9-22-2017

On a Frobenius Problem for Polynomials

Ricardo Conceição
Gettysburg College

R. Gondim

M. Rodriguez

Conceição, R.; Gondim, R.; Rodriguez, M. On a Frobenius problem for polynomials. Rocky Mountain Journal of Mathematics 47 (2017), no. 5, 1427-1462.

On a Frobenius Problem for Polynomials

Abstract
We extend the famous diophantine Frobenius problem to a ring of polynomials over a field~k. Similar to the classical problem we show that the $n = 2$ case of the Frobenius problem for polynomials is easy to solve. In addition, we translate a few results from the Frobenius problem over $\mathbb{Z}$ to $k[t]$ and give an algorithm to solve the Frobenius problem for polynomials over a field k of sufficiently large size.

Keywords
Frobenius problem, polynomials, arithmetic of function fields

Disciplines
Algebra | Mathematics | Number Theory

ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 47, Number 5, 2017

ON A FROBENIUS PROBLEM FOR POLYNOMIALS

R. CONCEIÇÃO, R. GONDIM AND M. RODRIGUEZ

ABSTRACT. We extend the famous diophantine Frobenius problem to a ring of polynomials over a field k. Similar to the classical problem we show that the $n = 2$ case of the Frobenius problem for polynomials is easy to solve. In addition, we translate a few results from the Frobenius problem over $\mathbb{Z}$ to $k[t]$ and give an algorithm to solve the Frobenius problem for polynomials over a field k of sufficiently large size.

1. Introduction. The Frobenius problem (FP) is a problem in basic number theory related to nonnegative integer solutions $(x_1, \ldots, x_n)$ of

$$x_1a_1 + \cdots + x_na_n = f,$$

where the a_is and f are positive integers and $\gcd(a_1, \ldots, a_n) = 1$. In particular, the Frobenius number $g = g(a_1, \ldots, a_n)$ is the largest f so that this equation fails to have a solution and the Frobenius problem is to compute g. This classical problem has a long history and has found many applications in mathematics as seen in [**1**], which contains the state-of-the-art on FP as well as almost 500 references on the subject and its applications.

As early as the mid 19th century mathematicians began to notice a strong relationship between the ring of integers $\mathbb{Z}$ and the ring of polynomials $k[t]$ over a field k, especially when k is finite. The discovery of this connection has proved very fruitful to number theory, and it has grown into an area of active research known as the arithmetic of function fields, see for instance, [**2, 3**]. In the arithmetic of function fields many of the classical results and conjectures in number theory, such as the prime number theorem, Falting's theorem or the Riemann hypothesis, have found an analogous statement over $k[t]$. Surprisingly,

2010 AMS *Mathematics subject classification.* Primary 11D07, Secondary 11C20, 13F20.

Keywords and phrases. Frobenius problem, polynomials, arithmetic of function fields.

Received by the editors on March 3, 2015, and in revised form on January 6, 2016.

DOI:10.1216/RMJ-2017-47-5-1

FP is one of the few classical and folkloric results in number theory for which an analogous statement over function fields cannot be found in the literature. The main goal of this note is to propose an analogous FP over $k[t]$.

Note that every non-zero element of $\mathbb{Z}$ can be written as a product αn of a unit α and a positive integer n. Similarly, every non-zero polynomial in $k[t]$ has a unique representation as a product αf, where $\alpha \in k^*$ is a unit and f is a monic polynomial. Consequently, the set of monic polynomials is a natural choice to be an analogue for the set of "positive" elements of $k[t]$.

Definition 1.1. We denote by $k[t]_{\geq 0}$ the set of all monic polynomials over a field k together with the zero element.

Given monic polynomials $A_1, \ldots, A_n, F$, our formulation of FP over $k[t]$ is related to solutions of

$$x_1 A_1 + \cdots + x_n A_n = F, \tag{1.1}$$

with $x_i \in k[t]_{\geq 0}$. It is based on the following theorem, whose proof we delay until the next section.

Theorem 1.2. *Let $n \geq 2$ be an integer, and let $A_1, \ldots, A_n$ be coprime monic polynomials in $k[t]$. Then, there exists an integer $g = g(A_1, \ldots, A_n)$ such that, for all monic polynomials F with $\deg F > g$, (1.1) has a solution with $x_1, \ldots, x_n \in k[t]_{\geq 0}$.*

This shows that the degree of a polynomial F for which (1.1) has no solutions in $k[t]_{\geq 0}$ has an upper bound. Our formulation is concerned with how large the upper bound of the Frobenius problem is for polynomials.

Definition 1.3. If (1.1) has a solution in $k[t]_{\geq 0}$ for all monic polynomials F, then we define $g(A_1, A_2, \ldots, A_n) = -\infty$. Otherwise, we define $g(A_1, \ldots, A_n)$ as the largest degree of a monic polynomial F for which equation (1.1) has no solutions in $k[t]_{\geq 0}$. We call $g(A_1, \ldots, A_n)$ the *Frobenius degree* of $A_1, \ldots, A_n$.

We consider the following statement over $k[t]$ as an analogue to the classical Frobenius problem.

The Frobenius problem for polynomials in dimension n-FPP. Given coprime monic polynomials $A_1, \ldots, A_n$, compute $g(A_1, \ldots, A_n)$.

Remark 1.4. It is worth noting that, technically, $g = g(A_1, \ldots, A_n)$ also depends on the field k over which the A_is are defined. There are two reasons why we have dropped dependence on the base field from the notation of g. First, we are mainly concerned with computing g over a fixed field k. Second, although there are instances where g changes if we replace k by one of its field extensions K, it turns out that g is not affected by field extensions as long as $|k|$ is sufficiently large. See subsection 3.2 and Corollary 6.10 for a proof of a more precise version of this statement.

Since a set of polynomials of bounded degree does not contain a "largest" polynomial, one would not expect the existence of a unique polynomial F with $\deg F = g(A_1, \ldots, A_n)$ for which (1.1) has no solution in $k[t]_{\geq 0}$. This observation inspires the next definition.

Definition 1.5. If $g = g(A_1, \ldots, A_n) > -\infty$, then a monic polynomial F with $\deg F = g$ for which equation (1.1) has no solutions in $k[t]_{\geq 0}$ is said to be a *critical example* to FPP for $A_1, \ldots, A_n$.

An alternative version of FPP could deal not only with the computation of $g(A_1, \ldots, A_n)$ but also with the construction of a critical example to FPP. In Section 6, we provide an algorithm that in most cases solves both versions of FPP. It is worth pointing out that the results in Section 6 suggest that the construction of a critical example to FPP is more challenging than simply finding $g(A_1, \ldots, A_n)$.

The rest of this article is dedicated to further comparison between the classical FP and FPP, and it covers some natural questions about FPP. It is organized as follows:

• Two proofs of Theorem 1.2 are given in the next section.

• In Section 3, we give some remarks on FPP and how it differs from the classical problem. For instance, given a field k of positive characteristic p, in Theorem 3.3 we show that, if $n > p$, then $g(A_1, \ldots, A_n) = -\infty$

for all $A_1, \ldots, A_n \in k[t]_{\geq 0}$ with positive degree. Thus, FPP is trivial if the dimension is large in comparison with the characteristic of the base field.

• Section 4 is devoted to presenting two examples for which the Frobenius degree can be explicitly computed. One of our results is as follows: suppose that $\gcd(A_1, \ldots, A_{n-1}) = D$ and $D \neq A_i$ for all $1 \leq i \leq n-1$. Under mild assumptions on the characteristic of the base field, in Theorem 4.4, we prove that, if $\deg A_n > g(A_1/D, \ldots, A_{n-1}/D)$, then

$$g(A_1, \ldots, A_n) = \max\{\deg A_n, g(A_1/D, \ldots, A_{n-1}/D)\} + \deg D,$$

or

$$g(A_1, \ldots, A_n) = g(A_1, \ldots, A_{n-1}),$$

if $D \neq 1$ or $D = 1$, respectively.

We use these examples to prove the sharpness of the upper and lower bounds for $g(A_1, \ldots, A_n)$ given by Remark 2.3 and Corollary 6.8, respectively. We also show that, in odd or zero characteristic, $g(A, B) = \deg A + \deg B$ and that, similar to Sylvester's classical result, $AB - A - B$ is a critical example in dimension 2, see Corollary 4.2.

• Section 5 gives a version for polynomials of the classical denumerant function. We also compute an asymptotic formula that resembles Schur's classical asymptotic formula for the number of non-negative integral solutions of $a_1x_1 + \cdots a_nx_n = f$, as $f \to \infty$.

• In Section 6, we give an algorithm for solving FPP for $n \geq 3$ that is dependent upon the size of the base field k. We also prove that $g(A_1, \ldots, A_n)$ is not affected by base field extensions K/k, if $|k|$ is sufficiently large.

• In Section 7, we provide a few ideas for future research on FPP.

2. Proof of Theorem 1.2. We give two proofs of Theorem 1.2; both provide upper bounds for the Frobenius degree $g(A_1, \ldots, A_n)$. The bound given by the first proof below is never sharp for $n > 2$; nonetheless, it is included here because part of its argument is used later in Theorem 5.4. It also provides the base case for induction for our second proof of Theorem 1.2, which in turn yields a sharp upper bound for $g(A_1, \ldots, A_n)$.

Lemma 2.1. *Let $n \geq 2$ be an integer, and let $A_1, \ldots, A_n$ be coprime monic polynomials in $k[t]$. If F is monic with*

$$\deg F > \sum_{i=1}^{n} \deg A_i,$$

then there exist $x_1, \ldots, x_n \in k[t]_{\geq 0}$ such that $x_1A_1 + \cdots + x_nA_n = F$.

Proof. The coprimality condition on the A_is implies that the linear equation $\widehat{x}_1A_1 + \cdots + \widehat{x}_nA_n = F$ has a solution $(\widehat{x}_1, \ldots, \widehat{x}_n) \in (k[t])^n$. Let

$$P = \prod_{i=1}^{n} A_i \quad \text{and} \quad \widetilde{A}_i = \frac{P}{A_i}.$$

Using the Euclidean algorithm to write $\widehat{x}_i = \overline{x}_i\widetilde{A}_i + r_i$, with $\deg r_i < \deg \widetilde{A}_i$, we rewrite F as

$$F = \left(\widehat{x}_1 + \sum_{i=2}^{n}(\overline{x}_i - 1)\widetilde{A}_1\right)A_1 + \sum_{i=2}^{n}(r_i + \widetilde{A}_i)A_i.$$

This shows that we can represent F as a linear combination

$$x_1A_1 + \cdots + x_nA_n = F$$

with $\deg x_i = \deg \widetilde{A}_i$, for $2 \leq i \leq n$. Note that, in such representation, for $2 \leq i \leq n$, we have $x_i = r_i + \widetilde{A}_i$ is monic and $\deg x_iA_i = \deg P$. Therefore, if we assume that

$$\deg F > \sum_{i=1}^{n} \deg A_i = \deg P,$$

we conclude that

$$x_1A_1 = F - \sum_{i=2}^{n} x_iA_i$$

is a monic polynomial. Consequently, x_1 is monic, and the result follows. □

Remark 2.2.

