The generalized Frobenius problem via restricted partition functions

Kevin Woods*

Abstract

Given relatively prime positive integers, $a_1, \dots, a_n$, the Frobenius number is the largest integer with no representations of the form $a_1 x_1 + \cdots + a_n x_n$ with nonnegative integers x_i. This classical value has recently been generalized: given a nonnegative integer k, what is the largest integer with at most k such representations? Other classical values can be generalized too: for example, how many nonnegative integers are representable in at most k ways? For sufficiently large k, we give a complete answer to these questions by understanding how the output of the restricted partition function (the function $f(t)$ giving the number of representations of t) "interlaces" with itself. Furthermore, we give the full asymptotics of all of these values, as well as reprove formulas for some special cases (such as the $n = 2$ case and a certain extremal family from the literature). Finally, we obtain the first two leading terms of the restricted partition function as a so-called quasi-polynomial.

1 Introduction

Given relatively prime positive integers, $a_1, \dots, a_n$, we define the *Frobenius number* to be the largest integer not contained in the semigroup

$$\{a_1 x_1 + \cdots + a_n x_n : \ x_i \in \mathbb{Z}_{\geq 0}\}.$$

Formulas for some special cases have been known since at least Sylvester [17] in the 1880's; for example, if $n = 2$, the Frobenius number is $a_1 a_2 - a_1 - a_2$. See the Ramírez Alfonsín text [15] for much more background.

More recently, Beck and Robins [7] propose a generalization. While the classical Frobenius number is the largest integer that can be represented as a nonnegative integer combination of $a_1, \dots, a_n$ in *zero* ways, we could instead take a fixed k and look at integers that can be represented in exactly k distinct ways. To be precise:

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

Definition 1.1. Given a vector $\mathbf{a} = (a_1, \ldots, a_n)$ of relatively prime positive integers and given $t \in \mathbb{Z}_{\geq 0}$, define the *restricted partition function*

$$f(\mathbf{a}; t) = \#(x_1, \ldots, x_n) \in \mathbb{Z}^n_{\geq 0} : \ a_1 x_1 + \cdots + a_n x_n = t$$

to be the number of ways to represent t by a nonnegative integer combination of the a_i. We write it as $f(t)$ when $\mathbf{a}$ is clear from context. Then define

- $g_{=k}$ to be the maximum $t \in \mathbb{Z}_{\geq 0}$ such that $f(t) = k$ (the largest integer that can be represented in *precisely* k ways), if any such t exist, and
- $g_{\leq k}$ to be the maximum $t \in \mathbb{Z}_{\geq 0}$ such that $f(t) \leq k$ (the largest integer that can be represented in *at most* k ways).

The Frobenius number is $g_{=0} = g_{\geq 0}$, but these numbers may differ for larger k:

Example 1.2. (Shallit and Stankewicz [16]) For $\mathbf{a} = (8, 9, 15)$, we have $g_{=15} = 169$, but $g_{\leq 15} = g_{=14} = 172$.

Remark 1.3. A consequence of Theorem 1.12 will be that $g_{=k} = g_{\leq k}$, for all sufficiently large k.

Example 1.4. Take $\mathbf{a} = (3, 4, 6)$. Here is a table of t and $f(t)$ for small t:

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	$\cdots$
$f(t)$	1	0	0	1	1	0	2	1	1	2	2	1	4	2	2	4	4	2	6	4	4	6	6	4	$\cdots$

For example, $g_{=0} = 5$ is the Frobenius number, and $g_{=2} = 17$; the two representations of 17 are $17 = 3 \cdot 1 + 4 \cdot 2 + 6 \cdot 1 = 3 \cdot 3 + 4 \cdot 2 + 6 \cdot 0$. Except for $k = 0$, which appears 3 times on this list of $f(t)$, values of k seem to appear either 6 times ($k = 1, 2, 4, \ldots$) or not at all $k = 3, 5, \ldots$. Figure 1 (inspired by Bardomero and Beck [3, Figure 1]) illustrates how these interlace in a periodic manner.

