The Parametric Frobenius Problem

Bjarke Hammersholt Roune[*]
Department of Mathematics
University of Kaiserslautern
Kaiserslautern, Germany
bjarke.roune@gmail.com

Kevin Woods
Department of Mathematics
Oberlin College
Oberlin, Ohio, USA
Kevin.Woods@oberlin.edu

Submitted: Mar 18, 2015; Accepted: May 9, 2015; Published: May 22, 2015
Mathematics Subject Classifications: 11D07, 52C07, 11H06

Abstract

Given relatively prime positive integers $a_1, \dots, a_n$, the Frobenius number is the largest integer that cannot be written as a nonnegative integer combination of the a_i. We examine the parametric version of this problem: given $a_i = a_i(t)$ as functions of t, compute the Frobenius number as a function of t. A function $f : \mathbb{Z}_+ \to \mathbb{Z}$ is a quasi-polynomial if there exists a period m and polynomials $f_0, \dots, f_{m-1}$ such that $f(t) = f_{t \bmod m}(t)$ for all t. We conjecture that, if the $a_i(t)$ are polynomials (or quasi-polynomials) in t, then the Frobenius number agrees with a quasi-polynomial, for sufficiently large t. We prove this in the case where the $a_i(t)$ are linear functions, and also prove it in the case where n (the number of generators) is at most 3.

1 Introduction

Given positive integers a_i, $1 \leqslant i \leqslant n$, let

$$\langle a_1, \dots, a_n \rangle = \left\{ \sum_{i=1}^{n} p_i a_i \,\middle|\, p_i \in \mathbb{Z}_{\geqslant 0} \right\}$$

be the semigroup generated by the a_i. If the a_i are relatively prime, define the *Frobenius number* $F(a_1, \dots, a_n)$ to be the largest integer not in $\langle a_1, \dots, a_n \rangle$. The *Frobenius problem* of determining $F(a_1, \dots, a_n)$ has a long history — Sylvester proved [8] in 1884 that $F(a, b) = ab - a - b$, and see Ramírez Alfonsín's book [5] for many subsequent results.

It will be convenient to also define $F(a_1, \dots, a_n)$ in the case where the a_i are not relatively prime, so that there is no largest integer not in the semigroup. A reasonable

[*] Currently at Google. Research supported by Algorithmische und Experimentelle Methoden in Algebra, Geometrie und Zahlentheorie (SPP 1489).

definition seems to be the largest integer in the group $\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$ that is not in the semigroup $\langle a_1, \ldots, a_n \rangle$. That is, if d is the greatest common divisor of $a_1, \ldots, a_n$, then $F(a_1, \ldots, a_n) = dF(\frac{a_1}{d}, \ldots, \frac{a_n}{d})$. Sylvester's identity then becomes $F(a, b) = \operatorname{lcm}(a, b) - a - b$.

The *parametric Frobenius problem* is, given functions $a_i : \mathbb{Z}_+ \to \mathbb{Z}_+$ to determine $F\big(a_1(t), \ldots, a_n(t)\big)$ as a function of t. For example, using Sylvester's identity,

$$F(t, t+2) = \begin{cases} t(t+2) - t - (t+2) & \text{if } t \text{ is odd,} \\ \frac{t(t+2)}{2} - t - (t+2) & \text{if } t \text{ is even.} \end{cases}$$

We see that $F(t, t+2)$ is a *quasi-polynomial*; a function $f : \mathbb{Z}_+ \to \mathbb{Z}$ is a quasi-polynomial if there exist an $m \in \mathbb{Z}_+$ and polynomials $f_0, \ldots, f_{m-1} \in \mathbb{Q}[t]$ such that $f(t) = f_{t \bmod m}(t)$ for all $t \in \mathbb{Z}_+$. Here m is a *period* of f and the f_i are *components* of f. We will assume that all of our functions are integer-valued, but note that the $F(t, t+2)$ example shows that we may need polynomials with rational coefficients.

In general, our functions may misbehave for small t. We say that a property is *eventually* true if it is true for all sufficiently large t. We say that $f(t) \in \mathrm{EQP}$ (short for *eventual quasi-polynomial*) if $f(t)$ eventually agrees with a quasi-polynomial. We say that the *degree* of $f \in \mathrm{EQP}$ is the maximum degree of its components.

We conjecture that, if $a_i(t) \in \mathrm{EQP}$, then $F\big(a_1(t), \ldots, a_n(t)\big) \in \mathrm{EQP}$. We prove this for the special case where the $a_i(t)$ are linear functions and for the special case where $n \leqslant 3$.

Conjecture 1.1. *Suppose that $a_i(t) \in \mathrm{EQP}$, $1 \leqslant i \leqslant n$, are eventually positive. Then $F\big(a_1(t), \ldots, a_n(t)\big) \in \mathrm{EQP}$.*

Theorem 1.2. *Suppose that $a_i(t) \in \mathrm{EQP}$, $1 \leqslant i \leqslant n$, are eventually positive and have degree at most 1. Then $F\big(a_1(t), \ldots, a_n(t)\big) \in \mathrm{EQP}$, with degree at most 2.*

Theorem 1.3. *Suppose that $a_i(t) \in \mathrm{EQP}$, $1 \leqslant i \leqslant n$, are eventually positive, with $n \leqslant 3$. Then $F\big(a_1(t), \ldots, a_n(t)\big) \in \mathrm{EQP}$.*

These results are examples of so-called "unreasonable" appearances of quasi-polynomials, as discussed by Woods [10]. "Reasonable" appearances trace back to Ehrhart's classical result [3] that, if $P \subseteq \mathbb{R}^n$ is a polytope with rational vertices, then $f(t) = \#(tP \cap \mathbb{Z}^n)$ is a quasi-polynomial. Note that if P is defined with linear inequalities $\mathbf{b}_i \cdot \mathbf{x} \leqslant c_i$, then tP is defined with linear inequalities $\mathbf{b}_i \cdot \mathbf{x} \leqslant c_i t$. As t changes, these linear inequalities move, but their normal vectors $(\mathbf{b}_i)$ remain the same. Indeed, Woods proved [11] that any example over the integers defined with linear inequalities, boolean operations (and, or, not), and quantifiers ($\forall$, $\exists$) has this quasi-polynomial behavior. This is true even if there is more than one parameter; for example,

$$\#\left\{(x, y) \in \mathbb{Z}^2_{\geqslant 0} \,\middle|\, 2x \leqslant t,\ 3y \leqslant s\right\} = \left(\left\lfloor \frac{t}{2} + 1 \right\rfloor\right)\left(\left\lfloor \frac{s}{3} + 1 \right\rfloor\right)$$

is a quasi-polynomial of period 2 in t and period 3 in s.