(1) Note that Lemma 2.1 proves that

$$g(A_1, \ldots, A_n) \leq \sum_{i=1}^{n} \deg A_i.$$

For $n > 2$ and $A_i \neq 1$, this upper bound is never sharp. Indeed, in the proof of Lemma 2.1, we can replace $\widetilde{A}_i$ by A_1 and adapt the argument accordingly to show that

$$g(A_1, \ldots, A_n) \leq \max_{2 \leq i \leq n} \{\deg A_1 + \deg A_i\}.$$

(2) The proof of Lemma 2.1 actually shows that, if

$$\deg F > \sum_{i=1}^{n} \deg A_i,$$

then, for any fixed $1 \leq j \leq n$, there exists a solution in $k[t]_{\geq 0}$ of (1.1) that satisfies

$$\deg x_j = \deg F - \deg A_j$$

and

$$\deg x_k = \sum_{i=1}^{n} \deg A_i - \deg A_k,$$

for $k \neq j$.

Proof of Theorem 1.2. The proof is by induction on n, with the base case for induction given by the $n = 2$ case of Lemma 2.1. If $\gcd(A_1, \ldots, A_{n-1}) = 1$, then the result easily follows by induction. Thus we assume that $D = \gcd(A_1, \ldots, A_{n-1})$ is a monic polynomial of positive degree. Write $\widetilde{A}_i = A_i/D$. Note that $\gcd(\widetilde{A}_1, \ldots, \widetilde{A}_{n-1}) = 1$ and $\gcd(A_n, D) = 1$. By the induction hypothesis, there exists an integer $\widetilde{g} = g(\widetilde{A}_1, \ldots, \widetilde{A}_{n-1})$ such that the equation

$$x_1\widetilde{A}_1 + \cdots + x_{n-1}\widetilde{A}_{n-1} = z$$

has a solution satisfying $x_1, \ldots, x_{n-1} \in k[t]_{\geq 0}$ whenever $\deg z > \widetilde{g}$. We will prove that (1.1) has a solution with $x_1, \ldots, x_n \in k[t]_{\geq 0}$, whenever

$$\deg F > \max\{\deg A_n, \widetilde{g}\} + \deg D. \tag{2.1}$$

First note that (2.1), together with the $n = 2$ case of Remark 2.2, imply that the equation

$$x_n A_n + zD = F,$$

has a solution with $x_n, z \in k[t]_{\geq 0}$ and $\deg z = \deg F - \deg D$. Thus, it follows from (2.1) that $\deg z > \widetilde{g}$. Therefore, by the induction hypothesis, the equation

$$x_1 \widetilde{A}_1 + \cdots + x_{n-1}\widetilde{A}_{n-1} = z = \frac{F - x_n A_n}{D}, \tag{2.2}$$

has a solution with $x_1, \ldots, x_{n-1} \in k[t]_{\geq 0}$, and the result follows after multiplying (2.2) by D. □

Remark 2.3. Note that implicit in the previous proof of Theorem 1.2 are the following upper bounds for the Frobenius degree of coprime monic polynomials $A_1, \ldots, A_n$ with $n > 2$. If $\gcd(A_1, \ldots, A_{n-1}) = 1$, then

$$g(A_1, \ldots, A_n) \leq g(A_1, \ldots, A_{n-1}).$$

If $D = \gcd(A_1, \ldots, A_{n-1})$ has positive degree, then

$$g(A_1, \ldots, A_n) \leq \max\left\{ \deg A_n, g\left(\frac{A_1}{D}, \ldots, \frac{A_{n-1}}{D}\right)\right\} + \deg D.$$

We show in Lemma 4.4 that this upper bound is sharp.

Remark 2.4. Clearly, the upper bound given in Remark 2.3 depends upon the ordering of the A_is and computation of the Frobenius degree of $n-1$ coprime polynomials. In order to avoid such dependence, we consider $S = \{B_1, \ldots, B_m\}$ to be a subset of $\{A_1, \ldots, A_n\}$ and inductively define the following function $U(S)$. We let $U(S) = \deg B_1 + \deg B_2$, if $m = 2$. Otherwise, $U(S) = U(B_1, \ldots, B_{m-1})$, if $\gcd(B_1, \ldots, B_{m-1}) = 1$; or $D_S = \gcd(B_1, \ldots, B_{m-1})$ has positive degree and

$$U(S) = \max\left\{ \deg B_m, U\left(\frac{B_1}{D_S}, \ldots, \frac{B_{m-1}}{D_S}\right)\right\} + \deg D_S.$$

Thus, Remark 2.3 and Lemma 2.1 imply that, for $n > 2$,

$$g(A_1, \ldots, A_n) \leq \min\{U(S) : S \subset \{1, \ldots, n\}, |S| = n - 1\}.$$

3. Remarks on FPP. Unlike $\mathbb{Z}$, the group of units in $k[t]$ can be quite large. Although this difference allows flexibility when choosing the "sign" of a polynomial, it does not prevent FPP from being a well-posed problem in the arithmetic of function fields. There exist other significant differences between $\mathbb{Z}$ and $k[t]$ that create some striking contrast between the classical FP and FPP. In this section, we present two results intrinsic to the function field setting that stem from these differences.

The first notable difference is the existence of base fields of positive characteristic p. As proved in Theorem 3.3 below, FPP in dimension n is trivial if $n \geq p$. As noted in the introduction, another striking difference between the classical and the polynomial Frobenius problem is the existence of base field extensions of the ring $k[t]$. We show in this section that, if we fix coprime monic polynomials $A_1, \ldots, A_n$ over $k[t]$, then, for some field extension K/k, $g(A_1, \ldots, A_n)$ may increase if we consider solutions of (1.1) over $K[t]_{\geq 0}$ instead.

3.1. Issues in positive characteristics. Over $\mathbb{Z}$, the sum $a_1 + \cdots + a_n$ of non-negative integers a_is is a non-negative integer of size at least as large as the size of each of its summands. This fact plays a crucial role in many of the arguments related to the classical FP. Unfortunately, the analogous fact is generally not true in the ring $k[t]$. It is easy to construct examples of monic polynomials $A_1, \ldots, A_n$, whose sum $S = A_1 + \cdots + A_n$ is not a monic polynomial. Moreover, even if S is monic, we do not have control over the "size" of S. We can easily construct examples of a monic S over a field of positive characteristic for which $\deg S < \max_{1 \leq i \leq n}\{\deg A_i\}$. The next lemma, whose proof is left to the reader, shows that, in such a case, n needs to be large.

Lemma 3.1. *Let $A_1, \ldots, A_n$ be monic polynomials over a field of characteristic p. If $\deg(A_1 + \cdots + A_n) < \max_{1 \leq i \leq n}\{\deg A_i\}$, then $p > 0$ and $n \geq p$.*

As a consequence, if $n < p$ or $p = 0$, then the solutions in $k[t]_{\geq 0}$ of (1.1) satisfy

$$\deg x_i \leq \deg F - \min_{1\leq i\leq n}\{\deg A_i\}. \tag{3.1}$$

The first direct consequence of this result is the following lower bound for the Frobenius degree.

Corollary 3.2. *Let $A_1, A_2, \ldots, A_n$ be coprime non-constant monic polynomials over a field k. Suppose* $\operatorname{char}(k) = 0$ *or* $n < \operatorname{char}(k)$. *Then,*

$$\min_{1\leq i\leq n}\{\deg A_i\} \leq g(A_1, \ldots, A_n).$$

Inequality (3.1) also shows that, whenever $p = 0$ or $n < p$, the polynomials x_is in a solution of (1.1) have bounded degree.

Next, we show that condition $n < p$ or $p = 0$ is not only sufficient but also necessary to guarantee the boundedness of the degree of the monic solutions of (1.1).

Theorem 3.3. *Let $A_1, A_2, \ldots, A_n$ be coprime monic polynomials in $k[t]$, with k a field of characteristic $p > 0$. For any monic polynomial F,* (1.1) *has solutions $x_i \in k[t]_{\geq 0}$ with arbitrarily large degree if and only if $n \geq p$.*

Proof. As discussed above, if $n < p$, then the degrees of the solutions $x_i \in k[t]_{\geq 0}$ of (1.1) are bounded above by (3.1). Thus, it remains to show that, if $n \geq p$, then (1.1) has solutions $x_i \in k[t]_{\geq 0}$ of unbounded degree. Write $n = ap + b$ with $a > 0$ and $0 \leq b < p$. Here, we only consider the case where $b \neq 0$ since the same proof works for $b = 0$ after some minor adjustments.

Let $R = \{1, 2, \ldots, pa\}$ and $S = \{n - p + 1, n - p + 2, \ldots, n\}$. Note that $R \cup S = \{1, 2, \ldots, n\}$, $|S|$ and $|R|$ are divisible by p and that $|R \cap S| = p - b + 1$. For $s \in S$ and $r \in R$, the monic polynomials

$$y_s = \frac{\prod_{l\in S} A_l}{A_s} \quad \text{and} \quad z_r = \frac{\prod_{l\in R} A_l}{A_r}$$

satisfy

$$\sum_{s\in S} y_s A_s = \sum_{r\in R} z_r A_r = 0. \tag{3.2}$$

Since $\gcd(A_1,\dots,A_n)=1$, we can find polynomials $G_1,\dots,G_n$ such that $F = A_1G_1+\cdots+A_nG_n$. Let l and m be positive integers satisfying

$$l > m + \max\{\deg z_r : r\in R\} > \max\{\deg G_i : 1\le i\le n\}.$$

Thus, the polynomials

$$x_i = \begin{cases} t^l y_i + G_i & \text{if } i\in R\backslash R\cap S \\ t^l y_i + t^m z_i + G_i & \text{if } i\in R\cap S \\ t^m z_i + G_i & \text{if } i\in S\backslash R\cap S \end{cases}$$

are monic and have unbounded degree. The result follows from (3.2) and the following computation

$$\begin{aligned}\sum_{i=1}^{n} x_iA_i &= \sum_{i\in R\backslash R\cap S}(t^l y_i + G_i)A_i + \sum_{i\in R\cap S}(t^l y_i + t^m z_i + G_i)A_i \\ &\quad + \sum_{i\in S\backslash R\cap S}(t^m z_i + G_i)A_i \\ &= t^l\sum_{i\in R} y_iA_i + t^m\sum_{i\in S} z_iA_i + \sum_{i=1}^{n} G_iA_i = F. \end{aligned}$$ □

Remark 3.4. The previous result shows that, over a field of positive characteristic p, $g(A_1,\dots,A_n) > -\infty$ if and only if $n < p$ or $1\notin\{A_1,\dots,A_n\}$. In contrast, in the classical case, we have $g(A_1,\dots,A_n) > -\infty$ if and only if $1\notin\{A_1,\dots,A_n\}$.