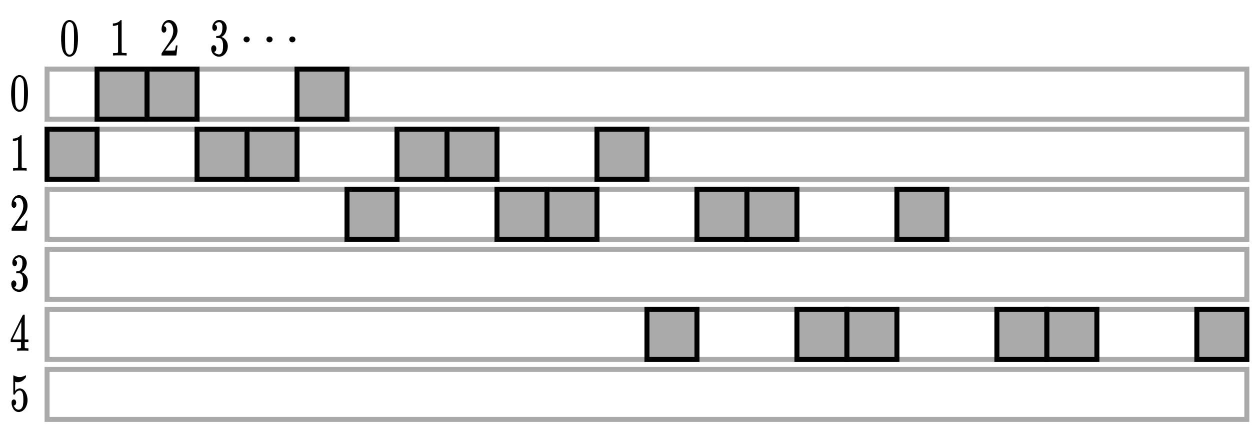

Figure 1: The horizontal axis is $t = 0, 1, 2, 3, \ldots$ and the vertical axis is $f(t)$, in Example 1.4.

In order to attack the generalized Frobenius problem, we will generalize Figure 1 and characterize (for sufficiently large t) how the level sets of $f(t)$ will interlace, and how they will increase with t. We will make heavy use of the fact that $f(t)$ is a very "nice" function. In fact, it is a *quasi-polynomial*:

Definition 1.5. A function $f : \mathbb{Z}_{\geq 0} \to \mathbb{Q}$ is a *quasi-polynomial of period* m if there exist polynomials $f_0, f_1, \ldots, f_{m-1} \in \mathbb{Q}[t]$ such that

$$f(t) = f_i(t), \text{ for } t \equiv i \bmod m.$$

The polynomials, f_i, are called the *constituent polynomials* of f.

The following folklore theorem shows that our f is a quasi-polynomial:

Proposition 1.6. *Let* $\mathbf{a} = (a_1, \ldots, a_n)$ *be a vector of relatively prime positive integers. Then* $f(\mathbf{a}; t)$ *is a quasi-polynomial of period* $m = \operatorname{lcm}(\mathbf{a}) = \operatorname{lcm}(a_1, \ldots, a_n)$*. Furthermore, the leading term of all of the constituent polynomials is*

$$\frac{1}{(n-1)! a_1 \cdots a_n} t^{n-1}.$$

This proposition is apparently due to Issai Schur; see Wilf [20, Section 3.15], and we present a proof as part of Proposition 1.19.

Our first theorem will tell us exactly how to determine whether $f(s) = f(t)$, $f(s) > f(t)$, or $f(s) < f(t)$, for sufficiently large s and t, and elucidate the structure of the output of f. First some notation:

Notation 1.7. For $1 \leq i \leq n$, define $\mathbf{a}_{-i} = (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$, so that, for example, $\gcd(\mathbf{a}_{-i}) = \gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$.