If we look at the parametric Frobenius problem, however, we see that it does not fit this pattern. For example, if we want to ask whether $u \in \langle t, t+1, t+2\rangle$, we are asking whether the polytope

$$\left\{(x,y,z) \in \mathbb{R}^3_{\geqslant 0} \,\middle|\, u = tx + (t+1)y + (t+2)z\right\}$$

contains any integer points. For a fixed t, this is a 2-dimensional triangle in $\mathbb{R}^3$; as t changes, this triangle "twists" (the normal vector changes). Examples such as this were categorized in [10] as "unreasonable", though they are conjectured to still lead to eventual quasi-polynomial behavior.

This paper adds a third example to the list of recent results demonstrating this phenomenon; previously Chen, Li, and Sam [2] showed that the number of integer points in a polytope whose vertices are rational functions of t is in EQP, and Calegari and Walker [1] showed that the vertices of the integer hull of such a polytope have coordinates in EQP. A critical tool used in all of these results is that the division algorithm and the gcd of polynomials has quasi-polynomial behavior (cf. Lemma 3.1); for example, the Euclidean algorithm yields

$$\gcd(2t+1, 5t+6) = \gcd(t+4, 2t+1) = \gcd(7, t+4) = \begin{cases} 7 & \text{if } t \equiv 3 \bmod 7, \\ 1 & \text{otherwise.} \end{cases}$$

Note that unlike in the "reasonable" case, these results only hold with one parameter variable. For example $F(s,t) = \operatorname{lcm}(s,t) - s - t$ is not a quasi-polynomial in s and t.

The original inspiration for this paper comes from a conjecture of Wagon [9] (see [4, Section 17]) that, for any fixed M and residue class j of t mod M^2, there exist (usually positive) integers $c_{M,j}$ and $d_{M,j}$ such that eventually

$$F(t, t+1^2, t+2^2, \ldots, t+M^2) = \frac{1}{M^2}\left(t^2 + c_{M,j}t\right) - d_{M,j}.$$

Using the proof of Theorem 1.2, we can prove that there is indeed quasi-polynomial behavior with period M^2. In fact, such a result holds in greater generality:

Corollary 1.4. *Suppose $b_1 < b_2 < b_3 < \cdots < b_n$ are integers. Then $F(t+b_1, t+b_2, \ldots, t+b_n) \in$ EQP with period $b_n - b_1$.*

When the b_i form an arithmetic sequence, a precise quasi-polynomial formula was previously given by Roberts [6]:

$$F(t, t+d, \ldots, t+sd) = \left(\left\lfloor \frac{t-2}{s} \right\rfloor + 1\right)t + (d-1)(t-1) - 1.$$

In Section 2, we work through the example

$$F(t, t+1, t+2) = \left(\left\lfloor \frac{t-2}{2} \right\rfloor + 1\right)t - 1 = \begin{cases} \frac{t^2}{2} & \text{if } t \text{ even,} \\ \frac{t^2}{2} - \frac{t}{2} - 1 & \text{if } t \text{ odd,} \end{cases}$$

which will give a flavor of our general proof. In Section 3, we prove Theorem 1.2. In Section 4, we prove the various lemmas needed. In Section 5, we prove Corollary 1.4. In Section 6, we prove Theorem 1.3, using Rødseth's algorithm [7] for the 3 generator Frobenius problem.

The proof of Theorem 1.2 relies on the fact that semigroups with only two generators are much easier to deal with. Indeed, we have the following definition and lemma:

Definition 1.5. Let $a, b \in \mathbb{Z}_+$ be relatively prime, and let $c \in \mathbb{Z}$. The *canonical form* for c is given by $c = pa + qb$ with $p, q \in \mathbb{Z}$ and $0 \leqslant p < b$.

Lemma 1.6. *Let $a, b \in \mathbb{Z}_+$ be relatively prime, and let $c \in \mathbb{Z}$.*

1. *The canonical form for c exists and is unique. In particular, if $c = p'a + q'b$ is any form with $p', q' \in \mathbb{Z}$, and if k and r are the quotient and remainder when p' is divided by b, then the canonical form for c is $ra + (q' + ka)b$.*

2. *If $c = pa + qb$ is in canonical form, $c \in \langle a, b\rangle$ if and only if $q \geqslant 0$.*

2 An Example

In this example, we compute $F(t, t+1, t+2)$. Let $a = t$, $b = t+1$, and $c = t+2$ be our three generators, let $S = \langle a, b, c\rangle$, and let $T = \langle a, c\rangle$. Notice that $2b = a + c$. This implies that $S = T \cup (b + T)$, as follows: if $pa + qb + rc$ is a representation of an element of S, with $p, q, r \in \mathbb{Z}_{\geqslant 0}$ and $q \geqslant 2$, then $(p+1)a + (q-2)b + (r+1)c$ is also a representation, so we may assume without loss of generality that q is 0 or 1 (cf. Lemma 3.4). Next, we run the extended Euclidean algorithm on the integers a and c, and get

$$\gcd(a, c) = \gcd(t, t+2) = \gcd(2, t)$$

(cf. Lemma 3.1). The next division step in the algorithm depends on the parity of t, and rather than end up with the messy $\lfloor t/2\rfloor$, we divide into two cases.

The case *t* is odd: Let $t = 2s+1$, so that $a = 2s+1$, $b = 2s+2$, and $c = 2s+3$. Now

$$\gcd(a, c) = \gcd(2, 2s+1) = \gcd(1, 2) = 1,$$

and the extended Euclidean algorithm yields $1 = (s+1)a - sc$. Let $u \in \mathbb{Z}$, and we are wondering whether $u \notin S$, that is, $u \notin T$ and $u \notin b + T$. Suppose that

$$u = pa + qc$$

is the canonical form for u (see Definition 1.5). Lemma 1.6(2) tells us that $u \in T$ if and only if $q \geqslant 0$. Since we are looking for $u \notin T$, we may assume from here on out that $q < 0$. To characterize when $u \in b + T$ (that is, $u - b \in T$) we must find the canonical form for $u - b$.