3.2. FPP over extensions of the base field. Another critical difference between the arithmetic of function fields and that of $\mathbb{Q}$ is the existence of constant field extensions. Concerning FPP, we first observe that, for a fixed set of coprime monic polynomials $A_1,\dots,A_n$ over k, our definition of the Frobenius degree is, a priori, dependent on the base field k. In order to study such dependence on the base field, given a field extension K/k, we write $g_K = g_K(A_1,\dots,A_n)$ for the largest degree of a monic polynomial F over K for which (1.1) has

no solutions in $K[t]_{\geq 0}$. Clearly, $g_k \leq g_K$. As shown below, there are examples of field extensions K/k where $g_k < g_K$.

Example 3.5. Let $A_i = t + i$. Remark 2.4 implies that $g(A_1, A_2, A_3) \leq 2$. In order to find all monic polynomials F of degree 2 for which (1.1) has a solution in $k[t]_{\geq 0}$, we only need to compute all possible linear combinations:

$$x(t+1) + y(t+2) + z(t+3), \tag{3.3}$$

with $(x, y, z) \in (k[t]_{\geq 0})^3$ and $\deg x = 1$ and $\deg y$, $\deg z < 1$; or $\deg y = 1$ and $\deg x$, $\deg z < 1$; or $\deg z = 1$ and $\deg x$, $\deg y < 1$.

If we take $k = \mathbb{F}_5$, then a computer search shows that all degree 2 monic polynomials appear as the linear combination described in (3.3). This shows that $g_k(A_1, A_2, A_3) < 2$. On the other hand, the same computation with $K = \mathbb{F}_{5^2}$ shows that not all degree 2 polynomials appear as a linear combination in (3.3); hence, $g_K(A_1, A_2, A_3) = 2$.

In the previous example, the existence of field extensions K/k for which $g_k < g_K$ is proven by looking at all possible monic linear combinations of $A_1, \ldots, A_n$. In Section 6, this basic argument is extended to prove that $g_k = g_K$, if $|k|$ is "sufficiently large." In particular, $g_K(A_1, \ldots, A_n)$ is independent of the field extension K/k, whenever k is infinite. The proof is given in Corollary 6.10, where a description is also given regarding how large $|k|$ needs to be in order to ensure that $g_K = g_k$.

4. Two interesting examples. In this section, we give two examples of families of coprime monic polynomials $A_1, \ldots, A_n$ for which we can compute $g(A_1, \ldots, A_n)$ explicitly. Such examples are used to prove that the upper and lower bounds given by Remark 2.3 and Corollary 6.8, respectively, are sharp. Additionally, we use the next result to settle the two-dimensional case of FPP.

Lemma 4.1. *For $n \geq 2$, let $A_1, \ldots, A_n$ be pairwise coprime and non-constant monic polynomials over a field k. Suppose that* $\operatorname{char}(k) = 0$ *or $n < \operatorname{char}(k)$. Define*

$$P = \prod_{i=1}^{n} A_i, \quad \widetilde{A}_i = \frac{P}{A_i} \quad \textit{and} \quad F = P - \sum_{i=1}^{n} \widetilde{A}_i.$$

Then, the equation

$$x_1\widetilde{A}_1 + \cdots + x_n\widetilde{A}_n = F,$$

has no solution with $x_i \in k[t]_{\geq 0}$. *Moreover,*

$$g(\widetilde{A}_1, \ldots, \widetilde{A}_n) = \deg F = \deg A_1 + \cdots + \deg A_n.$$

Proof. Suppose, for the sake of contradiction, that we can find $x_i \in k[t]_{\geq 0}$, satisfying

$$x_1\widetilde{A}_1 + \cdots + x_n\widetilde{A}_n = P - \sum_{i=1}^{n} \widetilde{A}_i.$$

This implies that

$$(x_1 + 1)\widetilde{A}_1 + \cdots + (x_n + 1)\widetilde{A}_n = \prod_{i=1}^{n} A_i, \tag{4.1}$$

and that $A_i \mid \widetilde{A}_i(x_i + 1)$. Since by hypothesis $\gcd(A_i, \widetilde{A}_i) = 1$, we have that

$$x_i + 1 = A_i B_i \tag{4.2}$$

for some polynomial B_i. Notice that B_i is non-zero and monic, since we are assuming that x_i is monic and A_i is non-constant. From (4.1) and (4.2), we arrive at

$$B_1 + \cdots + B_n = 1. \tag{4.3}$$

The hypothesis on $\mathrm{char}(k)$ and the fact that $B_1, \ldots, B_n$ are monic imply that (4.3) contradicts Lemma 3.1. Therefore, the initial assumption that $x_i \in k[t]_{\geq 0}$ does not hold, and the result follows.

In order to prove the "moreover" part, we first note that the argument above proves that $g(\widetilde{A}_1, \ldots, \widetilde{A}_n) \geq \deg F$. The proof is obtained by showing through induction on n that, if $A_1, \ldots, A_n$ are pairwise coprime monic polynomials, then $g(\widetilde{A}_1, \ldots, \widetilde{A}_n) \leq \deg A_1 + \cdots + \deg A_n$.

The base case $n = 2$ was proven in Lemma 2.1. Let

$$P_{n-1} = \prod_{i=1}^{n-1} A_i \quad \text{and} \quad \widetilde{A}_{i,n-1} = \frac{P_{n-1}}{A_i},$$

for $1 \leq i \leq n-1$. By the induction hypothesis,

$$g(\widetilde{A}_{1,n-1}, \ldots, \widetilde{A}_{n-1,n-1}) \leq \deg A_1 + \cdots + \deg A_{n-1}.$$

Note that $\widetilde{A}_{i,n-1} = \widetilde{A}_i/A_n$ and that $A_n = \gcd(\widetilde{A}_1, \ldots, \widetilde{A}_{n-1})$. This fact and the upper bound in Remark 2.3 imply that

$$\begin{aligned} g(\widetilde{A}_1, \ldots, \widetilde{A}_n) &\leq \max\left\{ \deg \widetilde{A}_n, g\left(\frac{\widetilde{A}_1}{A_n}, \ldots, \frac{\widetilde{A}_{n-1}}{A_n}\right)\right\} + \deg A_n \\ &\leq \max\left\{ \sum_{i=1}^{n-1} \deg A_i, g(\widetilde{A}_{1,n-1}, \ldots, \widetilde{A}_{n-1,n-1})\right\} + \deg A_n \\ &\leq \deg A_1 + \cdots + \deg A_n, \end{aligned}$$

as desired. □

Clearly, the two-dimensional case of FPP is $n = 2$ of the previous result. However, we restate it below for future reference.

Corollary 4.2. *Let A and B be coprime monic polynomials over a field k. Suppose that* $\operatorname{char}(k) = 0$ *or* $\operatorname{char}(k)$ *is odd. Then,*

$$g(A, B) = \deg A + \deg B,$$

and $G = AB - A - B$ is a critical example to FPP *for A, B.*

Remark 4.3. It is enlightening to compare this with the classical Frobenius problem. In the latter case, Sylvester's well-known result shows that $g(p, q) = pq - p - q$ for relatively prime positive integers p and q. As seen above, the natural translation of this formula over to $k[t]$ solves FPP in dimension 2.

The next result shows that, for all $n \geq 2$, the upper bound in terms of the degree of the input polynomials in Remark 2.3 cannot be improved.

Lemma 4.4. *Let $A_1, A_2, \ldots, A_n$ be coprime non-constant monic polynomials over a field k. Suppose that* $\operatorname{char}(k) = 0$ *or* $n < \operatorname{char}(k)$*. Also, suppose that* $\gcd(A_1, \ldots, A_{n-1}) = D$ *and* $D \neq A_i$ *for all* $1 \leq i \leq n-1$.

If $\deg A_n > g(A_1/D, \ldots, A_{n-1}/D)$*, then*

$$g(A_1, \ldots, A_n) = \max\left\{ \deg A_n, g\left(\frac{A_1}{D}, \ldots, \frac{A_{n-1}}{D}\right)\right\} + \deg D,$$

or

$$g(A_1, \ldots, A_n) = g(A_1, \ldots, A_{n-1}),$$

if $D \neq 1$ *or* $D = 1$*, respectively.*

Proof. We assume that $D \neq 1$, since the case $D = 1$ is simpler and may be proved in a similar way. Remark 2.3 provides us with the upper bound

$$g(A_1, \ldots, A_n) \leq \max\left\{ \deg A_n, g\left(\frac{A_1}{D}, \ldots, \frac{A_{n-1}}{D}\right)\right\} + \deg D.$$

We show that the previous equality holds by constructing a critical example to FPP for $A_1, \ldots, A_n$, with the appropriate degree.

Write $\widetilde{g} = g(A_1/D, \ldots, A_{n-1}/D)$. Let G with $\deg G = \widetilde{g}$ be a counterexample for the Frobenius problem for $A_1/D, \ldots, A_{n-1}/D$ (which exists since $A_i/D \neq 1$ for all i). We show that the equality

$$x_1A_1 + \cdots + x_nA_n = DG + (D-1)A_n \tag{4.4}$$

does not hold with $x_1, \ldots, x_n \in k[t]_{\geq 0}$. Assume the opposite. Since, by hypothesis, $\deg A_n > \widetilde{g}$, comparison of degrees in (4.4) yields $\deg x_n \leq \deg D$. This fact, together with $\gcd(D, A_n) = 1$ and

$$D\left(x_1\frac{A_1}{D} + \cdots + x_{n-1}\frac{A_{n-1}}{D} - G\right) = (D - 1 - x_n)A_n,$$

imply that $x_n = D - 1$. Consequently,

$$x_1\frac{A_1}{D} + \cdots + x_{n-1}\frac{A_{n-1}}{D} = G,$$

which contradicts the fact that G is a critical example of FPP for the polynomials $A_1/D, \ldots, A_{n-1}/D$. Since

$$\deg(DG + (D-1)A_n) = \max\left\{ \deg A_n, g\left(\frac{A_1}{D}, \ldots, \frac{A_{n-1}}{D}\right)\right\} + \deg D,$$

the result follows. □

5. The type-denumerant function. In this section, we provide an analogous statement to the following classical result of Schur closely related to FP.