Theorem 1.8. *Let* $\mathbf{a} = (a_1, \ldots, a_n)$ *be a vector of relatively prime positive integers. For* $1 \leq i \leq n$*, let* $d_i = \gcd(\mathbf{a}_{-i})$*, and let* $p = d_1 \cdots d_n$*. Then*

1. *If* $s \in \mathbb{Z}_{\geq 0}$ *and* $b_i \in \mathbb{Z}$ *with* $0 \leq b_i < d_i$*, then*

$$f\left(sp + \sum_i a_i b_i\right) = f(sp).$$

2. *If* $t \in \mathbb{Z}_{\geq 0}$ *is sufficiently large, then there exists* $s \in \mathbb{Z}_{\geq 0}$ *and* $b_i \in \mathbb{Z}$ *with* $0 \leq b_i < d_i$ *such that*

$$t = sp + \sum_i a_i b_i$$

(that is, since all sufficiently large integers can be so represented, Part (1) implies we can concentrate on understanding $f(sp)$*).*

3. *For $1 \le i \le n$, let*
$$a_i' = \frac{a_i}{\prod_{j \neq i} d_i}$$
and $\mathbf{a}' = (a_1', \ldots, a_n')$. Then
$$f(\mathbf{a}; sp) = f(\mathbf{a}'; p),$$
for $s \in \mathbb{Z}_{\ge 0}$.

4. *For all sufficiently large $s \in \mathbb{Z}_{\ge 0}$,*
$$f\big(\mathbf{a}; (s+1)p\big) > f(\mathbf{a}; sp).$$

Example 1.9. Continuing Example 1.4 with $\mathbf{a} = (3, 4, 6)$, we can now better understand Figure 1. Since $d_1 = \gcd(4, 6) = 2$, $d_2 = \gcd(3, 6) = 3$, and $d_3 = \gcd(3, 4) = 1$, we have $p = 2 \cdot 3 \cdot 1 = 6$. If we take $b_i \in \mathbb{Z}$ with $0 \le b_i < d_i$, then the possible values of $\sum_i a_i b_i$ are

$$\begin{aligned} &3 \cdot 0 + 4 \cdot 0 + 6 \cdot 0 = 0, \quad && 3 \cdot 0 + 4 \cdot 1 + 6 \cdot 0 = 4, \quad && 3 \cdot 0 + 4 \cdot 2 + 6 \cdot 0 = 8, \\ &3 \cdot 1 + 4 \cdot 0 + 6 \cdot 0 = 3, \quad && 3 \cdot 1 + 4 \cdot 1 + 6 \cdot 0 = 7, \quad && 3 \cdot 1 + 4 \cdot 2 + 6 \cdot 0 = 11. \end{aligned}$$

Therefore, given $s \in \mathbb{Z}_{\ge 0}$, $f(6s + c)$ will be identical for $c \in \{0, 3, 4, 7, 8, 11\}$, which is exactly what we see in Figure 1. Furthermore, the value of $f(6s)$ will eventually increase with s; in this example, it is increasing for all s: $f(0) = 1$, $f(6) = 2$, $f(12) = 4$, $f(18) = 6$, and so on. All sufficiently large values in the range $f(\mathbb{Z}_{\ge 0})$ (in this case, all but $f(t) = 0$) will appear on this list.

Finally, $a_1' = 3/3 = 1$, $a_2' = 4/2 = 2$, and $a_3' = 6/6 = 1$. One can check by hand that

$$f(\mathbf{a}; 6s) = f(\mathbf{a}'; s) = \begin{cases} \frac{s^2}{4} + s + 1 & \text{if } s \text{ is even,} \\ \frac{s^2}{4} + s + \frac{3}{4} & \text{if } s \text{ is odd.} \end{cases}$$

Remark 1.10. Since $f(t)$ is a quasi-polynomial of period $m = \operatorname{lcm}(\mathbf{a})$ and we only need to look at values of t that are multiples of p, we must compute m/p of the constituent polynomials of f. In the above Example, $m/p = 12/6 = 2$ and we need two polynomials.