First we compute the canonical form for b. Multiplying the equation $1 = (s+1)a - sc$ by $b = 2s+2$ yields *some* form for b:

$$b = (2s+2)(s+1)a - (2s+2)sc.$$

By Lemma 1.6(1), we may find the canonical form by dividing $(2s+2)(s+1)$ by $c = 2s+3$: the quotient is s with remainder $s+2$, giving the canonical form for b as

$$b = (s+2)a - sc.$$

Note that we got a little lucky here: our remainder of $s+2$ is clearly less than $c = 2s+3$; if our remainder had instead been $s+7$, say, then we would only have the canonical form for sufficiently large s.

Now we have that *some* form for $u-b$ is

$$u - b = (p-s-2)a + (q+s)c.$$

Is this the canonical form? There are two cases:

If $p \geqslant s+2$, then $0 \leqslant p-s-2 \leqslant p < c$, and this is in canonical form. Therefore, to have $u - b \in T$, we must have $q + s \geqslant 0$ (again using Lemma 1.6(2)), that is, $q \geqslant -s$.

If $p < s+2$, then the canonical form is

$$u - b = (p-s-2+c)a + (q+s-a)c = (p+s+1)a + (q-s-1)c$$

(to check that this is canonical, note that $p \geqslant 0$ and $s+2 < c$ imply $p-s-2+c \geqslant 0$, and $p < s+2$ implies $p-s-2+c < c$). In this case, to have $u-b \in T$, we must have $q \geqslant s+1$. This implies that $q \geqslant 0$, but we have assumed $q < 0$ (so that $u \notin T$). Therefore this case never has $u - b \in T$.

To summarize across both cases, if $u = pa + qc$, with $0 \leqslant p < c = 2s+3$ in the canonical form, then $u \notin S$ if and only if

$$\text{not}(q \geqslant 0) \quad \text{and} \quad \text{not}\big((p,q) \geqslant (s+2, -s)\big)$$

(cf. Lemma 3.5). The set of such (p,q) has a "stairstep" shape, as can be seen in Figure 1 for $t = 5$. In particular, the set of such (p,q) can be rewritten as $p \geqslant 0$ and

$$\big(p \leqslant s+1 \quad \text{and} \quad q \leqslant -1\big) \quad \text{or} \quad \big(p \leqslant 2s+2 \quad \text{and} \quad q \leqslant -s-1\big)$$

(cf. proof of Lemma 3.6, $d = 1$ case). The two "corners" in this picture, where both inequalities of one of these two conjunctions are tight, give our candidates for the largest $u \notin S$: it must be either

$$(s+1)a - 1c = 2s^2 + s - 2 \quad \text{or} \quad (2s+2)a + (-s-1)c = 2s^2 + s - 1.$$

The latter is always larger (in general, one might only be eventually larger than the other), and so we have

$$F(t, t+1, t+2) = 2s^2 + s - 1 = \frac{t^2}{2} - \frac{t}{2} - 1,$$

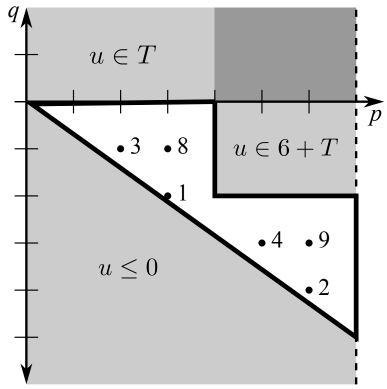

Figure 1: The $t = 5$ case of the example. We have $T = \langle 5, 7\rangle$ and $S = \langle 5, 6, 7\rangle = T \cup (6+T)$. Points $(p, q) \in \mathbb{Z}^2$ with $0 \leqslant p < 7$ are the canonical forms for $u = 5p + 7q \in \mathbb{Z}$. Then $q \geqslant 0$ corresponds to $u \in T$, $(p, q) \geqslant (4, -2)$ corresponds to $u \in 6 + T$, and positive u such that $u \notin S$ are labelled beside their corresponding (p, q). The "corners" $u = 8$ and $u = 9$ are candidates for the Frobenius number, and so $F(5, 6, 7) = \max\{8, 9\} = 9$.

in this case where $t = 2s + 1$ is odd.

The case t is even: Let $t = 2s$, so that $a = 2s$, $b = 2s + 1$, and $c = 2s + 2$. To have $u \notin S$ we must have both $u \notin T = \langle a, c\rangle$ and $u \notin b + T$. Note that every element in T is even and every element of $b + T$ is odd. Therefore the largest even integer not in S is the largest even integer not in T, which since T has only 2 generators is simply $\mathrm{lcm}(a, c) - a - c = 2s^2 - 2s - 2$ (we're getting lucky here that we didn't have to do an analysis similar to the t is odd case). Similarly the largest odd integer not in S is the largest odd integer not in $b+T$, which is $b+(2s^2-2s-2) = 2s^2-1$. The largest integer not in S is then the maximum of these two candidates, so $F(t, t+1, t+2) = 2s^2 - 1 = \frac{t^2}{2} - 1$ (cf. proof of Lemma 3.6, $d > 1$ case), in this case where t is even.

Combining the even and odd case, we have proved that

$$F(t, t+1, t+2) = \begin{cases} \frac{t^2}{2} & \text{if } t \text{ even,} \\ \frac{t^2}{2} - \frac{t}{2} - 1 & \text{if } t \text{ odd.} \end{cases}$$

3 Proof of Theorem 1.2

This first lemma gives us the basic tools we need:

Lemma 3.1. *Given $f, g \in \mathrm{EQP}$,*

1. *There exists an $m \in \mathbb{Z}_+$ such that, for each $0 \leqslant j < m$, $f(ms+j)$ eventually agrees with a polynomial in $\mathbb{Z}[s]$.*

2. *If* $\deg(g) > 0$*, there exists* $q, r \in \mathrm{EQP}$ *such that* $f(t) = q(t)g(t) + r(t)$ *and* $\deg(r) < \deg(g)$*. Note that this is the analogue of the traditional division algorithm over* $\mathbb{Q}[t]$*.*

3. *If* $g(t)$ *is eventually positive, there exists* $q, r \in \mathrm{EQP}$ *such that* $f(t) = q(t)g(t) + r(t)$ *and eventually* $0 \leqslant r(t) < g(t)$*. Furthermore,* $\deg(r) \leqslant \deg(g)$*. Note that this is the analogue of the traditional division algorithm over* $\mathbb{Z}$*.*

4. *There exists* $p, q, d \in \mathrm{EQP}$ *such that* $\gcd\big(f(t), g(t)\big) = d(t)$ *and* $d(t) = p(t)f(t) + q(t)g(t)$*.*

5. *We have* $\max\big(f(t), g(t)\big) \in \mathrm{EQP}$*.*

These are proved in Section 4 of [2] (and also in [1]), so in Section 4 we merely give an outline of the important steps.