Theorem 5.1. (Schur, [**1,** Theorem 4.2.1]). *Let $a_1, \dots, a_n$ be coprime positive integers, and let $P_n = \prod_{i=1}^{n} a_i$. Given a positive integer f, let $d(f; a_1, \dots, a_n)$ be the number of solutions of $x_1a_1 + \cdots + x_na_n = f$ with integers $x_i \geq 0$. Then,*

$$d(f; a_1, \dots, a_n) \sim \frac{f^{n-1}}{P_n(n-1)!} \quad \text{as } f \to \infty.$$

Before translating this result to FPP, we observe that, for a fixed monic polynomial F, the number of "non-negative" solutions of (1.1) may be infinite (see, for instance, Theorem 3.3). In order to circumvent this difficulty and find an analogue to Schur's result, we give the following definition.

Definition 5.2. Let $A_1, \dots, A_n$ be coprime monic polynomials. For a fixed monic polynomial F, we define the *type* of a solution $(x_1, \dots, x_n) \in (k[t]_{\geq 0})^n$ of (1.1) as the n-tuple $(\deg x_1, \dots, \deg x_n)$. The number of types associated to F is given by the *type-denumerant* function $\mathcal{T}(F; A_1, \dots, A_n)$.

Remark 5.3. Over a field k of characteristic p, (3.1) and Theorem 3.3 imply that $\mathcal{T}(F; A_1, \dots, A_n)$ is finite if and only if $n < p$ or $p = 0$.

Given the above definition, the analogous statement over $k[t]$ of Theorem 5.1 is as follows.

Theorem 5.4. *Let $A_1, A_2, \dots, A_n$ be coprime non-constant monic polynomials over a field k. Suppose that* $\operatorname{char}(k) = 0$ *or* $n < \operatorname{char}(k)$. *Then,*

$$\mathcal{T}(F; A_1, \dots, A_n) \sim n\left(\deg F - \sum_{i=1}^{n} \deg A_i\right)^{n-1} \quad \text{as } \deg F \to \infty.$$

Proof. Since we want to estimate $\mathcal{T}(F; A_1, \ldots, A_n)$ as $\deg F \to \infty$, we may assume that F is a monic polynomial with

$$\deg F > 1 + \sum_{i=1}^{n} \deg A_i.$$

First, note that the possible types associated to F are of the form $(e_1, \ldots, \deg F - \deg A_j, \ldots, e_n)$, for some $1 \leq j \leq n$, with $e_i = -\infty$ or $0 \leq e_i < \deg F - \deg A_i$. In order to prove our result, we use the polynomial

$$\widetilde{A}_i = \frac{\prod_{j=1}^{n} A_j}{A_i}$$

to partition the set of types associated to F in the following way. We let $S \subset \{1, \ldots, n\}$ be such that $S \cap \{j\} = \emptyset$ and define $\chi_j(S)$ to be the number of types of the form $(e_1, \ldots, \deg F - \deg A_j, \ldots, e_n)$ such that $e_i < \deg \widetilde{A}_i$, for $i \in S$, and $\deg \widetilde{A}_i \leq e_i < \deg F - \deg A_i$, for $i \notin S \cup \{j\}$. Thus,

$$\mathcal{T}(F; A_1, \ldots, A_n) = \sum_{j=1}^{n} \sum_{\substack{S \subset \{1,\ldots,n\} \\ S \cap \{j\} = \emptyset}} \chi_j(S),$$

and $\mathcal{T}(F; A_1, \ldots, A_n)$ is estimated by approximating $\chi_j(S)$. To this end, we first show that

$$\chi_j(\emptyset) = \left(\deg F - \sum_{i=1}^{n} \deg A_i \right)^{n-1}. \tag{5.1}$$

Note that $\chi_j(\emptyset)$ counts the number of types of the form $(e_1, \ldots, \deg F - \deg A_j, \ldots, e_n)$ for which $\deg \widetilde{A}_i \leq e_i < \deg F - \deg A_i$ for all $i \neq j$. Since

$$\deg F - \sum_{i=1}^{n} \deg A_i > 1,$$

Remark 2.2 shows that there is a solution $(\overline{x}_1, \ldots, \overline{x}_n)$ of the type

$$(\deg \widetilde{A}_1, \ldots, \deg F - \deg A_j, \ldots, \deg \widetilde{A}_n).$$

Moreover, any monic polynomial z_i with

$$1 \leq \deg z_i < \deg F - \sum_{i=1}^{n} \deg A_i$$

produces a solution

$$\left(\overline{x}_1 + z_1 \widetilde{A}_1, \ldots, \overline{x}_j - \sum_{\substack{i=1 \\ i \neq j}}^{n} z_i \widetilde{A}_j, \ldots, \overline{x}_n + z_n \widetilde{A}_n \right),$$

of the type $(\deg z_1 + \deg \widetilde{A}_1, \ldots, \deg F - \deg A_j, \ldots, \deg z_n + \deg \widetilde{A}_n)$. In this fashion, we can obtain all types of the form $(e_1, \ldots, \deg F - \deg A_j, \ldots, e_n)$ with

$$\deg \widetilde{A}_i \leq e_i < \deg F - \deg A_i,$$

which shows that (5.1) holds and

$$\mathcal{T}(F; A_1, \ldots, A_n) \geq n \Big(\deg F - \sum_{i=1}^{n} \deg A_i \Big)^{n-1}.$$

In order to obtain an upper bound for $\mathcal{T}(F; A_1, \ldots, A_n)$, we note that the argument used in the computation of $\chi_j(\emptyset)$ may also be used to show that

$$0 \leq \chi_j(S) \leq \prod_{i \in S} \deg \widetilde{A}_i \Big(\deg F - \sum_{i=1}^{n} \deg A_i \Big)^{n-1-|S|},$$

for a non-empty subset S. Consequently, for $C = \deg F - \sum_{i=1}^{n} \deg A_i$,

$$nC^{n-1} \leq \mathcal{T}(F; A_1, \ldots, A_n) \leq nC^{n-1} + n \sum_{\substack{S \subset \{1, \ldots, n\} \\ S \cap \{j\} = \emptyset}} C^{n-1-|S|} \prod_{i \in S} \deg \widetilde{A}_i,$$

and the result follows. □

Remark 5.5. We can say a bit more about $\mathcal{T}(F; A_1, A_2)$, when $\deg F > \deg A_1 + \deg A_2$. Using the notation in the proof of Theorem 5.4, we have

$$\begin{aligned}\mathcal{T}(F;A_1,A_2) &= \sum_{j=1}^{2} \sum_{\substack{S\subset\{1,2\}\\ S\cap\{j\}=\emptyset}} \chi_j(S)\\ &= 2(\deg F - \deg A_1 - \deg A_2) + \chi_1(\{2\}) + \chi_2(\{1\}).\end{aligned}$$

Note that $\chi_1(\{2\})$ counts the number of types $(\deg F - \deg A_1, e_2)$ with $e_2 < \deg A_1$. It is easy to show that, if the equation $xA_1 + yA_2 = F$ has a solution with $\deg y < \deg A_1$, then this solution is unique. Therefore, $\chi_1(\{2\}) \leq 1$. Similarly, $\chi_2(\{1\}) \leq 1$. Consequently, $\mathcal{T}(F;A_1,A_2)$ depends upon whether or not the equation $xA_1 + yA_2 = F$ has solutions with $\deg x < A_2$ or $\deg y < A_1$ and

$$\begin{aligned}2(\deg F - \deg A_1 - \deg A_2) &\leq \mathcal{T}(F;A_1,A_2)\\ &\leq 2(\deg F - \deg A_1 - \deg A_2) + 2,\end{aligned}$$

which shows that, in this case, the upper bound for $\mathcal{T}(F;A_1,A_2)$ is much smaller than that found in the proof of Theorem 5.4.

6. An algorithm for solving FPP.

6.1. Set-up and notation. In this section, we construct an algorithm for computing $g(A_1,\ldots,A_n)$. In order to avoid trivial cases, we assume that $1 \notin \{A_1,\ldots,A_n\}$ and that the base field has characteristic 0 or greater than n. Our algorithm is based on the fact that, given a fixed polynomial F, we can decide whether or not (1.1) has a solution $(x_1,\ldots,x_n)$ by considering the coefficients of the polynomials in $(x_1,\ldots,x_n)$ as variables and solving the corresponding system of linear equations. This strategy was previously used in the example in subsection 3.2 and is formalized in what follows.

- We write $a_i = \deg A_i$ and

$$A_i = t^{a_i} + \sum_{j=0}^{a_i-1} \alpha_{ij} t^j.$$

- As a consequence of Corollary 3.2, we assume that d is a positive integer satisfying $d \geq \min\{a_i : 1 \leq i \leq n\}$.
- The k-vector space of polynomials of degree $\leq d$ is $\mathcal{P}_d$.

• In k^{d+1}, we identify a polynomial

$$\sum_{i=0}^{e} \psi_i t^i \in \mathcal{P}_d$$

of degree e with either the vector

$$(\underbrace{0,\dots,0}_{d-e},\underbrace{\psi_e,\psi_{e-1},\dots,\psi_0}_{e+1}), \tag{6.1}$$

or a column matrix, which is the transpose of the above vector. Note that often we use the polynomial and matrix representation of an element in $\mathcal{P}_d$ interchangeably.

• Since, by assumption, $A_i \in \mathcal{P}_d$, we let D_i be the column matrix associated to A_i under the above identification of $\mathcal{P}_d$ with k^{d+1}.

• The set of monic polynomials of degree d is $\mathcal{M}_d$.

• The set of monic polynomials F of degree d for which (1.1) has a solution with $x_i \in k[t]_{\geq 0}$ is $\mathcal{F}_d$. Note that $d = g(A_1,\dots,A_n)$ is the largest integer d for which $\mathcal{F}_d \subsetneq \mathcal{M}_d$.

• $\mathcal{T}_d = \mathcal{T}_d(a_1,\dots,a_n)$ is the set of n-tuples $T = (e_1,\dots,e_n)$ such that:

(1) there exists a unique integer $j = j(T)$ such that $1 \leq j \leq n$ and $e_j = d - a_j \geq 0$; and
(2) for $i \neq j$, we have $e_i = -\infty$ or e_i is an integer satisfying $0 \leq e_i < d - a_i$.

Note that $\mathcal{T}_d$ is closely related to the set of types as defined in Section 5.

• Consider the following subsets of the integers $1 \leq i \leq n$:

$$\mathcal{R}_T = \{i : 0 < e_i \leq d - a_i\} \quad \text{and} \quad \mathcal{S}_T = \{i : e_i = 0\}. \tag{6.2}$$

Note that, if $\mathcal{R}_T = \emptyset$, then $d = a_{j(T)}$, and consequently, $\mathcal{S}_T \neq \emptyset$. Also, if $i \notin \mathcal{R}_T \cup \mathcal{S}_T$, then $e_i = -\infty$.

