Journal of Integer Sequences, Vol. 12 (2009),
Article 09.1.2

Characterizing Frobenius Semigroups by Filtration

Inga Johnson, Sean Powers, Colin Starr, Charles Trevelyan and Craig Webster
Department of Mathematics
Willamette University
Salem, OR 97301
USA
ijohnson@willamette.edu
cstarr@willamette.edu

Abstract

For a given base a, and for all integers k, we consider the sets

$$G_a(k) = \{a^k, a^k + a^{k-1}, \ldots, a^k + a^{k-1} + \cdots + a^1 + a^0\},$$

and for each $G_a(k)$ the corresponding "Frobenius set"

$$F_a(k) = \{n \in \mathbb{N} \mid n \text{ is not a sum of elements of } G_a(k)\}.$$

The sets $F_a(k)$ are nested and their union is $\mathbb{N}$. Given an integer n, we find the smallest k such that $n \in F_a(k)$.

1 Introduction and statement of result

The **Frobenius problem** for a given set $A = \{a_1, a_2, \ldots, a_n\}$ of positive relatively prime integers is the problem of finding the largest integer that cannot be expressed as a sum of (possibly repeated) elements of A. This largest such number is the *Frobenius number* of the set A, denoted by $g(A)$.

Finding the Frobenius number for sets A has been a widely studied problem since the early 1900's, when Frobenius was reported to have posed the question frequently in lectures. Sylvester [12] is widely credited with showing that for relatively prime integers a and b,

$g(\{a,b\}) = ab - (a+b)$, but he actually addressed a slightly different problem. In 1990, Curtis showed that for an arbitrary relatively prime set A the Frobenius number cannot be expressed in terms of a finite set of polynomials [2], although Greenberg and later Davison found algorithms that are reasonably quick in practice in the $n = 3$ case [3, 4]. In 1996, Ramírez-Alfonsín proved that the Frobenius problem for sets A of three or more elements is NP-hard [9]. However, R. Kannan has shown that for every fixed n, there is a method that solves the Frobenius problem in polynomial time (although the degree of the polynomial grows rapidly with n) [6].

In this paper we study a family of sets $G_a(k)$, defined below, and for each such set we study not only the Frobenius number but the set of all numbers which are not sums of elements of $G_a(k)$. More precisely, let the base $a \in \mathbb{N}$ be fixed. For each $k \in \mathbb{N}$, we define

$$G_a(k) = \{a^k, a^k + a^{k-1}, a^k + a^{k-1} + a^{k-2}, \ldots, a^k + a^{k-1} + \cdots + a^1 + a^0\}.$$

Note that the rightmost (and largest) element listed in the set above is a geometric series equal to $\frac{a^{k+1}-1}{a-1}$, and henceforth we will write it as such without further comment. For the sets $G_a(k)$ we study the Frobenius sets

$$F_a(k) = \{n \in \mathbb{N} \mid n \text{ is not a sum of the elements of } G_a(k)\}.$$

A straightforward calculation shows that the sets $F_a(k)$ are nested (i.e., $F_a(k-1) \subseteq F_a(k)$), and the union of the sets $F_a(k)$ over all k is $\mathbb{N}$. This paper investigates the following question: for arbitrary $n \in \mathbb{N}$, what is the least integer k such that $n \in F_a(k)$? We denote this least positive integer as $f_a(n) := \min\{k \mid n \in F_a(k)\}$ and call it the *Frobenius level* of n with respect to the sets $G_a(k)$.

Example 1. With $a = 2$ and $k \leq 3$, we have

$$\begin{array}{cc}
G_2(1) = \{2,3\} & F_2(1) = \{1\} \\
G_2(2) = \{4,6,7\} & F_2(2) = \{1,2,3,5,9\} \\
G_2(3) = \{8,12,14,15\} & F_2(3) = \{1,2,3,4,5,6,7,9,10, \\
 & 11,13,17,19,25,33\}
\end{array}$$

The sets $G_2(k)$, for $k = 1, 2, \ldots$ form the sequence A023758 of Sloane's Encyclopedia.

We see that $f_2(9) = 2$ and $f_2(19) = 3$; however, there is not enough information given in Example 1 to determine $f_2(30)$. I. Johnson and J. L. Merzel [5] determined the Frobenius level of an integer n with respect to the sets $G_2(k)$ while studying factorizations in the Steenrod algebra at the prime 2. Their paper serves as motivation for studying these more general sets $G_a(k)$ for arbitrary a and the solution presented in this paper is a generalization of their results. It is believed that the results presented here will have implications in the Steenrod algebra for odd primes analogous to those found at the prime 2 by Johnson and Merzel. For a discussion of the Steenrod algebra and its role in the field of algebraic topology, see [7, 10, 11, 13].

Our solution of this Frobenius level problem relies on careful study of base a arithmetic, and the following definitions and notations are required to state our result. For a positive integer n, let $[n]$ denote a base a expansion of n. This means if $w_i \in \{0, 1, \ldots, a-1\}$ for all i and

$$n = w_k a^k + w_{k-1} a^{k-1} + \cdots + w_2 a^2 + w_1 a^1 + w_0 a^0,$$

then $[n] = w_k w_{k-1} \ldots w_1 w_0$. We note that this expansion is unique up to leading zeros. For example, in base 3 (ternary) we may view $[41]$ as 1112 or 0001112. We call an ordered string of digits $b_k b_{k-1} b_{k-2} \ldots b_2 b_1 b_0$ with each digit b_i in $\{0, 1, \ldots, a-1\}$ a *base a string*, and given integers i, j such that $k \geq i + j \geq i \geq 0$ the base a string $b_{i+j} \ldots b_{i+1} b_i$ is called a *substring* of $b_k b_{k-1} b_{k-2} \ldots b_2 b_1 b_0$. We will use roman characters to denote integers and Greek letters to denote strings and substrings.

For a given base-a string β, let $|\beta|$ denote the integer with expansion β in base a. The length of the string β will be denoted by $\mathrm{len}(\beta)$. Of course, the length is only defined for a given base a string. Expressions such as $\mathrm{len}([n])$ are not well-defined and will not be used.