We now describe what this means for $g_{=k}$ and $g_{\le k}$, for sufficiently large k. We also describe some other quantities that often appear in both the classical and generalized Frobenius problem:

Definition 1.11. Let $\mathbf{a} = (a_1, \ldots, a_n)$ be a vector of relatively prime positive integers. For $k \in \mathbb{Z}_{\ge 0}$, define

- $h_{=k}$ to be the minimum $t \in \mathbb{Z}_{\ge 0}$ such that $f(t) = k$ (if any such t exist),
- $h_{\ge k}$ to be the minimum $t \in \mathbb{Z}_{\ge 0}$ such that $f(t) \ge k$,
- $c_{=k}$ to be the number of $t \in \mathbb{Z}_{\ge 0}$ such that $f(t) = k$,

- $c_{\leq k}$ to be the number of $t \in \mathbb{Z}_{\geq 0}$ such that $f(t) \leq k$,
- $s_{=k}$ to be the sum of all $t \in \mathbb{Z}_{\geq 0}$ such that $f(t) = k$,
- $s_{\leq k}$ to be the sum of all $t \in \mathbb{Z}_{\geq 0}$ such that $f(t) \leq k$,
- $F_{=k}(x)$ to be the generating function

$$\sum_{t \in \mathbb{Z}_{\geq 0}:\ f(t)=k} x^t,$$

- $F_{\geq k}(x)$ to be the generating function

$$\sum_{t \in \mathbb{Z}_{\geq 0}:\ f(t)\geq k} x^t.$$

Theorem 1.12. *Let $\mathbf{a} = (a_1, \ldots, a_n)$ be a vector of relatively prime positive integers, and define p, d_i as in Theorem 1.8. Define $g_{=k}, g_{\leq k}, h_{=k}, h_{\geq k}, c_{=k}, c_{\leq k}, s_{=k}, s_{\leq k}, F_{=k}(x), F_{\geq k}(x)$ as in Definitions 1.1 and 1.11. Then there are constants C_1, C_2 such that, for sufficiently large $s \in \mathbb{Z}_{\geq 0}$,*

$$\begin{aligned}
g_{=f(sp)} = g_{\leq f(sp)} &= sp + \sum_{i=1}^{n} (d_i - 1)a_i, \\
h_{=f(sp)} = h_{\geq f(sp)} &= sp, \\
c_{=f(sp)} &= p, \\
c_{\leq f(sp)} &= sp + C_1, \\
s_{=f(sp)} &= sp^2 + \sum_{i=1}^{n} \frac{pa_i(d_i - 1)}{2}, \\
s_{\leq f(sp)} &= \frac{1}{2}(sp)^2 + \left(\frac{p + \sum_{i=1}^{n} a_i(d_i - 1)}{2} \right) sp + C_2, \\
F_{=f(sp)}(x) &= x^{sp} \prod_i \frac{1 - x^{d_i a_i}}{1 - x^{a_i}}, \\
F_{\geq f(sp)}(x) &= \frac{x^{sp}}{1 - x^p} \prod_i \frac{1 - x^{d_i a_i}}{1 - x^{a_i}}.
\end{aligned}$$

Remark 1.13. Let's call k such that $c_{=k} = 0$ *trivial.* Then, for sufficiently large k, the only nontrivial k are of the form $k = f(sp)$, and the values of such $g_{=f(sp)}$, etc., are given by the above theorem. But this also gives us the values for trivial k: for example, $g_{\leq k} = g_{\leq f(sp)}$, if $f(sp) \leq k < f\big((s+1)p\big)$.