• Let the *index* of T be

$$\operatorname{ind}(T) = \sum_{i=1}^{n} \max(e_i, 0).$$

Observe that $\mathcal{R}_T \neq \emptyset$ if and only if $\operatorname{ind}(T) > 0$. If this is the case, then $\operatorname{ind}(T) = \sum_{i\in\mathcal{R}_T} e_i$.

Remark 6.1. The elements of $\mathcal{T}_d$ are related to FPP in the following way. Any $(x_1, \ldots, x_n) \in (k[t]_{\geq 0})^n$ such that $(\deg x_1, \ldots, \deg x_n) \in \mathcal{T}_d$ yields a solution to (1.1) for some monic polynomial F of degree d. Conversely, given a monic polynomial F of positive degree d, a solution $(x_1, \ldots, x_n) \in (k[t]_{\geq 0})^n$ of (1.1) yields the n-tuple $(\deg x_1, \ldots, \deg x_n) \in \mathcal{T}_d$.

The strategy of our algorithm is to run through all integers d which are not larger than the upper bound given by Remark 2.4 and find the largest d for which $\mathcal{F}_d \subsetneq \mathcal{M}_d$. In order to follow this strategy, we need to find criteria for deciding whether or not $\mathcal{F}_d = \mathcal{M}_d$. In this section, we give such a criterion. It is based upon the fact that $\mathcal{F}_d$ is a finite union of affine subspaces of $\mathcal{P}_d$.

Definition 6.2. Let $\mathcal{V}$ be a finite-dimensional k-vector space. We say that $\mathcal{A}$ is an *affine subspace* of $\mathcal{V}$ if there exist a vector subspace $\mathcal{U} \subset \mathcal{V}$ and a vector $\mathbf{v} \in \mathcal{V}$ such that $\mathcal{A} = \mathcal{U} + \mathbf{v}$. The *dimension* of $\mathcal{A}$, $\dim \mathcal{A}$, is defined to be $\dim \mathcal{U}$.

Remark 6.3. In the sequence, we use the following easy facts about affine subspaces whose proofs are left to the reader.

(1) Let $\mathcal{A}$ and $\mathcal{B}$ be affine subspaces with $\dim \mathcal{A} = \dim \mathcal{B}$. If $\mathcal{A} \subset \mathcal{B}$, then $\mathcal{A} = \mathcal{B}$.

(2) If $\mathbf{u}, \mathbf{v} \in \mathcal{A}$ and $\alpha \in k$, then $(1 - \alpha)\mathbf{u} + \alpha\mathbf{v}$ is also an element of $\mathcal{A}$.

(3) Note that, inside of k^{d+1}, the set $\mathcal{M}_d$ of monic polynomials of degree d is the affine subspace $(1, 0, \ldots, 0) + (0, \psi_{d-1}, \psi_{d-2}, \ldots, \psi_0)$ and $\dim \mathcal{M}_d = d$.

For each $T \in \mathcal{T}_d$, below we define a matrix A_T and a column matrix B_T, both with $d+1$ rows. Ultimately, we associate to each T the affine space given by the translation of the column space of A_T by the vector B_T. In the case where $\mathcal{R}_T = \emptyset$, we define A_T and B_T to be the zero matrix of order $(d+1) \times 1$ and $\sum_{i \in \mathcal{S}_T} D_i$, respectively.

Otherwise, for $i \in \mathcal{R}_T$, we give a definition of the next $(d+1) \times (e_i+1)$ matrix where the jth column of M_i is the vector representation in k^{d+1} of the polynomial $A_i t^{e_i - j + 1}$, for $1 \leq j \leq e_i + 1$. Let $\overline{M}_i$ be the $(d+1)$

$\times e_i$ matrix obtained from M_i by removing its first column C_i. We define A_T to be the block row matrix of order $(d+1) \times \operatorname{ind}(T)$

$$A_T = [\overline{M}_i]_{i \in \mathcal{R}_T}$$

and B_T to be the column matrix of order $(d+1) \times 1$

$$B_T = \sum_{i \in \mathcal{R}_T} C_i + \sum_{i \in \mathcal{S}_T} D_i,$$

where $\sum_{i \in \mathcal{S}_T} D_i$ is defined to be the zero vector, if $\mathcal{S}_T = \emptyset$.

$$M_i = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \alpha_{i(a_i-1)} & 1 & 0 & \ldots & 0 \\ \alpha_{i(a_i-2)} & \alpha_{i(a_i-1)} & 1 & \ddots & \vdots \\ \vdots & \alpha_{i(a_i-2)} & \alpha_{i(a_i-1)} & \ddots & 0 \\ \alpha_{i1} & \vdots & \alpha_{i(a_i-2)} & \ddots & 1 \\ \alpha_{i0} & \alpha_{i1} & \vdots & \ddots & \alpha_{i(a_i-1)} \\ 0 & \alpha_{i0} & \alpha_{i1} & \vdots & \alpha_{i(a_i-2)} \\ 0 & 0 & \alpha_{i0} & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \alpha_{i1} \\ 0 & 0 & 0 & \cdots & \alpha_{i0} \end{bmatrix}.$$

Remark 6.4.

(1) If $x_i = \sum_{j=0}^{e_i} \chi_{ij} t^j$ is a polynomial with $\deg x_i = e_i$, then the product of polynomials $x_i A_i$ is an element of $\mathcal{P}_d$ and can be identified under (6.1) with the product of matrices $M_i X_i$, where X_i is the column vector $(\chi_{ie_i}, \ldots, \chi_{i0})$.

(2) We have that rank $A_T \leq d$. This is obvious if $\mathcal{R}_T = \emptyset$. If $\mathcal{R}_T \neq \emptyset$, first note that the highest possible rank for the matrices M_i can only happen when the first entry in C_i is 1. Even in this case, if we remove the first column C_i of M_i, we are left with the matrix $\overline{M}_i$ whose first row is zero. Consequently, A_T has at most d non-zero rows.

(3) For any $T \in \mathcal{T}_d$, the first entry in B_T is 1. Therefore, if $\mathcal{V}_T$ is the column space of the matrix A_T, then $\mathcal{V}_T + B_T \subset \mathcal{M}_d$ under the identification given by (6.1).

We are now ready to prove the first main result of this section.

Theorem 6.5. *Let d, $\mathcal{F}_d$, A_T and B_T be as defined above. Then $\mathcal{F}_d$ is the union of a finite number of affine subspaces of $\mathcal{P}_d$. More precisely, under the identification of $\mathcal{P}_d$ with k^{d+1},*

$$\mathcal{F}_d = \bigcup_{T \in \mathcal{T}_d} (\mathcal{V}_T + B_T),$$

where $\mathcal{V}_T$ is the column space of the matrix A_T.

Proof. All we need to do is to prove the equality

$$\mathcal{F}_d = \bigcup_{T \in \mathcal{T}_d} (\mathcal{V}_T + B_T).$$

Let $T = (e_1, \ldots, e_n) \in \mathcal{T}_d$, and let $\mathcal{R}_T$ and $\mathcal{S}_T$ be defined as in (6.2). For such a T, we construct an n-tuple $(x_1, \ldots, x_n) \in (k[t]_{\geq 0})^n$ such that $T = (\deg x_1, \ldots, \deg x_n)$. First, we let $x_i = 1$ or $x_i = 0$, if $i \in S_T$ or $i \notin \mathcal{R}_T \cup \mathcal{S}_T$, respectively. Otherwise, $i \in \mathcal{R}_T$, and we can choose x_i to be any monic polynomial of degree e_i

$$x_i = t^{e_i} + \sum_{j=0}^{e_i - 1} \chi_{ij} t^j.$$

Consider the $(e_i + 1) \times 1$ matrix

$$X_i = \begin{bmatrix} 1 \\ \chi_{i(e_i-1)} \\ \vdots \\ \chi_{i0} \end{bmatrix},$$

and let $\overline{X}_i$ be the $e_i \times 1$ matrix obtained from X_i by removing its first row. By definition of $\mathcal{T}_d$, the product $x_i A_i$ is a polynomial of degree $\leq d$, which we identify with a $(d+1) \times 1$ column matrix as in (6.1). The column matrix $x_i A_i$ is the zero matrix if $i \notin \mathcal{R}_T \cup \mathcal{S}_T$; it is the matrix

D_i, if $i \in \mathcal{S}_T$; and if $i \in \mathcal{R}_T$, it is equal to the product of matrices $M_i X_i$.

In the case where $\mathcal{R}_T \neq \emptyset$, the above discussion shows that $\sum_{i=1}^{n} x_i A_i$, when identified with the $(d+1)\times 1$ column matrix in (6.1), satisfies

$$\begin{aligned}\sum_{i=1}^{n} x_i A_i &= \sum_{i\in\mathcal{R}_T} M_i X_i + \sum_{i\in\mathcal{S}_T} D_i \\ &= \sum_{i\in\mathcal{R}_T} C_i + \sum_{i\in\mathcal{R}_T} \overline{M}_i \overline{X}_i + \sum_{i\in\mathcal{S}_T} D_i \\ &= \sum_{i\in\mathcal{R}_T} \overline{M}_i \overline{X}_i + B_T,\end{aligned}$$

It follows from the basic properties of matrices that $\sum_{i\in\mathcal{R}_T} \overline{M}_i \overline{X}_i$ is a linear combination of the columns of matrix A_T. Therefore, under the identification in (6.1), the set of linear combinations

$$\sum_{i=1}^{n} x_i A_i$$

such that

$$\begin{aligned}&(x_1, \ldots, x_n) \in (k[t]_{\geq 0})^n, \\ &(\deg x_1, \ldots, \deg x_n) \in \mathcal{T}_d\end{aligned}$$

and

$$\mathcal{R}_{(\deg x_1, \ldots, \deg x_n)} \neq \emptyset$$

is equal to

$$\bigcup_{\substack{T\in\mathcal{T}_d \\ \mathcal{R}_T\neq\emptyset}} (\mathcal{V}_T + B_T).$$

When $\mathcal{R}_T = \emptyset$, then

$$\sum_{i=1}^{n} x_i A_i = \sum_{i\in\mathcal{S}_T} D_i = A_T + B_T,$$

which shows that, in any case, the set of linear combinations $\sum_{i=1}^{n} x_i A_i$ such that $(x_1, \ldots, x_n) \in (k[t]_{\geq 0})^n$ and $(\deg x_1, \ldots, \deg x_n) \in \mathcal{T}_d$ is equal

to

$$\bigcup_{T\in\mathcal{T}_d}(\mathcal{V}_T + B_T).$$

On the other hand, as a consequence of the definition of $\mathcal{T}_d$, it follows that the set of linear combinations $\sum_{i=1}^n x_i A_i$ such that $(x_1,\dots,x_n) \in (k[t]_{\geq 0})^n$ and $(\deg x_1,\dots,\deg x_n) \in \mathcal{T}_d$ is equal to $\mathcal{F}_d$. Therefore,

$$\mathcal{F}_d = \bigcup_{T\in\mathcal{T}_d}(\mathcal{V}_T + B_T),$$

as desired. □

The second main result of this section gives a criterion for deciding whether $\mathcal{F}_d = \mathcal{M}_d$. It is a consequence of the description of $\mathcal{F}_d$ contained in the previous result and the fact that a vector space cannot be covered by a finite union of proper subspaces.