Let $\beta = b_{i+j} b_{i+j-1} \ldots b_i$ be a substring of $b_k \ldots b_2 b_1 b_0$. Then β is a *non-increasing substring* if and only if $b_m \leq b_{m-1}$ for $i < m \leq i+j$. That is, we will read from right to left to determine whether a string is increasing, and of course constant strings are non-increasing. (For our purposes, "*constant string*" refers to a string of length at least two in which all digits are equal.) For an arbitrary base-a string $b_k \ldots b_2 b_1 b_0$ we say that a *drop* occurs at b_m provided $b_{m+1} < b_m$. A non-increasing substring $b_{i+j} \ldots b_{i+1} b_i$ of $b_k \ldots b_2 b_1 b_0$ is said to *follow a drop* provided $i \neq 0$ and a drop occurs at b_{i-1}. Given a base a string $\beta = b_k \ldots b_m \ldots b_1 b_0$, the digit b_m is said to *contribute* to β if b_m is itself a digit in a non-increasing substring of β that follows a drop. In examples and diagrams we will underline contributing digits. We remark that a digit b_m contributes to a string β if and only if (1) a drop occurs at b_{m-1}, or (2) b_{m-1} contributes and $b_m \leq b_{m-1}$. Thus whether or not a digit contributes is completely determined by the behavior of the digit to its immediate right.

Example 2. Here is an example of a string, $\gamma = 201120100121$, with drops indicated by arrows and contributing digits underlined.

$$\gamma: \quad 2 \quad \underline{0} \quad \underline{1} \quad \underline{1} \overset{drop}{\longleftarrow} 2 \quad \underline{0} \overset{drop}{\longleftarrow} 1 \quad \underline{0} \quad \underline{0} \quad \underline{1} \overset{drop}{\longleftarrow} 2 \quad 1$$

Note that we have not indicated drops within contributing substrings since the important characteristic is whether a digit contributes.

Definition 3. For a given base-a string β, define $z(\beta)$ to be the number of digits in β that contribute to β.

For instance, in ternary, $z(\underline{0}\underline{1}2\underline{0}21000) = 3$ and $z(10\underline{1}2\underline{1}\underline{1}2) = 4$. The contributing digits have been underlined.

The function z exhibits a "*quasi-linear*" property in the sense of the following lemma.

Lemma 4. *Let β be a base-a string, $\beta = b_k \cdots b_j \cdots b_2 b_1 b_0$, where b_j is not a digit in a constant substring that follows a drop. Then*

$$z(\beta) = z(b_k \cdots b_j) + z(b_j \cdots b_1 b_0).$$

Proof. If $j = k$ or $j = 0$ the result is clear. Suppose $k > j > 0$. The assumption on b_j implies that either b_j does not contribute to β, or it does contribute and $b_j \neq b_{j+1}$ and $b_j \neq b_{j-1}$. The result is clear in the case that b_j does not contribute to β, so suppose b_j does contribute to β. Then we have the following two cases:

(i) $b_{j+1} < b_j < b_{j-1}$ (ii) $b_{j+1} > b_j$ and $b_j < b_{j-1}$.

It suffices to prove that each digit of β that contributes to β also contributes to the sum $z(b_k \cdots b_j) + z(b_j \cdots b_0)$ once and only once. In case (i), b_j contributes to $b_j b_{j-1} \ldots b_1 b_0$; however, it cannot contribute to $b_k \cdots b_{j+1} b_j$ as it cannot follow a drop. Thus the digit b_j contributes once to the sum. The digits in the substring $b_j b_{j-1} \ldots b_1$ are contributing if and only if they contribute to β. Since b_{j+1} contributes to β, the digits of the substring $b_k \cdots b_{j+1}$ contribute to $b_k \cdots b_{j+1} b_j$ if and only if they contribute to β. The proof for case (ii) is analogous except that b_{j+1} does not contribute to β and does not contribute to $b_k \cdots b_{j+1} b_j$, but all contributions from the left of b_{j+1} are the same in both strings. □

Given strings α and β, their concatenation will be denoted by $\alpha\beta$. Lastly, we define the "star" notation.

Definition 5. For nonempty strings α and β, we define the relation $*$ by

$$\alpha * \beta \Leftrightarrow |\alpha| < z(\beta)$$

Example 6. Consider the ternary string 1211111201. If $\alpha = 12$ and $\beta = 11111201$, then $z(\beta) = 6$ and $|\alpha| = 5$. In this case, $12 * 11111201$ holds; note that $\text{len}(\beta) = 8 = 7 + 1$. However, $121 * 1111201$ does not hold as $16 \not< 5$.

The following theorem is one of the main results of this paper. In Section 3 we give an algorithmic description of this theorem and briefly discuss its complexity.

Theorem 7. *Let $n \in \mathbb{N}$. Then the Frobenius level of n, $f_a(n)$, is the smallest k for which we can write $n = |\alpha\beta|$ with $len(\beta) = k + 1$ and $\alpha * \beta$.*

The previous example shows that the Frobenius level of $n = 36091 = |1211111201|$ is $f_3(36091) = 7$.

Theorem 7 reduces to the results of Johnson and Merzel when $a = 2$. In the Johnson and Merzel paper $z(\beta)$ is defined as the number of non-trailing zeros in β and our definition of $z(\beta)$ reduces to the Johnson-Merzel definition in the case $a = 2$.

2 Proof of Theorem 1

The proof of Theorem 7 is organized as follows: Lemma 8 gives a particularly useful way to represent integers that are not in $F_a(k)$. Lemmas 9 and 10 show that the sets $F_a(k)$ can be described recursively. Lemmas 13 and 14 set up technical details to assist in the proof of Theorem 15 by induction. Theorem 7 is then a corollary of Theorem 15. Along the way, Theorem 11 gives an explicit formula for the Frobenius number of $G_a(k)$ which corresponds to the well-known results of Nijenhuis and Wilf [8].