Notice that $g_{\le k}$ (like several of the other quantities) is of the form $g_{\le f(sp)} = sp + C$, where C is a constant. That is, it is roughly the inverse of f. Writing $q_1(x) \sim q_2(x)$, if $\lim_{x\to\infty} q_1(x)/q_2(x) = 1$, Proposition 1.6 gives that

$$f(t) \sim \frac{1}{(n-1)!a_1 \cdots a_n} t^{n-1}.$$

Therefore, if $k \sim f(sp)$ (in particular, if $f(sp) \le k < f\big((s+1)p\big)$), we have

$$sp \sim \big((n-1)!a_1 \cdots a_n k\big)^{1/(n-1)},$$

and we immediately get the asymptotics of these functions of k:

Corollary 1.14. *Given a vector* $\mathbf{a} = (a_1, \ldots, a_n)$ *of relatively prime positive integers, let* p *be the constant defined in Theorem 1.8. Then (restricting to* k *where the values are defined/nonzero)*

- $g_{=k}, g_{\le k}, h_{=k}, h_{\ge k}, c_{\le k} \;\sim\; \big((n-1)!a_1 \cdots a_n k\big)^{1/(n-1)}$,
- $c_{=k} \sim p$,
- $s_{=k} \sim p\big((n-1)!a_1 \cdots a_n k\big)^{1/(n-1)}$,
- $s_{\le k} \sim \frac{1}{2}\big((n-1)!a_1 \cdots a_n k\big)^{2/(n-1)}$.

Fukshansky and Schürmann [12] give bounds for $g_{\le k}$, for sufficiently large k, matching these asymptotics, and Aliev, Fukshansky, and Henk [2] find bounds on $g_{\le k}$ that are good for all k. The asymptotics of the other quantities seem to be new here.

These quantities have already been calculated exactly for $n = 2$, in Beck and Robins [7] and Bardomero and Beck [3]. We will reproduce these results nicely using Theorem 1.8:

Proposition 1.15. *Given relatively prime positive integers a_1, a_2,*

$$\begin{aligned}
g_{=k} = g_{\leq k} &= (k+1)a_1a_2 - a_1 - a_2, \\
\text{for } k \geq 1,\ h_{=k} = h_{\geq k} &= (k-1)a_1a_2, \\
h_{=0} &= 1 \ (\text{unless } a_1 = 1 \text{ or } a_2 = 1), \\
\text{for } k \geq 1,\ c_{=k} &= a_1a_2, \\
c_{=0} &= \frac{a_1a_2 - a_1 - a_2 + 1}{2}, \\
c_{\leq k} &= ka_1a_2 + c_{=0}, \\
\text{for } k \geq 1,\ s_{=k} &= \frac{a_1a_2(2a_1a_2k - a_1 - a_2)}{2}, \\
s_{=0} &= \frac{(a_1-1)(a_2-1)(2a_1a_2 - a_1 - a_2 - 1)}{12}, \\
s_{\leq k} &= \frac{a_1^2a_2^2}{2}k^2 + \frac{a_1a_2(a_1a_2 - a_1 - a_2)}{2}k + s_{=0}, \\
\text{for } k \geq 1,\ F_{=k}(x) &= \frac{x^{(k-1)a_1a_2}\left(1 - x^{a_1a_2}\right)^2}{\left(1 - x^{a_1}\right)\left(1 - x^{a_2}\right)}, \\
F_{=0}(x) &= \frac{1}{1-x} - \frac{1 - x^{a_1a_2}}{\left(1 - x^{a_1}\right)\left(1 - x^{a_2}\right)}, \\
\text{for } k \geq 1,\ F_{\geq k}(x) &= \frac{x^{(k-1)a_1a_2}\left(1 - x^{a_1a_2}\right)}{\left(1 - x^{a_1}\right)\left(1 - x^{a_2}\right)}, \\
F_{\geq 0} &= \frac{1}{1-x}.
\end{aligned}$$

The formulas for $g_{=k}, g_{\leq k}, h_{=k}, h_{\geq k}, c_{=k}, c_{\leq k}$ are due to (or immediately derivable from) [7] and the formulas for $s_{=k}, s_{\leq k}, F_{=k}(s), F_{\geq k}(x)$ are due to [3]. The $k = 0$ cases were previously known: see Sylvester [17] for $g_{=0}, c_{=0}$, Brown and Shiue [9] for $s_{=0}$, and Székely and Wormald [18] for $F_{=0}(x), F_{\geq 1}(x)$. Proposition 1.15 is an immediate corollary (the $n = 2$ case) of Proposition 1.16 and Remark 1.17 below:

Proposition 1.16. *Let $d_1, \ldots, d_n$ be pairwise coprime positive integers, and let $a_i = \prod_{j \neq i} d_i$, for $1 \leq i \leq n$. Let $p = d_1 \cdots d_n$ and $\sigma = a_1 + \cdots + a_n$. Other than $k = 0$, the only nontrivial*

k (that is, such that $c_{=k} > 0$) are $k = \binom{s+n-1}{n-1}$, for $s \in \mathbb{Z}_{\geq 0}$, and we have

$$\begin{aligned}
g_{=k} = g_{\leq k} &= (s+n)p - \sigma, \\
h_{=k} = h_{\geq k} &= sp, \\
c_{=k} &= p, \\
c_{\leq k} &= (s+1)p + \frac{(n-1)p - \sigma + 1}{2}, \\
s_{=k} &= \frac{p\big((2s+n)p - \sigma\big)}{2}, \\
F_{=k}(x) &= \frac{x^{sp}\,(1-x^p)^n}{(1-x^{a_1})\cdots(1-x^{a_n})}, \\
F_{\geq k}(x) &= \frac{x^{sp}\,(1-x^p)^{n-1}}{(1-x^{a_1})\cdots(1-x^{a_n})}.
\end{aligned}$$

The formula for $g_{=k} = g_{\leq k}$ was given in Beck and Kifer [6]. The other formulas seem to be new. If $n = 2$, then $a_1 = d_2$ and $a_2 = d_1$ are generic relatively prime positive integers; setting $k = \binom{s+1}{1} = s+1$ retrieves Proposition 1.15 for $k \geq 1$; the $k = 0$ case is covered by the following remark:

Remark 1.17. For $k = 0$, Tripathi [19] proved that

$$g_{=0} = (n-1)p - \sigma \quad \text{and} \quad c_{=0} = \frac{(n-1)p - \sigma + 1}{2}.$$

These can be obtained from $F_{\geq 1}(x)$ above ($k = 1$ corresponds to $s = 0$), as follows: We have

$$F_{\geq 0}(x) = \sum_{t \in \mathbb{Z}_{\geq 0}} x^t = \frac{1}{1-x} \quad \text{and} \quad F_{=0}(x) = F_{\geq 0}(x) - F_{\geq 1}(x).$$

Then $g_{=0}$ is the degree of $F_{=0}(x)$ as a polynomial and $c_{=0} = F_{=0}(1)$. One could compute $s_{=0} = F'_{=0}(1)$, which would also allow us to give a formula for $s_{\leq k}$, but the answer seems a bit messy; however, $F'_{=0}(1)$ does match the $n = 2$ value of $s_{=0}$ given in Proposition 1.15.

The following well-known lemma gives a useful recurrence and is worth highlighting here:

Lemma 1.18. *Given $t \in \mathbb{Z}_{\geq 0}$, and given i with $t \geq a_i$,*

$$f(\mathbf{a}; t) = f(\mathbf{a}; t - a_i) + f(\mathbf{a}_{-i}; t).$$

The proof is immediate: the first term on the right-hand-side is the number of ways to represent t with at least one a_i, and the second term is the number of ways to represent t with no a_i's.