Remark 3.2. Lemma 3.1(1) will allow us to often simply say "without loss of generality, $f \in \mathbb{Z}[t]$": we may analyze $f(ms + j)$ for each j, recognize that statements may be false for small s, and then convert back to t using $s = (t - j)/m$.

Using this remark, we may assume that the $a_i(t)$ are polynomials in $\mathbb{Z}[t]$. Since they are of degree at most 1 and eventually positive, we have that

$$a_i(t) = \alpha_i t + \beta_i,$$

with either $\alpha_i \in \mathbb{Z}_+$, $\beta_i \in \mathbb{Z}$ or $\alpha_i = 0$, $\beta_i \in \mathbb{Z}_+$. Furthermore, without loss of generality, we may assume that they are *ordered* so that

$$\beta_i \alpha_j \leqslant \beta_j \alpha_i$$

for $i \leqslant j$, that is (for $\alpha_i \neq 0$),

$$\frac{\beta_1}{\alpha_1} \leqslant \frac{\beta_2}{\alpha_2} \leqslant \cdots \leqslant \frac{\beta_n}{\alpha_n}.$$

We first consider a degenerate case, where $\beta_i \alpha_j = \beta_j \alpha_i$, for all i, j.

Lemma 3.3. *If* $\beta_i \alpha_j = \beta_j \alpha_i$*, for all* i, j*, then there are* $\alpha_0, \beta_0 \in \mathbb{Z}_{\geqslant 0}$ *such that, for all* i*,* $\alpha_i = \gamma_i \alpha_0$ *and* $\beta_i = \gamma_i \beta_0$ *(for some* $\gamma_i \in \mathbb{Z}_+$*). Therefore*

$$F\big(a_1(t), \ldots, a_n(t)\big) = F(\gamma_1, \ldots, \gamma_n) \cdot (\alpha_0 t + \beta_0)$$

is a polynomial of degree at most 1.

Therefore, we can assume that $\beta_1 \alpha_n < \beta_n \alpha_1$. In particular, the polynomials a_1 and a_n do not share a linear factor, and so if $d(t) = \gcd\big(a_1(t), a_n(t)\big)$, then $d(t) \in \mathrm{EQP}$ is of degree 0, that is, $d(t)$ is eventually a periodic function. Let $S(t) = \langle a_1(t), \ldots, a_n(t) \rangle$, and let $T(t) = \langle a_1(t), a_n(t) \rangle$. $T(t)$ is a semigroup with only two generators, so it is much easier to analyze. The following lemma allows us to cover $S(t)$ with a finite number of translated copies of $T(t)$.

Lemma 3.4. *For $a_i(t) = \alpha_i t + \beta_i$ as described above, there exists a finite set H of integer-valued polynomials of degree at most 1 such that*

$$\langle a_1(t), \ldots, a_n(t)\rangle = \bigcup_{h \in H} \Big(h(t) + \langle a_1(t), a_n(t)\rangle \Big)$$

(for t sufficiently large so that $a_i(t) > 0, \forall i$). Furthermore, $0 \in H$ and the other $h \in H$ are eventually positive.

Assume for the moment that $a_1(t)$ and $a_n(t)$ are relatively prime. By Lemma 1.6(2), the set of all integers not in T will be in bijection to the set

$$\left\{ (p, q) \in \mathbb{Z}^2 \,\middle|\, 0 \leqslant p < a_n(t),\, q < 0 \right\},$$

under the bijection $(p, q) \mapsto pa_1(t) + qa_n(t)$. By Lemma 3.4, integers not in S must also not be in $h(t) + T$, for all $h \in H$. The following lemma gives an easy way to check this.

Lemma 3.5. *Let $f, g, h \in \mathrm{EQP}$, with $f(t)$ and $g(t)$ relatively prime for all t and with $f(t), g(t), h(t)$ eventually positive. There exists $r, s \in \mathrm{EQP}$ such that, given $p, q \in \mathbb{Z}$ with $0 \leqslant p < g(t)$ and $q < 0$,*

$$pf(t) + qg(t) \in h(t) + \langle f(t), g(t)\rangle \quad \textit{if and only if} \quad (p, q) \geqslant \big(r(t), s(t)\big)$$

component-wise. Furthermore, $\deg(r) \leqslant \deg(g)$ and $\deg(s) \leqslant \max\{\deg(f), \deg(h) - \deg(g)\}$,

In our case, this gives r, s of degree at most 1. If $a_1(t)$ and $a_n(t)$ are relatively prime, all that remains is to follow the implications of Lemmas 3.4 and Lemma 3.5, which will give us a staircase-shaped set such as in Figure 1. If $a_1(t)$ and $a_n(t)$ are not relatively prime, we must reduce to the case where they are. Both of these are accomplished in the following lemma, which (combined with Lemma 3.4 and the fact that $d(t) = \gcd\big(f(t), g(t)\big)$ is of degree 0) proves our theorem.

Lemma 3.6. *Let $f(t), g(t) \in \mathrm{EQP}$, and let $d(t) = \gcd\big(f(t), g(t)\big)$ be of degree 0, let $H \subseteq \mathrm{EQP}$ be a finite set, and let*

$$S(t) = \bigcup_{h \in H} \big(h(t) + \langle f(t), g(t)\rangle \big).$$

The function $F(t)$ giving the largest integer not in $S(t)$ is in EQP, with degree at most $\max\{\deg(f) + \deg(g), \deg(h)\}$.

In our case, this gives that F is of degree at most 2.

4 Proofs of Lemmas

Proof of Lemma 1.6. Part 1 is a standard result, using the extended Euclidean algorithm and the fact that if $c = p'a + q'b$ is one solution, then all solutions are given by $c = (p' - kb)a + (q' + ka)b$ for $k \in \mathbb{Z}$.