Lemma 8. *If $n \notin F_a(k)$, then there exist $c_1 \in \mathbb{Z}_{\geq 0}$, $c_2, \ldots, c_{k+1} \in \{0, \ldots, a-1\}$ such that $n = c_1 a^k + c_2(a^k + a^{k-1}) + \cdots + c_{k+1}(a^k + a^{k-1} + \cdots + a + 1)$.*

Proof. Suppose $n \notin F_a(k)$. Then there exist coefficients w_i, $1 \leq i \leq k+1$, such that

$$n = w_1 a^k + w_2(a^k + a^{k-1}) + \cdots + w_{k+1}(a^k + a^{k-1} + \cdots + a^1 + a^0).$$

If the coefficients w_i satisfy the conditions of the lemma then we are done; otherwise, let j be the largest subscript for which $w_j \geq a$. Using the division algorithm, write $w_j = aq + c_j$, where $0 \leq c_j < a$. Substitution gives

$$\begin{aligned} w_j(a^k + a^{k-1} + \cdots + a^{k-j+1}) &= (aq + c_j)(a^k + a^{k-1} + \cdots + a^{k-j+1}) \\ &= aq(a^k + a^{k-1} + \cdots + a^{k-j+1}) \\ &\quad + c_j(a^k + \cdots + a^{k-j+1}) \\ &= aq(a^k) + q(a^k + a^{k-1} + \cdots + a^{k-j+2}) \\ &\quad + c_j(a^k + \cdots + a^{k-j+1}). \end{aligned}$$

Next, define $c_m := w_m$ for all $j < m \leq k+1$. Thus n can be written as

$$\begin{aligned} n = \; & (w_1 + aq)a^k + w_2(a^k + a^{k-1}) + \cdots + w_{j-2}(a^k + a^{k-1} + \cdots + a^{k-j+3}) \\ & + (w_{j-1} + q)(a^k + a^{k-1} + \cdots + a^{k-j+2}) + c_j(a^k + a^{k-1} + \cdots + a^{k-j+1}) \\ & + c_{j+1}(a^k + a^{k-1} + \cdots + a^{k-j}) + \cdots + c_{k+1}(a^k + a^{k-1} + \cdots + a^1 + a^0). \end{aligned}$$

Now $c_j, c_{j+1}, ..., c_{k+1} \in \{0, 1, 2, \ldots, a-1\}$, and repeating the procedure above at most $j-2$ times gives the coefficients c_i in the desired range for $i = 2, 3, ..., k+1$. □

Lemma 9. *Let $n \in \mathbb{N}$, and let q and r be the unique integers such that $n = aq + r$, where $0 \leq r < a$. Let $R = r\frac{a^{k+1}-1}{a-1}$. Then $n \in F_a(k)$ if and only if $n < R$ or $\frac{n-R}{a} \in F_a(k-1)$.*

Proof. We prove that $n \notin F_a(k)$ if and only if $n \geq R$ and $\dfrac{n-R}{a} \notin F_a(k-1)$.

Suppose $n \geq R$ and $\frac{n-R}{a} \notin F_a(k-1)$. Then $\dfrac{n-R}{a}$ is a nonnegative-integral combination of the elements of $G_a(k-1)$; thus

$$\frac{n-R}{a} = c_1 a^{k-1} + c_2(a^{k-1} + a^{k-2}) + \cdots + c_k(a^{k-1} + a^{k-2} + \cdots + 1)$$

for some $c_1, \ldots, c_k \in \mathbb{Z}_{\geq 0}$. Therefore

$$n = c_1 a^k + c_2(a^k + a^{k-1}) + \cdots + c_k(a^k + a^{k-1} + \cdots + a) + R,$$

where c_1, c_2, ..., $c_k \in \mathbb{Z}_{\geq 0}$. Because $R = r\left(\frac{a^{k+1}-1}{a-1}\right) = r\left(a^k + a^{k-1} + \cdots + a + 1\right)$, $n \notin F_a(k)$.

Conversely, suppose $n \notin F_a(k)$. By Lemma 8, there exist $c_1 \in \mathbb{Z}_{\geq 0}$ and $c_2, c_3, \ldots, c_{k+1} \in \{0, \ldots, a-1\}$ such that

$$\begin{aligned} n &= c_1 a^k + c_2(a^k + a^{k-1}) + \cdots + c_{k+1}(a^k + \cdots + a + 1) \\ &= a(c_1 a^{k-1} + c_2(a^k + a^{k-1}) + \cdots + c_{k+1}(a^{k-1} + \cdots + 1)) + c_{k+1}. \end{aligned}$$

Since r is unique and $0 \leq c_{k+1} < a$, we see from the equation above that $c_{k+1} = r$. Therefore,

$$\frac{n-R}{a} = c_1 a^{k-1} + c_2(a^{k-1} + a^{k-2}) + \cdots + c_k(a^{k-1} + a^{k-2} + \cdots + 1).$$

Thus, $\frac{n-R}{a} \notin S_a(k-1)$. Since $n - R \geq 0$, $n \geq R$. $\square$

Lemma 10. *Let $n \not\equiv 0 \pmod{a}$. Then $n \in F_a(k)$ if and only if $n - \frac{a^{k+1}-1}{a-1} \in F_a(k)$.*

Proof. Let $n - \frac{a^{k+1}-1}{a-1} \notin F_a(k)$. Then $n \notin F_a(k)$ follows immediately.

Suppose $n \notin F_a(k)$. Write

$$n = c_1 a^k + c_2(a^k + a^{k-1}) + \cdots + c_{k+1}(a^k + a^{k-1} + \cdots + a + 1),$$

where $c_1 \in \mathbb{Z}^+$ and $c_2, c_3, \ldots, c_{k+1} \in \{0, 1, \ldots a-1\}$. Note that $c_{k+1} \geq 1$ since $n \not\equiv 0 \pmod{a}$. Then

$$n - \frac{a^{k+1}-1}{a-1} = c_1 a^k + c_2(a^k + a^{k-1}) + \cdots + (c_{k+1} - 1)\frac{a^{k+1}-1}{a-1},$$

which implies that $n - \frac{a^{k+1}-1}{a-1} \notin F_a(k)$. $\square$

We notice that the Frobenius number for the sets $G_a(k)$ is the largest element of $F_a(k)$, and since the sets $F_a(k)$ can be described recursively we present an easy to prove formula for $g(G_a(k))$ in Theorem 11. We note that the sets $G_a(k)$ are part of a well studied class known as sequentially redundant sets. Recall that a *sequentially redundant set* of positive integers is a set $A = \{a_1, a_2, \ldots, a_n\}$ such that for $j = 2, 3, \ldots, n$, there exist non-negative integers t_{ij} such that

$$\frac{a_j}{d_j} = \frac{1}{d_{j-1}} \sum_{i=1}^{j-1} t_{ij} a_i,$$

where $d_i = \gcd\{a_1, a_2, \ldots, a_i\}$ for each $1 \leq i \leq n$. The Frobenius number of a sequentially redundant set is well-known [8]; thus the result below is not new.