Finally, we note that a partial fractions approach provides an alternative proof of Theorem 1.8(4), and a standard proof of Proposition 1.6. We include it here, in case it is useful. While the leading term of $f(\mathbf{a}; t)$ is well-known, this approach (together with Theorem 1.8) also allows us to compute the second leading term(s) as well:

Proposition 1.19. *Let $\mathbf{a} = (a_1, \ldots, a_n)$ be a vector of relatively prime positive integers, and let $m = \operatorname{lcm}(\mathbf{a})$. For $1 \le i \le n$, let $d_i = \gcd(\mathbf{a}_{-i})$, and let $p = d_1 \cdots d_n$. Then*

1. *$f(\mathbf{a}; t)$ is a quasi-polynomial of period m, and the leading term of all of the constituent polynomials is*
$$\frac{1}{(n-1)!a_1 \cdots a_n} t^{n-1}.$$
2. *If $d_i = 1$ for all i, then the leading two terms of all of the constituent polynomials are*
$$\frac{1}{(n-1)!a_1 \cdots a_n} t^{n-1} + \frac{a_1 + \cdots + a_n}{2(n-2)!a_1 \cdots a_n} t^{n-2}.$$
3. *For sufficiently large $s \in \mathbb{Z}_{\ge 0}$, $f\big((s+1)p\big) > f(sp)$.*

Remark 1.20. Combining Proposition 1.19(2) and Theorem 1.8 allows us to compute the leading two terms even when $d_i > 1$, though the second term will now depend on the constituent polynomial: given i and $t \equiv i \pmod{p}$, compute $r \in \mathbb{Z}_{\ge 0}$ such that $t \equiv r \pmod{p}$ and $f(\mathbf{a}; t) = f(\mathbf{a}; t - r)$, using Theorem 1.8(1) and (2). Let $s \in \mathbb{Z}$ be such that $t = sp + r$, and then
$$f(\mathbf{a}; t) = f(\mathbf{a}; sp) = f(\mathbf{a}'; s),$$
by Theorem 1.8(3). The two leading terms of $f(\mathbf{a}'; s)$ are given by Proposition 1.19(2), and then these can be used to compute the two leading terms of $f(\mathbf{a}; t)$ as a polynomial in t, by substituting $s = (t - r)/p$.

In the next section, we prove Theorem 1.8, Theorem 1.12, Proposition 1.16, and Proposition 1.19. Then we conclude with some open questions.

2 Proofs

Proof of Theorem 1.8. To prove Part 1, we proceed by induction on $\sum_j b_j$. If all b_j are zero, then this is trivially true: $f(sp + 0) = f(sp)$. Now assume $b_i > 0$, for some i. By Lemma 1.18 and the induction hypothesis,
$$\begin{aligned} f\left(\mathbf{a}; sp + \sum_j a_j b_j\right) &= f\left(\mathbf{a}; sp + a_i(b_i - 1) + \sum_{j \ne i} a_j b_j\right) + f\left(\mathbf{a}_{-i}; sp + \sum_j a_j b_j\right) \\ &= f\left(\mathbf{a}; sp\right) + f\left(\mathbf{a}_{-i}; sp + \sum_j a_j b_j\right). \end{aligned}$$
We need to show that $f\left(\mathbf{a}_{-i}; sp + \sum_j a_j b_j\right) = 0$. Indeed, using the facts that p and a_j ($j \ne i$) are multiples of $d_i = \gcd(\mathbf{a}_{-i})$, that a_i is relatively prime to d_i (or else $\gcd(\mathbf{a}) > 1$), and b_i is not a multiple of d_i (since $0 < b_i < d_i$), we have
$$sp + \sum_j a_j b_j \equiv a_i b_i \not\equiv 0 \pmod{d_i}.$$

Such a number cannot be represented as a combination of $\mathbf{a}_{-i}$, since a_j ($j \neq i$) are multiples of d_i.

To prove Part 2, given $t \in \mathbb{Z}_{\geq 0}$, for $1 \leq i \leq n$, let b_i be defined so that $0 \leq b_i < d_i$ and $b_i \equiv a_i^{-1} t \pmod{d_i}$ (a_i is invertible mod d_i, since they are relatively prime). Since a_j ($j \neq i$) is a multiple of d_i,

$$\sum_j a_j b_j \equiv a_i b_i \equiv t \pmod{d_i}.$$

Since $p = d_1 \cdots d_n$ with the d_i pairwise coprime (or else $\gcd(\mathbf{a}) > 1$), the Chinese Remainder Theorem yields $\sum_j a_j b_j \equiv t \pmod{p}$. Let s be the integer $\left(t - \sum_j a_j b_j\right)/p$, so that $t = sp + \sum_j a_j b_j$. As long as t is sufficiently large ($t \geq \sum_j a_j(d_j - 1)$), s will be nonnegative, and Part 2 follows.