Lemma 6.6. *Let $\mathcal{A}$ be an affine space over a field k, and let $\mathcal{U}_i \subset \mathcal{A}$ be proper affine subspaces, for i in an indexing set I. If*

$$\mathcal{A} = \bigcup_{i\in I}\mathcal{U}_i,$$

then $|I| \geq |k| + 1$.

Proof. See, for instance, **[4,** Section 3]. □

Theorem 6.7. *Let d, $\mathcal{F}_d$, and A_T be defined as above. Suppose the base field k satisfies $|\mathcal{T}_d| < |k|$. Then $\mathcal{F}_d = \mathcal{M}_d$ if and only if* $\operatorname{rank} A_T = d$, *for some $T \in \mathcal{T}_d$.*

Proof. As before, we identify $\mathcal{P}_d$ with k^{d+1} using (6.1). Note that, from Theorem 6.5, $\mathcal{F}_d = \mathcal{M}_d$ implies that $\mathcal{M}_d$ is a finite union of proper affine subspaces. Therefore, the result we want to prove is essentially an application of Lemma 6.6. Nonetheless, below we provide a proof that follows that in **[4,** Section 3] but which is more suitable for computations. Our ultimate goal is to use it to find a critical example of FPP for $A_1,\dots,A_n$.

If $\operatorname{rank} A_T = d$, for some $T \in \mathcal{T}_d$, then $\dim(\mathcal{V}_T + B_T) = d = \dim \mathcal{M}_d$ and $\mathcal{F}_d = \mathcal{M}_d$ since $\mathcal{V}_T + B_T \subset \mathcal{F}_d \subset \mathcal{M}_d$. In order to prove the converse,

we show that, if

$$\operatorname{rank} A_T = \dim(\mathcal{V}_T + B_T) < d \quad \text{for all } T \in \mathcal{T}_d,$$

then

$$\bigcup_{T\in\mathcal{T}_d} (\mathcal{V}_T + B_T) \subsetneq \mathcal{M}_d.$$

First, let $\dim \mathcal{V}_T^{\perp}$ be the orthogonal complement of $\mathcal{V}_T$ under the canonical non-degenerate symmetric bilinear form $\mathbf{u}\cdot\mathbf{v}$ on k^{d+1}. If $\operatorname{rank} A_T < d$ for all $T \in \mathcal{T}_d$, then $\dim \mathcal{V}_T^{\perp} \geq 2$. From Remark 6.4, it follows that $\mathbf{e} = (1, 0, \ldots, 0) \in \mathcal{V}_T^{\perp}$. As a result, we can choose a non-zero vector $\mathbf{n}_T \in \mathcal{V}_T^{\perp}$ which is linearly independent of $\mathbf{e}$. Thus, $\mathcal{V}_T + B_T$ is a subset of

$$\mathcal{A}_T = \{\mathbf{u} \in k^{d+1} : \mathbf{e}\cdot\mathbf{u} = 1,\ \mathbf{n}_T\cdot\mathbf{u} = \mathbf{n}_T\cdot B_T\}.$$

Clearly, $\dim \mathcal{A}_T = d - 1$ for all $T \in \mathcal{T}_d$. Under these assumptions, it is enough to prove that

$$\bigcup_{T\in\mathcal{T}_d} \mathcal{A}_T \subsetneq \mathcal{M}_d.$$

Without loss of generality, we assume that, for all $U \in \mathcal{T}_d$,

$$\mathcal{A}_U \setminus \bigcup_{T\in\mathcal{T}_d\setminus\{U\}} \mathcal{A}_T \neq \emptyset.$$

This guarantees the existence of a vector $\mathbf{u} \in \mathcal{M}_d$ such that $\mathbf{u} \in \mathcal{A}_U$ but $\mathbf{u} \notin \mathcal{A}_T$ for all $T \neq U$. Additionally, we can choose $\mathbf{v} \in \mathcal{M}_d \setminus \mathcal{A}_U$. Consider the line $\mathcal{D} = \{(1-\alpha)\mathbf{u} + \alpha\mathbf{v} : \alpha \in k\} \subset \mathcal{M}_d$. The result follows if we are able to prove that $|\mathcal{A}_T \cap \mathcal{D}| \leq 1$ for all $T \in \mathcal{T}_d$. Indeed, in this case,

$$\left|\mathcal{D} \bigcap \Big(\bigcup_{T\in\mathcal{T}_d} \mathcal{A}_T \Big)\right| = \left| \bigcup_{T\in\mathcal{T}_d} \mathcal{A}_T \cap \mathcal{D} \right| \leq |\mathcal{T}_d|.$$

Since $|k| = |\mathcal{D}|$, this proves that

$$\bigcup_{T\in\mathcal{T}_d} \mathcal{A}_T \subsetneq \mathcal{M}_d \quad \text{if } |k| > |\mathcal{T}_d|.$$

In order to compute $\mathcal{A}_T \cap \mathcal{D}$, we need to solve for α the equation $\mathbf{n}_T \cdot [(1-\alpha)\mathbf{u} + \alpha\mathbf{v}] = \mathbf{n}_T \cdot B_T$, which can be simplified to

$$[\mathbf{n}_T \cdot (\mathbf{v} - \mathbf{u})]\alpha = \mathbf{n}_T \cdot (B_T - \mathbf{u}).$$

The above equation in α has more than one solution if and only if

$$\mathbf{n}_T \cdot (\mathbf{v} - \mathbf{u}) = 0 \quad \text{and} \quad \mathbf{n}_T \cdot (B_T - \mathbf{u}) = 0,$$

which, in turn, occurs if and only if

$$\mathbf{n}_T \cdot \mathbf{v} = \mathbf{n}_T \cdot B_T \quad \text{and} \quad \mathbf{n}_T \cdot \mathbf{u} = \mathbf{n}_T \cdot B_T.$$

This last equation is equivalent to the fact that $\mathbf{u}, \mathbf{v} \in \mathcal{A}_T$. Since this contradicts the choice of $\mathbf{u}$ and $\mathbf{v}$, we conclude that $\mathcal{A}_T \cap \mathcal{D}$ has at most one element. We can actually say a bit more: $\mathcal{A}_T \cap \mathcal{D} = \emptyset$, if $\mathbf{n}_T \cdot \mathbf{v} = \mathbf{n}_T \cdot \mathbf{u}$; otherwise,

$$[(1-\alpha)\mathbf{u} + \alpha\mathbf{v}] \in \mathcal{A}_T \quad \text{for } \alpha = \mathbf{n}_T \cdot \frac{B_T - \mathbf{u}}{\mathbf{n}_T \cdot (\mathbf{v} - \mathbf{u})}. \quad \square$$

This last result allows us to prove the following lower bound for the Frobenius degree of $A_1, \ldots, A_n$.

Corollary 6.8. *Suppose that the base field k satisfies $|\mathcal{T}_{g^+}| < |k|$ for some positive integer g^+. If $d \leq g^+$ is an integer such that*

$$\sum_{i=1}^{n} \max(d - a_i, 0) \leq d,$$

then $\mathcal{F}_d \subsetneq \mathcal{M}_d$. In particular,

$$\max\left\{ d \in \mathbb{Z} : \sum_{i=1}^{n} \max(d - a_i, 0) \leq d \right\} \leq g(A_1, \ldots, A_n).$$

Proof. First note that $d \leq g^+$ implies

$$|\mathcal{T}_d| \leq |\mathcal{T}_{g^+}| < |k|.$$

Therefore, the assumptions of Theorem 6.7 are satisfied for d. Moreover, assume that d is an integer such that $\sum_{i=1}^{n} \max(d - a_i, 0) \leq d$. As a consequence of Theorem 6.7, to show that $\mathcal{F}_d \subsetneq \mathcal{M}_d$, we need to prove that $\operatorname{rank} A_T < d$ for all $T \in \mathcal{T}_d$ with $\mathcal{R}_T \neq \emptyset$.

Since the number of columns of a matrix is an upper bound for its rank, it follows that

$$\operatorname{rank} A_T \leq \operatorname{ind}(T)$$

for all $T \in \mathcal{T}_d$ satisfying $\mathcal{R}_T \neq \emptyset$. If $\mathcal{R}_T = \{d - a_{j(T)}\}$, then

$$\operatorname{rank} A_T \leq \operatorname{ind}(T) = \sum_{i=1}^{n} \max(d - a_i, 0) = d - a_{j(T)} < d;$$

otherwise, $\mathcal{R}_T \neq \{d - a_{j(T)}\}$ and

$$\operatorname{ind}(T) \leq \sum_{i \in \mathcal{R}_T} e_i + \sum_{i \notin \mathcal{R}_T} \max(e_i, 0) < \sum_{i=1}^{n} \max(d - a_i, 0).$$

Thus, if d is an integer such that

$$\sum_{i=1}^{n} \max(d - a_i, 0) \leq d,$$

then $\operatorname{rank} A_T < d$, for all $T \in \mathcal{T}_d$ with $\mathcal{R}_T \neq \emptyset$. □

Remark 6.9. For every $n \geq 2$, we can use Lemma 4.1 to show that the lower bound given in Corollary 6.8 is sharp. In fact, choose pairwise coprime monic polynomials $A_1, \ldots, A_n$ such that $\deg A_i = a > 0$ for all $1 \leq i \leq n$. If

$$\widetilde{A}_i = \prod_{j=1}^{n} \frac{A_j}{A_i},$$

then $\deg \widetilde{A}_i = (n-1)a$ and, from Lemma 4.1,

$$g(\widetilde{A}_1, \ldots, \widetilde{A}_n) = \deg A_1 + \cdots + \deg A_n = na.$$

On the other hand, na satisfies

$$\sum_{i=1}^{n} \max(na - \deg \widetilde{A}_i, 0) = \sum_{i=1}^{n} \max(a, 0) \leq na.$$

Thus,

$$\begin{aligned} na &\leq \max\left\{ d \in \mathbb{Z} : \sum_{i=1}^{n} \max(d - \deg \widetilde{A}_i, 0) \leq d \right\} \\ &\leq g(\widetilde{A}_1, \ldots, \widetilde{A}_n) = na. \end{aligned}$$

As discussed in subsection 3.2, the Frobenius degree g of coprime monic polynomials $A_1, \ldots, A_n$ over k is not affected by a field extension K/k, if $|k|$ is sufficiently large. As is shown below, this statement is also a consequence of Theorem 6.7.

