_1(S)$ is telescopic (2-generated in fact), the Frobenius number of $L_1(S)$ is

$$g(L_1(S)) = p^{2n+1} - p^{n+1} - 1.$$

Let $x \in B_p(S) \setminus \{0\}$. By Lemma 5,

$$x \geq g-(p-1)d \geq g\left(L_1(S)\right) + p^{2n+1}\left(2p^n-2\right) - p^{n+2} + p^{n+1} - p + 1 > g\left(L_1(S)\right).$$

Therefore, $x \in L_1(S)$. It follows that for all $0 \leq i \leq p$,

$$B_i(S) \subseteq B_p(S) \subseteq L_1(S) \subseteq L_i(S).$$

□

# References

[1] V. Barucci, D. E. Dobbs and M. Fontana, Maximality properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains, Memoirs Amer. Math. Soc. **125/598** (1997).

[2] D. E. Dobbs and G. L. Matthews, On comparing two chains of numerical semigroups and detecting Arf semigroups, Semigroup Forum **63** (2001), 237-246.

[3] R. Fröberg, C. Gottlieb and R. Häggkvist, On numerical semigroups, Semigroup Forum **35** (1987), no. 1, 63–83.

[4] R. Fröberg, C. Gottlieb and R. Häggkvist, Semigroups, semigroup rings and analytically irreducible rings, Reports Dept. Math. Univ. Stockholm no. 1 (1986).

[5] R. Gilmer, Commutative semigroup rings. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1984.

[6] J. P. Hansen and H. Stichtenoth, Group codes on certain algebraic curves with many rational points, Appl. Algebra Engrg. Comm. Comput. **1** no. 1 (1990), 67–77.

[7] H. W. Henn, Funktionenkörper mit grosser automorphismengruppe, J. Reine Angew. Math. **302** (1978), 96–115.

[8] C. Kirfel and R. Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Trans. Inform. Theory **41** no. 6 (1995), 1720–1732.

[9] G. L. Matthews, On numerical semigroups generated by generalized arithmetic sequences, Comm. Alg. **32** no. 9 (2004), 3459–3469.

[10] G. L. Matthews, On triply-generated telescopic semigroups and chains of semigroups, Congressus Numerantium **154** (2001), 117-123.

[11] H. Stichtenoth, ber die Automorphismengruppe eines algebraischen Funktionenkrpers von Primzahlcharakteristik. I. Eine Abschtzung der Ordnung der Automorphismengruppe. Arch. Math. (Basel) **24** (1973) 527–544.

[12] H. Stichtenoth, ber die Automorphismengruppe eines algebraischen Funktionenkrpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkrpern. Arch. Math. (Basel) **24** (1973), 615–631.