Theorem 11. *The Frobenius number of the set $G_a(k)$ is*

$$g(\{a^k, a^k + a^{k-1}, \ldots, a^k + a^{k-1} + \cdots + a^0\}) = \frac{1 - a^{k+1}k - a^{k+1} + a^{k+2}k}{a-1}$$

Proof. We proceed by induction on k. $G_a(1) = \{a, a+1\}$, so using Sylvester's formula we have $g(\{a, a+1\}) = a(a+1) - (2a+1) = (a-1)(a+1) - a$ as desired. Next we assume the formula holds for $G_a(k-1)$. Then the largest number in $S_a(k-1)$ is

$$g(G_a(k-1)) = (a-1)\left(\sum_{i=1}^{k-1}(a^{k-1} + a^{k-2} + \cdots + a^{k-1-i})\right) - a^{k-1}.$$

Lemma 9 implies that if w is the largest element of $F_a(k-1)$, then for maximal R $aw + R$ is the largest element of $F_a(k)$. The largest possible R occurs for $r = a - 1$; thus $R = a^{k+1} - 1$.

Therefore

$$
\begin{aligned}
g(G_a(k)) &= a\left((a-1)\left(\sum_{i=1}^{k-1}(a^{k-1}+a^{k-2}+\cdots+a^{k-1-i})\right)-a^{k-1}\right) \\
&\quad +a^{k+1}-1 \\
&= (a-1)\left(\sum_{i=1}^{k}(a^{k}+a^{k-1}+\cdots+a^{k-i})\right)-a^{k} \\
&= \frac{1-a^{k+1}k-a^{k+1}+a^{k+2}k}{a-1}.
\end{aligned}
$$

$\square$

The next two lemmas describe the behavior of the function z when a base-a string of ones is subtracted from a base a string with a specific form. We precede these lemmas with the following motivating example.

Example 12. Let $a = 3$ and consider the ternary string

$$\gamma = 21101000100121.$$

Let $\delta = 111\cdots 1$ be a constant ternary string of ones with $\mathrm{len}(\delta) = 14$. We first calculate $\gamma - \delta$ and add a leading zero so $\mathrm{len}(\gamma - \delta)$ remains 14; $\gamma - \delta = 02212111212010$. Next we compare $z(\gamma)$ and $z(\gamma - \delta)$. Contributing digits are underlined below.

$$
\begin{array}{lcccccccccccccc}
\gamma: & 2 & 1 & 1 & \underline{0} & 1 & \underline{0} & \underline{0} & \underline{0} & 1 & \underline{0} & \underline{0} & \underline{1} & 2 & 1 \\
 & & & & \downarrow & & \downarrow & \downarrow & \downarrow & & \downarrow & & \downarrow & & \\
\gamma-\delta: & \underline{0} & 2 & 2 & \underline{1} & 2 & \underline{1} & \underline{1} & \underline{1} & 2 & \underline{1} & 2 & \underline{0} & 1 & 0
\end{array}
$$

Thus $z(\gamma) = 7 = z(\gamma - \delta)$. The key observation to make in this example is that all contributing digits in γ are paired with contributing digits in the same position in $\gamma - \delta$ except for the rightmost contributing zero in γ, which is paired with the leading contributing digit in $\gamma - \delta$.

Lemma 13. *Suppose a base-a string $\gamma = h_n h_{n-1} \cdots h_{l+1} h_l h_{l-1} \cdots h_1 h_0$ satisfies the following conditions:*

(i) for $0 \le i \le l-1$, $h_i > 0$,

(ii) $h_l = 0$ [note: it is possible that $l = 1$],

(iii) for $l+1 \le i \le n-1$, $h_i = 0$ or 1 (possibly empty), and

(iv) $h_n > 1$.

Suppose δ is a base-a string of 1's with length $n+1$. Then $z(\gamma-\delta)=z(\gamma)$, where $\gamma-\delta$ has the same length as γ (by appending a leading zero if necessary).

Proof. Firstly, note that $a>2$ is forced by the given conditions. Now, to compute $\gamma-\delta$, we "borrow" from each digit to the left of h_l. The result is

$$\gamma-\delta=[h_n-2][h_{n-1}+a-2]\cdots[h_{l+1}+a-2][h_l+a-1][h_{l-1}-1]\cdots[h_1-1][h_0-1].$$

Since $2\leq h_n\leq a-1$, $h_n-2<a-2$. Also, h_{n-1} is either a 0 or 1 in γ. Thus, the $n-1$ digit in $\gamma-\delta$ is $a-2$ more than the $n-1$ digit of γ: it increases by a due to borrowing from h_n, loses one because the $n-2$ digit borrows from it, and loses one more from subtracting δ. The value of the $n-1$ digit of $\gamma-\delta$ is thus either $a-2$ or $a-1$. Therefore, $h_n-2<h_{n-1}+a-2$, and the n digit will be a drop in $\gamma-\delta$. However, in γ, $h_n>h_{n-1}$, so there is a drop in $\gamma-\delta$ that is not in γ.

In $\gamma-\delta$, the $l+1$ through $n-1$ digits are each $a-2$ more than h_i (since $\gamma-\delta$ requires borrowing throughout these digits), and therefore this section yields the same digit-by-digit contribution to $\gamma-\delta$ as to γ.

Note that $h_l=0$, so the l-digit of $\gamma-\delta$ is $a-1$. (Since h_l is the first zero appearing in γ, no borrowing is necessary to the right of h_l.) If $h_{l+1}=0$ (and is hence part of a non-increasing sequence to the left of a drop) in γ, then the $l+1$ digit in $\gamma-\delta$ is $a-2$ and is therefore a drop and counted as it was for $z(\gamma)$. If $h_{l+1}=1$, then the $l+1$ digit in $\gamma-\delta$ has value $a-1$ and thus is not part of a non-increasing sequence following a drop; it is again counted as it was for $z(\gamma)$. Thus, in either case, the contribution to $\gamma-\delta$ from the $l+1$ digit is the same as it is in γ.