For part 2, we have $c = pa + qb$ with $0 \leqslant p < b$. The reverse implication is immediate: if $q \geqslant 0$, then we have written $c = pa + qb$ with $p, q \in \mathbb{Z}_{\geqslant 0}$, proving that $c \in \langle a, b \rangle$. Conversely, suppose $c \in \langle a, b \rangle$ so that $c = p'a + q'b$ with $p', q' \in \mathbb{Z}_{\geqslant 0}$. By part 1, if k and r are the quotient and remainder when p' is divided by b, then

$$c = ra + (q' + ka)b$$

is the canonical form for c, with $q = q' + ka \geqslant 0$. □

Proof of Lemma 3.1. As these are proved in Section 4 of [2], we simply give an outline here.

For part 1, this is mostly obvious: simply take component polynomials of the quasi-polynomial. The main subtlety, as seen in the example from Section 2, is that integer-valued polynomials may have non-integral coefficients. In this case, let m be the least common multiple of the denominators of the coefficients. Examining $f(ms + i)$, we see that all coefficients of s^k must be integral, except possibly the constant coefficient; since the function is integer-valued, the constant coefficient must also be integral.

For part 2, simply perform polynomial division. The main subtlety is the following: Suppose, for example, that $f(t) = t^2 + 3t$ and $g(t) = 2t + 1$. Then the leading coefficient of g does not divide the leading coefficient of f, and the traditional polynomial division algorithm would produce quotients that are not integer-valued. Instead, we look separately at each residue class of t modulo the leading coefficient of g; for example, if t is odd, then $t = 2s + 1$ for some $s \in \mathbb{Z}_{\geqslant 0}$, so substituting gives $f(2s + 1) = 4s^2 + 10s + 3$ and $g(2s + 1) = 4s + 3$, and now the leading term does divide evenly.

For part 3, first perform the polynomial division algorithm for part 2. For example, suppose $f(t) = 2t - 3$ and $g(t) = t$, yielding $f = 2g + -3$. For part 3, however, we want the integer division algorithm: $f(t) = 1g(t) + (t - 3)$, and the remainder $t - 3$ is between 0 and g as long as $t \geqslant 3$. In other words, if we have found $f = q'g + r'$ with $\deg(r') < \deg(g)$, but we eventually have $r'(t) < 0$, then we should use quotient $q = q' - 1$ and remainder $r = g + r'$ instead, as eventually $0 \leqslant g(t) + r'(t) < g(t)$.

For part 4, run the extended Euclidean algorithm, repeatedly performing the division algorithm of part 2.

For part 5, note that given two polynomials, one eventually dominates the other. □

Proof of Lemma 3.3. For each i, let $\gamma_i = \gcd(\alpha_i, \beta_i) \in \mathbb{Z}_+$, let $\alpha'_i = \alpha_i/\gamma_i$, and let $\beta'_i = \beta_i/\gamma_i$, with α'_i and β'_i relatively prime. Dividing $\beta_i\alpha_j = \beta_i\alpha_i$ by $\gamma_i\gamma_j$ yields $\beta'_i\alpha'_j = \beta'_j\alpha'_i$. Since α'_j divides $\beta'_j\alpha'_i$ and is relatively prime to β'_j, we have that α'_j divides α'_i. Similarly, α'_i divides α'_j, and so $\alpha'_i = \alpha'_j$. Similarly, $\beta'_i = \beta'_j$. Taking α_0 to be the common α'_i (equal for all i) and β_0 to be the common β'_i, the proof follows. □

Proof of Lemma 3.4. Let $r = \beta_n\alpha_1 - \beta_1\alpha_n$. We are given that $r > 0$ and that $\beta_j\alpha_i - \beta_i\alpha_j \geqslant 0$ for all $i \leqslant j$. Let

$$H = \left\{\lambda_2 a_2 + \cdots + \lambda_{n-1}a_{n-1} \,\middle|\, \lambda_i \in \mathbb{Z}_{\geqslant 0},\ \lambda_i < r\right\}.$$

We will prove that H has the required properties; certainly every element of H is of degree at most 1. We must show that, if $u \in \langle a_1(t), \dots, a_n(t)\rangle$, then there exists a $\lambda \in \mathbb{Z}^n_{\geqslant 0}$ such that $u = \lambda_1 a_1(t) + \cdots + \lambda_n a_n(t)$ and $\lambda_i < r$ for $2 \leqslant i \leqslant n-1$.

By definition of the semigroup, there exists a $\lambda \in \mathbb{Z}^n_{\geqslant 0}$ such that $u = \lambda_1 a_1(t) + \cdots + \lambda_n a_n(t)$. Suppose that $\lambda_i \geqslant r$ for some i with $2 \leqslant i \leqslant n-1$. Let $p = \beta_n\alpha_i - \beta_i\alpha_n$ and $q = \beta_i\alpha_1 - \beta_1\alpha_i$ and observe that $p, q \geqslant 0$. Then

$$\begin{aligned} pa_1(t) + qa_n(t) &= (\beta_n\alpha_i - \beta_i\alpha_n)(\alpha_1 t + \beta_1) + (\beta_i\alpha_1 - \beta_1\alpha_i)(\alpha_n t + \beta_n) \\ &= \beta_n\alpha_i\alpha_1 t - \beta_i\alpha_n\beta_1 + \beta_i\alpha_1\beta_n - \beta_1\alpha_i\alpha_n t \\ &= (\beta_n\alpha_1 - \beta_1\alpha_n)(\alpha_i t + \beta_i) \\ &= ra_i(t). \end{aligned}$$

Now define λ' by $\lambda'_1 = \lambda_1 + p$, $\lambda'_i = \lambda_i - r$, $\lambda'_n = \lambda_n + q$, and $\lambda'_j = \lambda_j$ for all other j. Then

$$u = \lambda'_1 a_1(t) + \cdots + \lambda'_n a_n(t)$$

is a new representation of u. Repeating this process eventually yields a representation with $\lambda_i < r$ for $2 \leqslant i \leqslant n-1$. □