Corollary 6.10. *Let $A_1, \ldots, A_n$ be coprime monic polynomials over a field k, let K/k be a field extension and let g^+ be the upper bound given in Remark* 2.4. *If $|k| > |\mathcal{T}_{g^+}|$, then*

$$g_K(A_1, \ldots, A_n) = g_k(A_1, \ldots, A_n).$$

Proof. For a field extension K/k, we let $g_K = g_K(A_1, \ldots, A_n)$. We want to show that $g_K = g_k$. First, note that

$$g_k \leq g_K \leq g^+.$$

Thus, it remains to prove $g_K \leq g_k$. For that matter, let d be any positive integer. It is not difficult to see that $\mathcal{T}_d$ depends only upon d and the polynomials $A_1, \ldots, A_n$, and not on the base field in which the solutions of (1.1) are defined. Similarly, for all $T \in \mathcal{T}_d$, A_T and B_T are independent of the base field in which FPP is being considered.

On the other hand, $\mathcal{F}_d$ and $\mathcal{M}_d$ depend on the base field K, and we make this dependence explicit by writing ${\mathcal{F}_d}^K$ and ${\mathcal{M}_d}^K$, respectively. Since

$$|\mathcal{T}_{g_K}| \leq |\mathcal{T}_{g^+}| < |k| \leq |K|,$$

and $\operatorname{rank} A_T$ is independent of the field extension K/k, it follows from the definition of g_K and two applications of Theorem 6.7 that $\mathcal{F}^k_{g_K} \subsetneq \mathcal{M}^k_{g_K}$. Therefore, $g_K \leq g_k$, as desired. □

6.2. The algorithm. The notation of the previous section is used in this subsection.

The algorithm described here only works under the assumption that the base field k satisfies $|k| > |\mathcal{T}_{g^+}|$, where g^+ is the upper bound obtained in Remark 2.4. Under this assumption, we can run through all integers $d \leq g^+$ in decreasing order and use Theorem 6.7 to check whether $\mathcal{F}_d = \mathcal{M}_d$. The first value of d for which $\mathcal{F}_d \subsetneq \mathcal{M}_d$ is the Frobenius degree of $A_1, \ldots, A_n$.

In the case where $|k| \leq |\mathcal{T}_{g^+}|$, the above strategy works except for the use of Theorem 6.7 to decide whether $\mathcal{F}_d = \mathcal{M}_d$. Instead, we can check whether such an equality holds by one of the following "brute force" methods. $\mathcal{F}_d$ can be constructed by computing all possible linear combinations

$$\sum_{i=1}^{n} x_i A_i = F,$$

with $x_i \in k[t]_{\geq 0}$ and $\deg F = d$. Then, $\mathcal{F}_d \subsetneq \mathcal{M}_d$ if and only if $|\mathcal{F}_d| < q^d = |\mathcal{M}_d|$.

Alternatively, one can construct

$$\bigcup_{T \in \mathcal{T}_d} (\mathcal{V}_T + B_T) = \mathcal{F}_d$$

and check whether

$$\left| \bigcup_{T \in \mathcal{T}_d} (\mathcal{V}_T + B_T) \right| = q^d.$$

It is unclear which of these two methods is less computationally expensive if implemented for checking $\mathcal{F}_d = \mathcal{M}_d$.

If we assume that $|k| > |\mathcal{T}_{g^+}|$, then the algorithm we use is less expensive than any of the above brute force methods since, when we consider the matrix A_T, we are simultaneously considering all solutions $(x_1, \ldots, x_n)$ of (1.1) with $T = (\deg x_1, \ldots, \deg x_n) \in \mathcal{T}_d$. Also, unlike the computation of $|\bigcup_{T \in \mathcal{T}_d} (\mathcal{V}_T + B_T)|$, it is unnecessary to solve the large number of systems of linear equations associated to all possible intersections of the form $(\mathcal{V}_T + B_T) \cap (\mathcal{V}_U + B_U)$. Our algorithm is easy to implement and seems to perform fast, if the computation is only of $g(A_1, \ldots, A_n)$ (see the accompanying `Sage` worksheet at `https://sites.google.com/site/rpconcei/research`). If one also wants to find a critical example of FPP for $A_1, \ldots, A_n$, then there are

some added complications. These are due to the unpacking of some of the theoretical aspects of the argument for Theorem 6.7. In what follows, we first give a pseudo-code for computing $g(A_1, \ldots, A_n)$. Later, we give more details on how to implement the construction of a critical example for FPP. In both cases, we assume that the reader is able to implement the following sub-routines:

- UpperBound$(A_1, \ldots, A_n)$.
  Calculate an upper bound g^+ based on Remark 2.4.
  Input: $A_1, \ldots, A_n$.
  Output: g^+.
- LowerBound$(A_1, \ldots, A_n)$.
  Calculate the lower bound g^- given in Corollary 6.8.
  Input: $A_1, \ldots, A_n$.
  Output: g^-.
- Types$(d, A_1, \ldots, A_n)$.
  Construct the set $\mathcal{T}_d$.
  Input: d and $A_1, \ldots, A_n$.
  Output: The list of elements in $\mathcal{T}_d$.
- Tmatrices(T).
  Construct the matrices A_T and B_T.
  Input: An element T of $\mathcal{T}_d$.
  Output: The matrices A_T and B_T.

The pseudo-code for the computation of $g(A_1, \ldots, A_n)$ is given in Algorithm 6.1.

6.3. Constructing a critical example of FPP. In order to construct a counter-example of FPP for $A_1, \ldots, A_n$, we first transform the following qualitative statements contained in the proof of Theorem 6.7 into statements which can be checked algorithmically (we follow the notation as in the proof of Theorem 6.7):

• **Statement 1.** *$\mathcal{V}_T + B_T$ is a subset of an affine space $\mathcal{A}_T$ with* $\dim \mathcal{A}_T = d - 1$. In order to be able to construct $\mathcal{A}_T$ explicitly, we need to construct a non-zero vector $\mathbf{n}_T$ orthogonal to $\mathcal{V}_T$ and linearly independent from $\mathbf{e} = (1, 0, \ldots, 0)$. This may be done by considering $\mathbf{n}_T$ to be any non-zero solution of the linear system $A_T^t \mathbf{x} = \mathbf{0}$ which is also not a multiple of $\mathbf{e}$. Therefore, $\mathcal{A}_T$ is simply the solution set of the

Algorithm 6.1: Calculate $g(A_1, \dots, A_n)$.

Input: $A_1, \dots, A_n$.
Output: $g(A_1, \dots, A_n)$.
Require: $\gcd(A_1, \dots, A_n) = 1$, $\deg A_i > 0$, $n < p$ and $|k| > |\mathcal{T}_d|$.
$g^+ \leftarrow \textsc{UpperBound}(A_1, \dots, A_n)$
$g^- \leftarrow \textsc{LowerBound}(A_1, \dots, A_n)$
for $d \leftarrow g^+$ **to** g^- **do**
  $\mathcal{T}_d \leftarrow \textsc{Types}(d, A_1, \dots, A_n)$
  for $T = (e_1, \dots, e_n)$ in $\mathcal{T}_d$ **do**
    if $\sum_i \max(e_i, 0) < d$ **then** ▷ If condition holds, then $\operatorname{rank} A_T < d$ and the algorithm can move on to the next T.
    else
      $A_T, B_T \leftarrow \textsc{Tmatrices}(T)$
      if $\operatorname{rank} A_T = d$ **then** ▷ $d \neq g(A_1, \dots, A_n)$.
        Decrease d and restart the loop for d.
      else
      end if
    end if
  end for
  return d
end for

system of linear equations on $\mathbf{u}$

$$\begin{cases} \mathbf{e} \cdot \mathbf{u} = 1 \\ \mathbf{n}_T \cdot \mathbf{u} = \mathbf{n}_T \cdot B_T. \end{cases}$$

• **Statement 2.** *There exists a* $U \in \mathcal{T}_d$ *such that* $\mathcal{A}_U \setminus \bigcup_{T \in \mathcal{T}_d \setminus \{U\}} \mathcal{A}_T \neq \emptyset$. In order to construct such a U, we choose any $U \in \mathcal{T}_d$ and construct a list $\mathcal{L}$ of all $T \in \mathcal{T}_d$ for which $\mathcal{A}_T \neq \mathcal{A}_U$. Indeed, this is a consequence of the following claim: if $\mathcal{A}_U \subset \bigcup_{T \in \mathcal{J}} \mathcal{A}_T$, for some non-empty $\mathcal{J} \subsetneq \mathcal{T}_d$, then $\mathcal{A}_U = \mathcal{A}_V$, for some $V \in \mathcal{J}$. First, note that, under the assumption $\mathcal{A}_U \subset \bigcup_{T \in \mathcal{J}} \mathcal{A}_T$, we have

$$\mathcal{A}_U = \bigcup_{T \in \mathcal{J}} (\mathcal{A}_T \cap \mathcal{A}_U).$$

Observe that either $\mathcal{A}_T \cap \mathcal{A}_U = \emptyset$ or $\mathcal{A}_T \cap \mathcal{A}_U$ is an affine subspace of $\mathcal{A}_U$. Moreover, not all non-empty $\mathcal{A}_T \cap \mathcal{A}_U$ are proper subspaces of $\mathcal{A}_U$; otherwise, Lemma 6.6 would contradict the assumption $|\mathcal{T}_d| < |k|$.

Therefore, there exists a $V \in \mathcal{J}$ such that $\mathcal{A}_V \cap \mathcal{A}_U = \mathcal{A}_U$ and, since $\dim \mathcal{A}_U = \dim \mathcal{A}_T$ for all $T \in \mathcal{T}_d$, it follows that $\mathcal{A}_U = \mathcal{A}_V$.

The intersection $\mathcal{A}_U \cap \mathcal{A}_T$ is given by the system of linear equations on $\mathbf{u}$:

$$\begin{cases} \mathbf{e} \cdot \mathbf{u} = 1 \\ \mathbf{n}_U \cdot \mathbf{u} = \mathbf{n}_U \cdot B_U \\ \mathbf{n}_T \cdot \mathbf{u} = \mathbf{n}_T \cdot B_T \end{cases}$$

Since $\dim \mathcal{A}_U = \dim \mathcal{A}_T$, this system has rank < 3 if and only if $\mathcal{A}_U = \mathcal{A}_T$. This fact can be used to check whether $\mathcal{A}_U = \mathcal{A}_T$ and construct $\mathcal{L}$. Without loss of generality, we may replace $\mathcal{T}_d \leftarrow \mathcal{L} \cup \{U\}$.