Since $h_{l-1}-1$ is less than $a-1$ and $h_l+a-1=a-1$, the l digit in $\gamma-\delta$ is not a drop. However, the digit at position l in γ is a drop since it is the first zero appearing in γ. Thus, $\gamma-\delta$ loses a drop that γ had.

For $l-1>i\geq 1$, each digit $h_i>0$, and therefore no borrowing is required for corresponding digits in $\gamma-\delta$. Thus these digits make the same contribution to $\gamma-\delta$ as to γ.

The net result of these considerations is that the contribution in γ that occurs at h_l is moved to the leading digit in $\gamma-\delta$, but all other contributions remain the same. Therefore $z(\gamma-\delta)=z(\gamma)$, as desired.

□

Before continuing with the next lemma, we pause to recall the relation $*$: if α and β are nonempty base-a strings, then $\alpha*\beta \iff |\alpha|<z(\beta)$.

Lemma 14. *Let $\beta=b_kb_{k-1}\cdots b_2b_1b_0$ and α be strings in base a. Let $\delta=1\cdots 1$ be a string of $k+1$ ones in base a.*

Suppose

(a) $\beta\not\equiv 0 \pmod{a}$,

(b) $z(\beta)>0$, *and*

(c) $|\alpha|>0$.

Then

(i) for $|\beta| > |\delta|$, $\alpha * \beta \Leftrightarrow \alpha * (\beta - \delta)$, and

(ii) for $|\beta| < |\delta|$, $\alpha * \beta \Leftrightarrow [|\alpha| - 1] * ([1]\beta - \delta)$, where 1 and β are concatenated to create $[1]\beta > \delta$.

Proof. **Case (i):** Suppose $|\beta| > |\delta|$. Then either β is zero-free or it contains a zero. If β is zero-free, then $\beta - \delta$ requires no borrowing, so $z(\beta) = z(\beta - \delta)$ and α does not change. (Note: this also implies that in Case (i), the hypotheses $|\alpha| > 0$ is unnecessary.) Thus $\alpha * \beta \iff \alpha * (\beta - \delta)$.

Now suppose that β contains at least one zero. Write $\beta = b_k b_{k-1} \cdots b_1 b_0$. Inductively define substrings β_i, $i = 1, 2, \dots m$, for $m < k + 1$, as follows:

$$\beta_1 = b_{j_1} \cdots b_{l_1} \cdots b_1 b_0,$$

where l_1 is the smallest subscript in β such that $b_{l_1} = 0$, and $j_1 > l_1$ is the smallest subscript in β such that $b_{j_1} > 1$. Note that this subscript exists since $|\beta| > |\delta|$. If $b_w = 0$ for some $w > j_1$, then define $\beta_2 = b_{j_2} \cdots b_{l_2} \cdots b_{j_1}$, where $l_2 > j_1$ is the smallest subscript such that $b_{l_2} = 0$, and $j_2 > l_2$ is the smallest subscript such that $b_{j_2} > 1$. A diagram of the basic structure of each β_i is included below.

$$\overbrace{\underbrace{b_{j_i}}_{>1}\ \underbrace{\cdots}_{\leq 1}\ \underbrace{b_{l_i}}_{=0}\ \underbrace{\cdots b_{j_{i-1}}}_{\neq 0}}^{\beta_i}$$

Create successively $\beta_1, \beta_2, \beta_3, \dots, \beta_m$ as above, where either b_k appears in β_m or $b_w > 0$ for all $w > j_m$. In the former case, define β_{m+1} to be the empty string; in the latter case, define $\beta_{m+1} = b_k b_{k-1} \cdots b_{j_m}$. The following diagram gives a picture of β and the β_i substrings.

$$\begin{array}{ll} \beta : & \overbrace{b_k \cdots b_{j_m}}^{\beta_{m+1}}\ \overbrace{\cdots \underline{b_{l_m}} \cdots b_{j_{m-1}}}^{\beta_m}\ \cdots\ \overbrace{b_{j_1} \cdots \underline{b_{l_1}} \cdots b_0}^{\beta_1} \\ \beta - \delta : & \qquad \underline{b_{j_m} - 2} \qquad\qquad\qquad\qquad \underline{b_{j_1} - 2} \end{array}$$

The β_i satisfy the hypotheses of Lemma 13 and of quasi-linearity. Thus each b_{l_i} is contributing in β and is paired with the contributing digit $b_{j_i} - 2$ in $\beta - \delta$.

Let δ_i denote a string of ones of length $\mathrm{len}(\beta_i)$ for $i = 1, \dots, m + 1$. We compute:

$$\begin{aligned} z(\beta) &= \sum_{i=1}^{m+1} z(\beta_i) \ \text{ by quasi-linearity} \\ &= \sum_{i=1}^{m+1} z(\beta_i - \delta_i) \ \text{ by Lemma 13.} \end{aligned}$$

It remains to show that $\sum_{i=1}^{m+1} z(\beta_i - \delta_i) = z(\beta - \delta)$. Notice that quasi-linearity does not apply to the strings $\beta_i - \delta_i$ as the leading digit of $\beta_i - \delta_i$ is one less than the last digit of

$\beta_{i+1} - \delta_{i+1}$. However, we can piece these strings together to form $\beta - \delta$ by deleting the last digit of each $\beta_i - \delta_i$ for $i = 2, \dots, m+1$ and concatenating appropriately. Recall that these last digits are not contributing digits to $\beta_i - \delta_i$ so none of them are underlined. In addition, every digit in each $\beta_i - \delta_i$ has the same right neighbor after forming $\beta - \delta$ (by deletion and concatenation) except $b_{j_{i-1}+1} - 1$, so we must only show that $b_{j_{i-1}+1} - 1$, for $i = 2, \dots, m+1$, contributes to $\beta_i - \delta_i$ if and only if it contributes to $\beta - \delta$. (That is, we must show that the deletion-concatenation procedure does not disturb any underlining.)