Proof of Lemma 3.5. Assume $0 \leqslant p < g(t)$ and $q < 0$. We need conditions on p, q for which $pf(t) + qg(t) - h(t) \in \langle f(t), g(t)\rangle$. By Lemma 3.1(4) and the fact that $f(t)$ and $g(t)$ are relatively prime, we may write $1 = r'(t)f(t) + s'(t)g(t)$, where $r', s' \in$ EQP. Multiplying this equation by $h(t)$ yields

$$h(t) = \big(h(t)r'(t)\big)f(t) + \big(h(t)s'(t)\big)g(t).$$

If we let $k(t)$ and $r(t)$ be the quotient and remainder when $h(t)r'(t)$ is divided by $g(t)$, using Lemma 3.1(3), and let $s(t) = h(t)s'(t) + k(t)f(t)$, then we have

$$h(t) = r(t)f(t) + s(t)g(t),$$

with $0 \leqslant r(t) < g(t)$. In particular, this gives us that $\deg(r) \leqslant \deg(g)$ and therefore $\deg(s) \leqslant \max\{\deg(f), \deg(h) - \deg(g)\}$. We have

$$pf(t) + qg(t) - h(t) = \big(p - r(t)\big)f(t) + \big(q - s(t)\big)g(t). \tag{1}$$

The case $\boldsymbol{p \geqslant r(t)}$: Then $0 \leqslant p - r(t) < g(t)$, and (1) is in canonical form. Then $pf(t) + qg(t) - h(t) \in \langle f(t), g(t)\rangle$ if and only if $q - s(t) \geqslant 0$, by Lemma 1.6(2).

The case $\boldsymbol{p < r(t)}$: Then the canonical form for $pf(t) + qg(t) - h(t)$ will be

$$\big(p - r(t) + g(t)\big)f(t) + \big(q - s(t) - f(t)\big)g(t), \tag{2}$$

since $0 \leqslant p < r(t)$ and $r(t) < g(t)$ imply that

$$0 < p - r(t) + g(t) < g(t).$$

Since $h(t)$, $r(t)$, $f(t)$, and $g(t)$ are eventually positive and $r(t) < g(t)$, we eventually have

$$0 < h(t) = r(t)f(t) + s(t)g(t) < g(t)\big(f(t) + s(t)\big),$$

and so eventually $f(t) + s(t) > 0$. Since we are assuming that $q < 0$, eventually $q - s(t) - f(t) < 0$. Therefore the canonical form (2) shows that $pf(t) + qg(t) - h(t) \notin \langle f(t), g(t)\rangle$, by Lemma 1.6(2).

Combining the two cases, we see that $pf(t) + qg(t) \in h(t) + \langle f(t), g(t)\rangle$ exactly when $p \geqslant r(t)$ and $q \geqslant s(t)$, as desired. □

Proof of Lemma 3.6. Since $d(t) \in \mathrm{EQP}$ is of degree zero, it is eventually a periodic function. By Remark 3.2, we may focus on a component of $d(t)$ and assume that $d(t) = d$ is a constant.

The case $d = 1$: We assume, without loss of generality, that $0 \in H$ and the other functions in H are eventually positive: if not, let $h_0(t)$ be the eventually minimal polynomial in H, and find the largest integer $F'(t)$ not in

$$S'(t) = \bigcup_{h \in H} \bigg(\big(h(t) - h_0(t)\big) + \langle f(t), g(t)\rangle \bigg);$$

then $F(t) = F'(t) + h_0(t)$.

We wish to describe the set $U(t)$ of (p, q) corresponding to canonical forms $u = pf(t) + qg(t)$ such that $u \notin S$. Canonical implies that $0 \leqslant p < g(t)$, and $u \notin (0 + \langle f(t), g(t)\rangle)$ implies that $q < 0$, by Lemma 1.6(2). Each $h \in H \setminus \{0\}$ gives the condition "$p < r_h(t)$ or $q < s_h(t)$", by Lemma 3.5. Then the set $U(t)$ has a "stairstep" shape as in Figure 1. To be precise, order the $\big(r_h(t), s_h(t)\big)$ such that $r_1(t) \leqslant r_2(t) \leqslant \cdots \leqslant r_m(t)$ (eventually). Notice that if $r_i(t) \leqslant r_j(t)$, then we may assume without loss of generality that $s_i(t) > s_j(t)$ (eventually), or else the condition "$p < r_j(t)$ or $q < s_j(t)$" would be redundant. Further include $\big(r_0(t), s_0(t)\big) = (0, 0)$ (corresponding to $u \notin 0 + \langle f(t), g(t)\rangle$) and $\big(r_{m+1}(t), s_{m+1}(t)\big) = \big(g(t), -f(t)\big)$ (corresponding to (p, q) being canonical). Finally, for $0 \leqslant i \leqslant m$, let $\big(\alpha_i(t), \beta_i(t)\big) = \big(r_{i+1}(t) - 1, s_i(t) - 1\big)$. Then the set of $(p, q) \in U(t)$ is exactly the set such that $0 \leqslant p$ and

$$(p, q) \leqslant \big(\alpha_0(t), \beta_0(t)\big) \quad \text{or} \quad \cdots \quad \text{or} \quad (p, q) \leqslant \big(\alpha_m(t), \beta_m(t)\big).$$

Since if $(p, q) \leqslant \big(\alpha_i(t), \beta_i(t)\big)$, then $pf(t) + qg(t) \leqslant \alpha_i(t)f(t) + \beta_i(t)g(t)$, our candidates for the largest integer not in $S(t)$ are the $\alpha_i(t)f(t) + \beta_i(t)g(t)$, $0 \leqslant i \leqslant m$. Then our final answer is

$$\max_{0 \leqslant i \leqslant m} \alpha_i(t)f(t) + \beta_i(t)g(t),$$

which is in EQP, by Lemma 3.1(5). Furthermore, using that $\deg(\alpha_i) = \deg(r_i) \leqslant \deg(g)$ and $\deg(\beta_i) = \deg(s_i) \leqslant \max\{\deg(f), \deg(h) - \deg(g)\}$, by Lemma 3.5, we have that our final degree is at most $\max\{\deg(f) + \deg(g), \deg(h)\}$.