• **Statement 3.** *There exist vectors* $\mathbf{u}, \mathbf{v} \in \mathcal{M}_d$ *such that* $\mathbf{u} \in \mathcal{A}_U$ *but* $\mathbf{u} \notin \mathcal{A}_T$ *for all* $T \neq U$, *and* $\mathbf{v} \notin \mathcal{A}_U$. In order to construct $\mathbf{u}$, we can randomly select $\mathbf{u} \in \mathcal{A}_U$ until

$$0 \neq \prod_{T \in \mathcal{T}_d} [\mathbf{n}_T \cdot (\mathbf{u} - B_T)].$$

From our choice of U, this routine is guaranteed to stop. The vector $\mathbf{v}$ can be chosen as a solution of

$$\mathbf{e} \cdot \mathbf{v} = 1 \quad \text{and} \quad \mathbf{n}_U \cdot \mathbf{v} = \mathbf{n}_U \cdot B_U + 1.$$

• **Statement 4.**

$$\bigcup_{T \in \mathcal{T}_d} \mathcal{A}_T \subsetneq \mathcal{M}_d \quad \text{if } |k| > |\mathcal{T}_d|.$$

Let $\Gamma = \{\alpha_T : T \in \mathcal{T}_d\}$, where $\alpha_T = 0$, if $\mathbf{n}_T \cdot \mathbf{v} = \mathbf{n}_T \cdot \mathbf{u}$; otherwise, $\alpha_T = \mathbf{n}_T \cdot (B_T - \mathbf{u})/[\mathbf{n}_T \cdot (\mathbf{v} - \mathbf{u})]$. Since $\alpha_U = 0$, it follows from an argument in the proof of Theorem 6.7 that

$$|\Gamma| = \left| \mathcal{D} \bigcap \left(\bigcup_{T \in \mathcal{T}_d} \mathcal{A}_T \right) \right| \leq |\mathcal{T}_d| < |k|.$$

Therefore, if we randomly select an element $\beta \in k \backslash \Gamma$, then $\mathbf{w} = (1 - \beta)\mathbf{u} + \beta\mathbf{v}$ is such that

$$\mathbf{w} \in \mathcal{M}_d \setminus \bigcup_{T \in \mathcal{T}_d} \mathcal{A}_T.$$

Algorithm 6.2: Calculate a critical example to FPP for $A_1, \ldots, A_n$.

Input: $A_1, \ldots, A_n$.
Output: A polynomial G with $\deg G = g(A_1, \ldots, A_n)$ for which (1.1) has no solution in $k[t]_{\geq 0}$.
Require: $\deg A_i > 0$, $n < p$ and $|k| > |\mathcal{T}_d|$.
Ensure: $g(A_1, \ldots, A_n) = d$
procedure NormalVector(A_T, B_T) ▷ Compute $\mathbf{n}_T$.
Solve $A_T^t \mathbf{x} = \mathbf{0}$
$\mathbf{n}_T \leftarrow$ Non-zero solution $\mathbf{x}$ that is not a multiple of $(1, 0, \ldots, 0)$.
return $[\mathbf{n}_T, B_T]$.
end procedure
$\mathbf{e} \leftarrow (1, 0, \ldots, 0)$
$\mathcal{T}_d \leftarrow$ Types($d, A_1, \ldots, A_n$)
$\mathcal{L} \leftarrow \{$NormalVector(Tmatrices($T$)) : $T \in \mathcal{T}_d\}$
Choose $U \in \mathcal{T}_d$.
$\mathcal{N} \leftarrow \emptyset$ ▷ Compute the set of normal vectors $\mathbf{n}_T$ without any redundancy with $\mathbf{n}_U$.
for $[\mathbf{n}_T, B_T]$ in $\mathcal{L}$ **do**
if $\operatorname{rank}\{\mathbf{e} \cdot \mathbf{w} = 1 \wedge \mathbf{n}_T \cdot \mathbf{w} = \mathbf{n}_T \cdot B_T \wedge \mathbf{n}_U \cdot \mathbf{w} = \mathbf{n}_U \cdot B_U\} = 3$
then $\mathcal{N} \leftarrow \mathcal{N} \cup \{[\mathbf{n}_T, B_T]\}$.
end if
end for
$\mathbf{u} \leftarrow$ RandomElement($\mathcal{A}_U$) ▷ Construct $\mathbf{u} \in \mathcal{A}_U \backslash \mathcal{A}_T$.
while $0 = \prod_{[\mathbf{n}_T, B_T] \in \mathcal{N}} [\mathbf{n}_T \cdot (\mathbf{u} - B_T)]$ **do**
$\mathbf{u} \leftarrow$ RandomElement($\mathcal{A}_U$)
end while
$\mathbf{v} \leftarrow$ solution of $\mathbf{e} \cdot \mathbf{v} = 1 \ \wedge \ \mathbf{n}_U \cdot \mathbf{v} = \mathbf{n}_U \cdot B_U + 1$ ▷ Construct $\mathbf{v} \in \mathcal{M}_d \backslash \mathcal{A}_U$.
$\Gamma \leftarrow \emptyset$ ▷ Construct the set Γ.
for $\mathbf{n}_T \in \mathcal{N}$ **do**
if $\mathbf{n}_T \cdot \mathbf{u} \neq \mathbf{n}_T \cdot \mathbf{v}$ **then**
$\Gamma \leftarrow \Gamma \cup \{\mathbf{n}_T \cdot (\mathbf{u} - B_T)/[\mathbf{n}_T \cdot (\mathbf{v} - \mathbf{u})]\}$
end if
end for
$\beta \leftarrow$ RandomElement(k^*)
while $\beta \in \Gamma$ **do**
$\beta \leftarrow$ RandomElement(k^*)
end while
return The polynomial associated to $(1 - \beta)\mathbf{u} + \beta\mathbf{v}$.

A pseudo-code for the construction of a critical example to FPP for $A_1, \ldots, A_n$ is given in Algorithm 6.2. It should be straightforward to implement it in parallel with Algorithm 6.1.

7. Further research on FPP. Generally, the research on problems translated from the arithmetic of $\mathbb{Z}$ into the realm of polynomials is as rich as its more classical counterpart. In the case at hand a quick glance at the long bibliography on FP shows that research on this topic has been diverse and extensive. This suggests that the study of FPP initiated in this paper may be extended and generalized in many directions. In this section, we present a brief overview of broad topics that have been the focus of research on the classical FP and some problems that are intrinsic to the setting of polynomials. We hope they will serve as a guide for future research on the problem over $k[t]$.

7.1. Formulae for $g(A_1, \ldots, A_n)$. In the classical FP, there exist formulae for particular values of n to compute the n-dimensional Frobenius number; however, none of them look as simple as Sylvester's formula for the two-dimensional FP: $g(p, q) = pq - p - q$. In fact, it was proven that, unlike the two-dimensional Frobenius problem, for $n > 3$, the Frobenius number of an n-tuple cannot be computed via a "polynomial" formula, see [**1,** Theorem 2.2.1].

There has also been interest in finding formulae for $g(a_1, \ldots, a_n)$ for special families of coprime numbers $a_1, \ldots, a_n$. For instance, [**1,** Theorem 3.3.2] shows that the Frobenius number of an arithmetic sequence is given by

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

where a, d and s are positive integers with $\gcd(a, d) = 1$.

Currently, none of the above results have analogues in the polynomial setting.

7.2. Complexity of computing $g(A_1, \ldots, A_n)$. FP is a difficult problem from the computational point of view. In fact, Alfonsin showed that FP is NP-hard, see [**1,** Theorem 1.3.1]. In the absence of a polynomial time algorithm that solves FP, the focus of research has

been on finding not-so-fast algorithms, algorithms for small values of n and algorithms for particular n-tuples.

The computational complexity of the algorithm for solving FPP developed in this paper has not been determined. However, we expect it to be high since it relies on the computation of the rank of a large number of matrices whose dimensions depend partially upon the number and the degree of the inputs $A_1, \ldots, A_n$. It would be interesting to find other algorithms which do not depend so heavily on rank computation.

7.3. Integers without representation. Closely related to the denumerant function and the classical FP is the function $N(a_1, \ldots, a_n)$ that counts the number of positive integers with no non-negative representation by coprime positive integers $a_1, \ldots, a_n$. A classical result is the formula for the two-dimensional case found by Sylvester **[5]**

$$N(p, q) = \frac{1}{2}(p-1)(q-1).$$

Even this simple case is not understood in the polynomial setting.

7.4. On the denumerant function. In Section 5, we considered the type-denumerant function as analogous to Sylvester's denumerant function. However, if the base field k is finite and $n < \mathrm{char}(k)$, then the number $d(F; A_1, \ldots, A_n)$ of monic solutions to (1.1) is finite and seems to be a more suitable analogue to Sylvester's denumerant function. We can compute a closed formula for $d(F; A_1, \ldots, A_n)$ when $n = 2$ and $\deg A_1 = \deg A_2 = 1$, but we are far from a complete understanding of such function in general. In particular, it would be interesting to compute an asymptotic formula for

$$d(F; A_1, \ldots, A_n) \quad \text{as } \deg F \to \infty.$$

7.5. Extension of the Frobenius problem to other integral domains. The first two authors are currently considering an axiomatization of the Frobenius problem that allows us to extend it to certain Euclidean rings and other integral domains. It is not certain whether or not this generalization can be used towards a natural extension of FP to a ring of integers of global fields.

Acknowledgments. We would like to thank the anonymous referee for a careful reading of the first draft of this paper, and the many suggestions that improved its presentation.

REFERENCES

1. J.L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Math. Appl. **30**, Oxford University Press, Oxford, 2005.

2. Michael Rosen, *Number theory in function fields*, Grad. Texts Math. **210**, Springer-Verlag, New York, 2002.

3. D.S. Thakur, *Function field arithmetic*, World Scientific Publishing Co., Inc., River Edge, NJ, 2004.

4. Pete L. Clark, *Covering numbers in linear algebra*, Amer. Math. Month. **119** (2012), 65–67.

5. J.J. Sylvester, *On subvariants, i.e. semi-invariants to binary quantics of an unlimited order*, Amer. J. Math. **5** (1882), 79–136.

Gettysburg College, Department of Mathematics, 300 North Washington Street, Gettysburg, PA 17325
Email address: **rconceic@gettysburg.edu**

Universidade Federal, Rural de Pernambuco, Departamento de Matemática, UFRPE, Rua Dom Manoel de Medeiros, s/n/ Dois Irmãos–CEP 52171-900, Recife/PE/Brazil
Email address: **rodrigo.gondim.neves@gmail.com**

DB Risk Center, Otto-Suhr-Allee 16, 10585 Berlin, Germany
Email address: **rodmiga@yahoo.com**