Now

$$\begin{aligned} b_{j_{i-1}+1} - 1 \text{ contributes to } \beta_i - \delta_i \quad &\Longleftrightarrow \quad b_{j_{i-1}+1} - 1 < b_{j_{i-1}} - 1 \\ &\Longleftrightarrow \quad b_{j_{i-1}+1} - 1 \leq b_{j_{i-1}} - 2. \end{aligned}$$

We know from the proof of Lemma 13 that $b_{j_{i-1}} - 2$ contributes to $\beta_{i-1} - \delta_{i-1}$, and hence to $\beta - \delta$. This implies that $b_{j_{i-1}+1} - 1 \leq b_{j_{i-1}} - 2$ if and only if $b_{j_{i-1}+1} - 1$ contributes to $\beta - \delta$.

Thus each contribution to $\beta_i - \delta_i$ is counted once and only once in $\beta - \delta$, so $\sum_{i=1}^{m+1} z(\beta_i - \delta_i) = z(\beta - \delta)$.

Case (ii): Now consider $|\beta| < |\delta|$. If β has no digits larger than 1, then form $\tilde{\beta}$ as below (with $t = -1$). If β has a digit larger than 1, let t be the largest integer such that $b_t > 1$. Apply case (i) to $\beta' = b_t \dots b_1 b_0$ and $\delta' = 1 \dots 1$, a string of $t+1$ ones. Then $z(\beta') = z(\beta' - \delta')$.

Consider $\tilde{\beta} = [1] b_k b_{k-1} \dots b_{t+1} = [a + b_k] b_{k-1} \dots b_{t+1}$ where $b_{t+1}, \dots, b_k \in \{0, 1\}$. Let $s \geq t+1$ be the least integer such that $b_s = 0$. Note that such a b_s exists since $|\beta| < |\delta|$. Let $\tilde{\delta} = 1 \dots 1$ be a string of $k - t$ ones. For i from $t+1$ through k, the digits c_i of $\tilde{\beta} - \tilde{\delta}$ are as follows:

$$\begin{cases} c_i = 0, & \text{if } t+1 \leq i < s; \\ c_s = a - 1; & \\ c_i = a - 1, & \text{if } i > s \text{ and } b_i = 1; \\ c_i = a - 2, & \text{if } i > s \text{ and } b_i = 0. \end{cases}$$

If $t \geq 0$, then the digits labelled $t+1$ through $s-1$ of $\tilde{\beta}$ are all 1, and the corresponding digits of $\tilde{\beta} - \tilde{\delta}$ are all 0. Since the $t+1$ digit is a drop in either case, both strings contribute the same. If $t = -1$, then digits $t+1 = 0$ through $s-1$ of $\tilde{\beta}$ are all 1 (since $\beta \not\equiv 0 \pmod{a}$) and the corresponding digits of $\tilde{\beta} - \tilde{\delta}$ are all 0, and none of these contribute. Note that the string of digits from $t+1$ to $s-1$ could be empty.

Now $b_s = 0$ contributes to $\tilde{\beta}$ since it is a drop from the preceding digit, but the sth digit of $\tilde{\beta} - \tilde{\delta}$ does not contribute since it equals $a - 1$. Thus, the contributions in β up through the sth digit are $z(\beta') + (s - t - 1) + 1$, and the contributions in $[1]\beta - \delta$ up through the sth digit are $z(\beta') + (s - t - 1)$.

From the table above, we see that the $s+1$ through k digits contribute in β if and only if they contribute in $[1]\beta - \delta$ since $0 \leftrightarrow a - 2$ and $1 \leftrightarrow a - 1$. For b_s becomes $a - 1$ in $\tilde{\beta} - \tilde{\delta}$. Therefore, if $b_{s+1} = 0$ (and therefore contributes to β), then the $s+1$ digit of $\tilde{\beta} - \tilde{\delta}$ is $a - 2$, which contributes to $\tilde{\beta} - \tilde{\delta}$. If $b_{s+1} = 1$ (and therefore does not contribute to β), then the $s+1$ digit of $\tilde{\beta} - \tilde{\delta}$ is $a - 1$, which does not contribute to $\tilde{\beta} - \tilde{\delta}$. The remaining digits of $\tilde{\beta} - \tilde{\delta}$ may be considered in the same way.

Thus, overall, we have $z([1]\beta - \delta) = z(\beta) - 1$ since only the sth digit contributes differently in β and $\tilde{\beta} - \tilde{\delta}$.

$\square$

Theorem 15. *For nonempty strings α and β with $|\alpha\beta| \neq 0$,*

$$\alpha * \beta \Leftrightarrow |\alpha\beta| \in F_a(len(\beta) - 1).$$

Proof. We proceed by induction on $n := |\alpha\beta|$. Set $k := len(\beta) - 1$, so the theorem asserts $\alpha * \beta \Leftrightarrow n \in F_a(k)$.

If $n = 1$, then $|\alpha| = 0, |\beta| = 1$, $\beta = \underbrace{0 \cdots 01}_{k+1 \text{ digits}}$ and $z(\beta) = k$, so $\alpha * \beta \Leftrightarrow |\alpha| < z(\beta) \Leftrightarrow 0 < k \Leftrightarrow 1 \in F_a(k)$, where the last equivalence follows from the definition of $F_a(k)$ and the fact that $1 \in F_a(k)$ exactly when $k > 0$.

Now assume that $n > 1$ and that the theorem holds for all smaller positive integers.

(i) Suppose $n \equiv 0 \pmod{a}$.

Write $\beta = \beta'0$, and note $\text{len}(\beta') = k$ and $z(\beta) = z(\beta')$ since appending a zero to the right of β' cannot introduce a drop. Then

$$\alpha * \beta \Leftrightarrow \alpha * \beta' \Leftrightarrow \frac{n}{a} = |\alpha\beta'| \in F_a(k-1) \Leftrightarrow n \in F_a(k),$$

where the second equivalence follows by induction and the last from Lemma 9 since $R = 0$.