The case $d > 1$: Let $H_j(t) = \{h \in H \mid h(t) \equiv j \bmod d\}$. The remainder when a given $h(t)$ is divided by d is a periodic function, by Lemma 3.1(3); applying Remark 3.2 as necessary, we may assume that these remainders are constant, that is, that $H_j = H_j(t)$ does not depend on t. Let $S_j(t) = \{u \in S(t) \mid u \equiv j \bmod d\}$. Since d divides every element of $\langle f(t), g(t)\rangle$,

$$S_j(t) = \bigcup_{h \in H_j} \Big(h(t) + \langle f(t), g(t)\rangle \Big).$$

Let $F_j(t)$ be the largest integer not in

$$\frac{1}{d}(S_j(t) - j) = \bigcup_{h \in H_j} \left(\frac{h(t)-j}{d} + \left\langle \frac{f(t)}{d}, \frac{g(t)}{d} \right\rangle \right).$$

By the case $d = 1$ proved above, $F_j(t)$ is in EQP. Since $dF_j(t) + j$ is the maximum $u \in j + d\mathbb{Z}$ such that $u \notin S_j(t)$, we get that $F(t) = \max_j \left(dF_j(t) + j\right)$. Lemma 3.1(5) then implies that $F(t)$ is in EQP. □

5 Proof of Corollary 1.4

Without loss of generality, we may assume that $b_1 = 0$ (substituting $s = t - b_1$, if necessary). For a fixed $j \in \mathbb{Z}$, look at all $t \equiv j \bmod b_n$, and let s be such that $t = b_n s + j$. Let $a_i(s) = t + b_i = b_n s + j + b_i$. We must prove that $F\big(a_1(s), \dots, a_n(s)\big)$ is a *polynomial* in s. We follow the proof of Theorem 1.2 and of the lemmas, looking for places where periodicity might be introduced. Note that the $a_i(s)$ are correctly ordered (as defined before the statement of Lemma 3.3) so that Lemma 3.4 gives us

$$S = \bigcup_{h \in H} \big(h(s) + \langle a_1(s), a_n(s)\rangle \big).$$

Following the proof of Lemma 3.4, note that each $h \in H$ is a nonnegative integer combination of $a_2(s), \dots, a_{n-1}(s)$. In particular, each $h \in H$ has the form $kb_n s + \ell$ for some integers k and ℓ.

Focus on a specific $h = kb_n s + \ell$. Let

$$d(s) = \gcd\big(a_1(s), a_n(s)\big) = \gcd(b_n s + j, b_n s + j + b_n) = \gcd(b_n, b_n s + j) = \gcd(j, b_n),$$

which is a constant. Finding p and q with $pj + qb_n = d$ gives us

$$d = (ps - q + p)a_1(s) - (ps - q)a_n(s).$$

Assume for the moment that $d = 1$. We next examine the proof of Lemma 3.5. The first step is to take

$$\begin{aligned} h = h \cdot 1 &= h \cdot \big((ps - q + p)a_1(s) - (ps - q)a_n(s)\big) \\ &= \big((kb_n s + \ell)(ps - q + p)\big)a_1(s) - \big((kb_n s + \ell)(ps - q + p)\big)a_n(s), \end{aligned}$$

and write it in canonical form. This involves taking the remainder when dividing

$$(kb_ns+\ell)(ps-q+p) = kpb_ns^2 + (\ell p - kb_nq + kb_np)s + (-\ell q + \ell p)$$

by $a_n(s) = b_ns + j + b_n$. The first step of polynomial long division works over the integers, because the leading coefficient, b_n, of $a_n(s)$ divides into the leading coefficient, kpb_n, of the dividend. This leaves a remainder that is linear in s. One more step of long division (dividing a linear in s function by a linear in s function and taking the linear in s remainder) will then lead to the final answer, without introducing extra periodicity.

No other steps in the entire proof have a possibility of adding periodicity, so we are done, in the case $d = 1$.

If $d > 1$, following the proof of Lemma 3.6 in the $d > 1$ case, let $b'_n = b_n/d$, $j' = j/d$, and $\ell' = \lfloor \ell/d \rfloor$ be integers. Then the reduction to the $d = 1$ case gives that we must examine,

$$\left\lfloor \frac{h(s)}{d} \right\rfloor + \left\langle \frac{a_1(s)}{d}, \frac{a_n(s)}{d} \right\rangle = (kb'_ns + \ell') + \langle b'_ns + j', b'_ns + j' + b'_n \rangle ,$$

and we have reduced to the $d = 1$ case.

6 Proof of Theorem 1.3

The $n = 1$ case is trivial: $F\big(a_1(t)\big) = -a_1(t)$ is the usual interpretation.

The $n = 2$ case follows from Sylvester's formula:

$$F\big(a_1(t), a_2(t)\big) = \operatorname{lcm}\big(a_1(t), a_2(t)\big) - a_1(t) - a_2(t) = \frac{a_1(t)a_2(t)}{\gcd\big(a_1(t), a_2(t)\big)} - a_1(t) - a_2(t),$$

and the gcd can be computed using Lemma 3.1.

For the $n = 3$ case, we show that the steps of Rødseth's algorithm [7] can be performed on eventual quasi-polynomials. We enumerate the steps of the algorithm as described for integers, and follow each step with a comment on how it works with elements of EQP.

(1) If $d(t) = \gcd\big(a_1(t), a_2(t), a_3(t)\big) \neq 1$, then use that

$$F\big(a_1(t), a_2(t), a_3(t)\big) = d(t)F\left(\frac{a_1(t)}{d(t)}, \frac{a_2(t)}{d(t)}, \frac{a_3(t)}{d(t)}\right).$$

For elements of EQP, Lemma 3.1(4) allows us to compute this gcd.

(2) We may assume that $a_1(t), a_2(t), a_3(t)$ are relatively prime where $a_1(t), a_2(t), a_3(t) \in$ EQP. If $e(t) = \gcd\big(a_1(t), a_2(t)\big) \neq 1$, then use that

$$F\big(a_1(t), a_2(t), a_3(t)\big) = e(t)F\left(\frac{a_1(t)}{e(t)}, \frac{a_2(t)}{e(t)}, a_3(t)\right) + a_3(t)\big(e(t) - 1\big).$$

This can again be done using Lemma 3.1(4).

(3) We may assume that $a_1(t)$ and $a_2(t)$ are relatively prime. Compute $s_0(t) \in \mathrm{EQP}$ such that $a_2(t)s_0(t) \equiv a_3(t) \bmod a_1(t)$ and $0 \leqslant s_0(t) < a_1(t)$.

To do this for elements of EQP, first use Lemma 3.1(4) to find $p, q \in \mathrm{EQP}$ such that $1 = p(t)a_1(t) + q(t)a_2(t)$. Then

$$a_2(t)\big(a_3(t)q(t)\big) = a_3(t)\big(q(t)a_2(t)\big) \equiv a_3(t) \cdot 1 \bmod a_1(t).$$

Now let $s_0(t)$ be the remainder when $a_3(t)q(t)$ is divided by $a_1(t)$, using Lemma 3.1(3). This is the desired $s_0(t)$.

(4) If $s_0(t) = 0$, then $a_3(t)$ is a multiple of $a_1(t)$, and the Frobenius problem reduces to the $n = 2$ case.

If some of the components of $s_0(t) \in \mathrm{EQP}$ are zero, we will have to split into cases, one for each component.

(5) Compute $q_1, s_1 \in \mathrm{EQP}$ such that

$$a_1(t) = q_1(t)s_0(t) - s_1(t), \quad 0 \leqslant s_1(t) < s_0(t).$$

If $\deg(s_0) = 0$, this is a slight variant of the usual integer division algorithm. If $\deg(s_0) > 0$, use Lemma 3.1(2) to compute $a_1(t) = q(t)s_0(t) + r(t)$, with $\deg(r) < \deg(s_0)$. If $r(t)$ is eventually negative or zero, simply set $q_1(t) = q(t)$ and $s_1(t) = -r(t)$, and we have that eventually $0 \leqslant s_1(t) < s_0(t)$. If $r(t)$ is eventually positive, set $q_1(t) = q(t) + 1$ and $s_1(t) = s_0(t) - r(t)$, which will eventually satisfy the bounds.

(6) Continue computing

$$\begin{aligned}
s_0(t) &= q_2(t)s_1(t) - s_2(t), \quad 0 \leqslant s_2(t) < s_1(t),\\
s_1(t) &= q_3(t)s_2(t) - s_3(t), \quad 0 \leqslant s_3(t) < s_2(t),\\
&\vdots\\
s_{m-2}(t) &= q_m(t)s_{m-1}(t) - s_m(t), \quad 0 \leqslant s_m(t) < s_{m-1}(t),\\
s_{m-1}(t) &= q_{m+1}(t)s_m(t) + s_{m+1}, \quad s_{m+1} = 0.
\end{aligned}$$

This is simply repeating the process from Step 5. We must establish that it terminates. It suffices to show that, if $\deg(s_i) > 0$, then $\deg(s_{i+2}) < \deg(s_i)$ (and then once $\deg(s_i) = 0$, the integers s_i strictly decrease, so this will eventually terminate). Indeed, as described in Step 5, Lemma 3.1(2) gives us $s_{i-1}(t) = q(t)s_i(t) + r(t)$, with $\deg(r) < \deg(s_i)$. If $r(t)$ is eventually negative or zero, we have $s_{i+1}(t) = -r(t)$, and the degree has decreased. If $r(t)$ is eventually positive, we have $s_{i+1}(t) = s_i(t) - r(t)$, which still have the same degree as s_i. But in the next step, $s_{i+1}(t) = 1 \cdot s_i(t) - r(t)$, and so $s_{i+2}(t) = r(t)$ has lower degree. Of course, different components of the eventual quasi-polynomials may terminate at different m, and we must analyze each separately.

(7) Define $s_{-1}(t) = a_1(t)$, $P_{-1}(t) = 0$, $P_0(t) = 1$, and recursively $P_{i+1}(t) = q_{i+1}(t)P_i(t) - P_{i-1}(t)$. Then

$$0 = \frac{s_{m+1}(t)}{P_{m+1}(t)} < \frac{s_m(t)}{P_m(t)} < \cdots < \frac{s_0(t)}{P_0(t)} < \frac{s_{-1}(t)}{P_{-1}(t)} = \infty.$$

Determine the unique index i such that

$$\frac{s_{i+1}(t)}{P_{i+1}(t)} \leqslant \frac{a_3(t)}{a_2(t)} < \frac{s_i(t)}{P_i(t)}.$$

Restricting to a fixed residue class modulo the period of the quasi-polynomials, such an index i exists, since each $s_i(t)/P_i(t)$ is a rational function, so is eventually greater than, eventually less than, or eventually equal to $a_3(t)/a_2(t)$.

(8) Then

$$\begin{aligned} F\big(a_1(t), a_2(t), a_3(t)\big) = -a_1(t) + a_2(t)\,(s_i(t) - 1) + a_3(t)\big(P_{i+1}(t) - 1\big) \\ - \min\big\{a_2(t)s_{i+1}(t), a_3(t)P_i(t)\big\}. \end{aligned}$$

This is in EQP, by Lemma 3.1(5).

References

[1] Danny Calegari and Alden Walker. Integer hulls of linear polyhedra and scl in families. *Transactions of the American Mathematical Society*, 365:5085–5102, 2011.

[2] Sheng Chen, Nan Li, and Steven V. Sam. Generalized Ehrhart polynomials. *Trans. Amer. Math. Soc.*, 364(1):551–569, 2012.

[3] Eugène Ehrhart. Sur les polyèdres rationnels homothétiques à n dimensions. *C. R. Acad. Sci. Paris*, 254:616–618, 1962.

[4] David Einstein, Daniel Lichtblau, Adam Strzebonski, and Stan Wagon. Frobenius numbers by lattice point enumeration. *Integers*, 7:A15, 63, 2007.

[5] J. L. Ramírez Alfonsín. *The Diophantine Frobenius problem*, volume 30 of *Oxford Lecture Series in Mathematics and its Applications*. Oxford University Press, Oxford, 2005.

[6] J. B. Roberts. Note on linear forms. *Proc. Amer. Math. Soc.*, 7:465–469, 1956.

[7] Øystein J. Rødseth. On a linear Diophantine problem of Frobenius. *J. Reine Angew. Math.*, 301:171–178, 1978.

[8] James J. Sylvester. Mathematical questions with their solutions. *Educational Times*, 41(21), 1884.

[9] Stan Wagon, personal comunication.

[10] Kevin Woods. The unreasonable ubiquitousness of quasi-polynomials. *Electron. J. Combin.*, 21(1):#P1.44, 2014.

[11] Kevin Woods. Presburger arithmetic, rational generating functions, and quasi-polynomials. *Journal of Symbolic Logic*, 80:433–449, 2015. Extended abstract in *ICALP 2013*.