(ii) Suppose $n \not\equiv 0 \pmod{a}$. Note that this implies that in base a, the last digit of β is nonzero. There are three cases:

(a) Suppose $z(\beta) = 0$. Then β has no drops and thus can be written as a sum of the elements in $G_a(k)$. Then $|\beta| = c_1 a^k + \cdots + c_{k+1}(a^k + \cdots + a + 1)$, and $n = |\alpha| \cdot a^{k+1} + c_1 a^k + \cdots + c_{k+1}(a^k + \cdots + a + 1) \notin F_a(k)$. In this case, $\alpha * \beta$ and $n \in F_a(k)$ are both false.

(b) Suppose $z(\beta) > 0$ and $|\alpha| = 0$. Certainly $n = |\beta| \leq a^{k+1} - 1$. In fact, since β has a drop, we have $n < a^{k+1} - 1$. (The base-a digits of β cannot all equal $a - 1$ since β has a drop.) There are two cases.

(1) If $|\beta| < a^k + \cdots + a + 1$, then $n < R$ ($n \not\equiv 0 \pmod{a} \implies R \geq a^k + \ldots + a^1 + a^0$). Thus, by Lemma 9, $n \in F_a(k)$, and therefore $\alpha * \beta$ and $n \in F_a(k)$ are both true.

(2) Again let δ be a string of $k+1$ ones in base a, and assume that $a^k + \cdots + a + 1 \leq |\beta| < a^{k+1} - 1$. Since $|\alpha| = 0$, we may apply Lemma 9 to obtain

$$\alpha * \beta \Leftrightarrow \alpha * (\beta - \delta) \Leftrightarrow |\alpha\beta| - |\delta| = n - (a^k + \ldots + a + 1) \in F_a(k) \Leftrightarrow n \in F_a(k),$$

where it is understood that $\text{len}(\beta - \delta) = \text{len}(\beta)$. The first equivalence follows from Lemma 14 (recall that the hypothesis $|\alpha| > 0$ was unnecessary for Case (i)), the second from the induction hypothesis, and the last from Lemma 10.

(c) Suppose $z(\beta) > 0$ and $|\alpha| > 0$; then by Lemma 14

$$\begin{aligned}\alpha * \beta &\Leftrightarrow \alpha * (\beta - \delta) \text{ or } \ [|\alpha| - 1] \ * ([1]\beta - \delta) \\ &\Leftrightarrow n - (a^k + \cdots + a + 1) \in F_a(k) \\ &\Leftrightarrow n \in F_a(k),\end{aligned}$$

where the first equivalence follows from Lemma 14, the second from the induction hypothesis, and the last from Lemma 10.

□

Theorem 7 is actually a corollary of Theorem 15. One can easily compute $f_a(n)$ from Theorem 7. Here are a few example calculations. Notice that to apply Theorem 7 it may be necessary to write a string with leading zeros.

Corollary 16. *Let $n \in \mathbb{Z}^+$. Then $n \in F_a(k)$ if and only if there exist base-a strings α and β such that*

1. $|\alpha\beta| = n$,
2. $\alpha * \beta$, *and*
3. $k = len(\beta) - 1$.

Proof. If such strings α and β exist, then $n = \alpha\beta \in F_a(k)$ by Theorem 15. Conversely, if $n \in F_a(k)$, then let β be the last $k+1$ digits of a base-a representation of n, and let α be the remaining digits, setting $\alpha = 0$ if otherwise α would be empty. This gives $|\alpha\beta| = n$ and $k = \text{len}(\beta) - 1$ directly. Furthermore, since $|\alpha\beta| = n \in F_a(k), \alpha * \beta$ by Theorem 15. □

Example 17.

1. For $n = 24 = |11000| = |0011000|$ with base $a = 2$, let $\alpha = 0$ and $\beta = 011000$; then $|\alpha\beta| = 24$ and $0 = |\alpha| < z(\beta) = 1$. We see that $f_2(24) = \text{len}(\beta) - 1 = 5$ since for no shorter β will we have a drop.

2. In ternary, for $n = 50_{10} = |1212_3|$, let $\alpha = 0$ and $\beta = 1212$; then $|\alpha\beta| = 50$ and $0 = |\alpha| < z(\beta) = 2$. Thus $f_3(50) = \text{len}(\beta) - 1 = 3$.

3. In base 7, for $n = 22413_{10} = |122226_7|$, let $\alpha = 1$ and $\beta = 22226$; then $|\alpha\beta| = 22413$ and $1 = |\alpha| < z(\beta) = 4$. Therefore $f_7(22413) = 4$.

We note that Theorem 15 and Corollary 16 completely characterize the Frobenius sets, $F_a(k)$. In addition, if $n \notin F_a(k-1)$ there is a simple algorithm giving n as a non-negative linear combination of the elements of $G_a(k-1)$.

Representation Algorithm: Assuming $n \notin F_a(k-1)$ the following algorithm gives $t_i \geq 0$ such that

$$n = t_0 a^{k-1} + t_1(a^{k-1} + a^{k-2}) + t_2(a^{k-1} + a^{k-2} + a^{k-3}) + \cdots + t_k(a^{k-1} + \cdots + a^1 + a^0).$$

1. Write n in base a as $n = c_r \cdots c_1 c_0$.
2. Let $t_k := c_0$ and $Remain := n - t_k(a^{k-1} + \cdots + a^1 + a^0)$.
3. If $Remain = 0$, put $t_{k-1} = t_{k-2} = \cdots = t_0 := 0$, then STOP.
4. Let $m := 1$.
5. Write $Remain$ in base a as $c_{mr} \ldots c_{m2} c_{mm} \overbrace{00\ldots0}^{m \text{ zeros}}$.
6. Let $t_{k-m} := c_{mm}$ and put $Remain := Remain - t_{k-m}(a^{k-1} + a^{k-2} + \cdots + a^m)$.
7. If $Remain = 0$, put $t_{k-m-1} = t_{k-m-2} \cdots = t_0 := 0$, then STOP.
8. If $Remain > 0$, put $m := m + 1$. If $m < k$ GOTO step (5).
9. If $Remain > 0$ and $m = k$, put $t_0 = \frac{Remain}{a^k}$. STOP.

Here is an example using the Representation Algorithm.

Example 18. Suppose $a = 3$. Let $n = 1541 = 2 \cdot 3^6 + 3^4 + 2$. The ternary representation of 1541 is 2010002. Since $2 * 010002$ holds but $20 * 10002$ is false, $1541 \in F_3(5)$ but $1541 \notin F_3(4)$ by Corollary 16. Recall that $G_3(4) = \{81, 108, 117, 120, 121\}$. We begin by writing the elements of $G_3(4)$ in base $a = 3$: $[G_3(4)]_3 = \{10000, 11000, 11100, 11110, 11111\}$. We will find non-negative coefficients t_i such that

$$2010002 = t_0(10000) + t_1(11000) + t_2(11100) + t_3(11110) + t_4(11111)$$

The ternary representation of 1541 implies $t_4 = 2$. The next few steps outlined below involve subtracting the appropriate multiple of the elements of $G_3(4)$. The quantity $Remain$ is changed by each subtraction and each new $Remain$ amount gives another t_i.

$$\begin{array}{rrr}
 & \text{Step 1} & \text{Step 2} \\
n = & 2010002 & 1210010 \\
 & \underline{-22222} & \underline{-11110} \\
Remain: & 1210010 & 1121200 \\
 & \Longrightarrow\ t_3 = 1 & \Longrightarrow\ t_2 = 2
\end{array}$$

$$\begin{array}{rrr}
 & \text{Step 3} & \text{Step 4} \\
n = & 1121200 & 1022000 \\
 & \underline{-22200} & \underline{-22000} \\
Remain: & 1022000 & 1000000 \\
 & \Longrightarrow\ t_1 = 2 & \Longrightarrow\ t_0 = 9
\end{array}$$

3 Theorem 15 as an Algorithm

Fix the integer $a \geq 2$. In this section we present the algorithm for determining, given $n \in \mathbb{Z}^+$, the least k such that $n \in F_a(k)$. We then briefly discuss the computational complexity of our algorithm.

Algorithm:

1. Write n in base $a : n = c_k \cdots c_1 c_0$.
2. Let $\alpha_0 := c_k \cdots c_1$ and $\beta_0 := c_0$.
3. If $\alpha_0 * \beta_0$, then $n \in F_a(0)$. STOP.
4. If not $\alpha_0 * \beta_0$, let $l := 1$.
5. Let $\alpha_l := c_k \cdots c_{l+1}$ and $\beta_l := c_l \cdots c_0$.
6. If $\alpha_l * \beta_l$, then $n \in F_a(l)$. STOP.
7. If $l < k - 1$, then put $l := l + 1$. GOTO step 5.
8. Let $\alpha_k := 0$ and $\beta_k := c_k \cdots c_0$.
9. If $\alpha * \beta$, then $n \in F_a(k)$. STOP.
10. Let $\alpha_{k+1} := 0$ and $\beta_{k+1} = 0c_k \cdots c_0$. Then $|\alpha| = 0$ and $z(\beta_{k+1}) = 1$, so $\alpha * \beta$ and $n \in F_a(k+1)$. STOP.

It is clear that the above algorithm terminates. Furthermore, since the algorithm checks membership in $F_a(k)$ for each value of k sequentially beginning with $k = 0$, it must determine the least value of k such that $n \in F_a(k)$, as desired.

In the worst case, steps 5 through 7 are repeated at most $\log_a(n-1) + 1$ times. Each iteration requires about $\log_a(n)$ operations (mostly from computation of $z(\beta)$). Steps outside of this loop require minimal computation, so the algorithm is $O(\log_a^2(n))$. Note that this algorithm can be improved to $O(\log(n))$ by repeated bisection of the base-a representation of n.

We note in closing that a working group at Willamette University has studied a similar Frobenius-level problem for the following related G-sets. For positive integers a, b, c, d such that $\gcd(a,b) = \gcd(c,d) = 1$ and $a < b$, define $G(0) = \{a, b\}$, $G(1) = \{ac, bc, bc + d\}$, and for $k \geq 2$

$$G(k) = \{ac^k, bc^k, bc^k + dc^{k-1}, bc^k + dc^{k-1} + dc^{k-2}, \ldots, bc^k + dc^k + \cdots + dc^0\}.$$

They have found necessary and sufficient conditions for nested corresponding Frobenius-sets. They are working to solve the Frobenius-level problem for these more general sequentially redundant sets [1].

References

[1] P. Cudworth, T. Dailey, M. Flink, G. Houser, I. Johnson, B. Kehr, P. Le, J. Petersen, and C. Starr, Characterizing a generalized infinite family of Frobenius semigroups by filtration, in preparation.

[2] F. Curtis, On formulas for the Frobenius number of a numerical semigroup, *Math. Scand.* **67** (1990), 190–192.

[3] J. L. Davison, On the linear Diophantine problem of Frobenius, *J. Number Theory* **48** (1994), 353–363.

[4] H. Greenberg, Solution to a linear Diophantine equation for nonnegative integers, *J. Algorithms* **9** (1988), 343–353.

[5] I. Johnson and J. L. Merzel, A class of left ideals of the Steenrod algebra, *Homology, Homotopy Appl.* **9** (2007), 185–191.

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

[7] R. E. Mosher and M. C. Tangora, *Cohomology Operations and Applications in Homotopy Theory*, Harper & Row, 1968.

[8] Albert Nijenhaus and Herbert S. Wilf, Representations of integers by linear forms in nonnegative integers, *J. Number Theory* **4** (1972), 98–106.

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

[10] D. C. Ravenel, *Complex Cobordism and Stable Homotopy Groups of Spheres,* Academic Press, 1986.

[11] N. E. Steenrod and D. B. A. Epstein, *Cohomology Operations,* Princeton University Press, 1962.

[12] J. J. Sylvester, Problem 7382, *Math. Quest. Sol. Educational Times* **41** (1884), ix, 21.

[13] R. M. W. Wood, Problems in the Steenrod algebra, *Bull. London Math. Soc.* **30** (1998), 449–517.

2000 *Mathematics Subject Classification*: Primary 11B37.
Keywords: Frobenius problem, Frobenius level, sequentially redundant, Frobenius semigroup.

(Concerned with sequence A023758.)

Received August 1 2006; revised versions received August 31 2007; September 13 2008; October 20 2008. Published in *Journal of Integer Sequences*, December 14 2008.

Return to Journal of Integer Sequences home page.