To prove Part 3, suppose $sp = \sum_j a_j x_j$ ($x_j \in \mathbb{Z}_{\geq 0}$) is a representation of sp by $\mathbf{a}$. For each i, p and a_j ($j \neq i$) are multiples of d_i, and so

$$a_i x_i \equiv \sum_j a_j x_j = sp \equiv 0 \pmod{d_i}.$$

Since a_i and d_i are relatively prime, x_i must be a multiple of d_i. Let $y_i \in \mathbb{Z}_{\geq 0}$ be such that $x_i = d_i y_i$. Then

$$sp = \sum_i a_i x_i = \sum_i \left(\prod_{j \neq i} d_i\right) a_i' \cdot d_i y_i = p \sum_i a_i' y_i,$$

So $s = \sum_i a_i' y_i$ is a representation of s by $\mathbf{a}'$. Conversely, given any representation $s = \sum_i a_i' y_i$ ($y_i \in \mathbb{Z}_{\geq 0}$) by $\mathbf{a}'$, $sp = \sum_i a_i(d_i y_i)$ is a representation of sp by $\mathbf{a}$. Therefore $f(\mathbf{a}; sp) = f(\mathbf{a}'; p)$, as desired.

To prove Part 4, we assume without loss of generality (by Part 3) that $d_i = 1$ for all i, so we are trying to prove that $f(s+1) > f(s)$, for sufficiently large $s \in \mathbb{Z}_{\geq 0}$. The complication is that $f(s)$ and $f(s+1)$ are evaluated on different constituent polynomials of f, and it seems like these might "jump around."

We do know that all sufficiently large integers can be represented by $\mathbf{a}$. In particular, let $q \in \mathbb{Z}_{\geq 0}$ be such that q and $q+1$ are both representable; that is, $q = \sum_i a_i x_i$ and $q + 1 = \sum_i a_i y_i$ for $x_i, y_i \in \mathbb{Z}_{\geq 0}$. Take $s \in \mathbb{Z}_{\geq 0}$ sufficiently large (in particular, take $s \geq q$). We will use Lemma 1.18 repeatedly to relate both $f(s)$ and $f(s+1)$ to $f(s-q)$. Let's start by applying the recursion x_1 times on $f(\mathbf{a}; s)$, using $i = 1$:

$$\begin{aligned} f(\mathbf{a}; s) &= f(\mathbf{a}; s - a_1) + f(\mathbf{a}_{-1}; s) = \\ &= f(\mathbf{a}; s - 2a_1) + f(\mathbf{a}_{-1}; s - a_1) + f(\mathbf{a}_{-1}; s) = \cdots \\ &= f(\mathbf{a}; s - a_1 x_1) + \sum_{j=0}^{x_1 - 1} f(\mathbf{a}_{-1}; s - j a_1). \end{aligned}$$

Now apply the recursion x_2 times with $i = 2$, and so on, and we get constants (independent of s) $u_{ij} \in \mathbb{Z}_{\geq 0}$ such that

$$f(\mathbf{a}; s) = f(\mathbf{a}; s - q) + \sum_{i=1}^{n} \sum_{j=0}^{x_i - 1} f(\mathbf{a}_{-i}; s - u_{ij}).$$

Now if we do the same thing for $f(\mathbf{a}; s+1)$, applying the recursion y_1 times with $i = 1$ and so forth, we get constants $w_{ij} \in \mathbb{Z}_{\geq 0}$ such that

$$f(\mathbf{a}; s+1) = f\big(\mathbf{a}; s + 1 - (q+1)\big) + \sum_{i=1}^{n} \sum_{j=0}^{y_i - 1} f(\mathbf{a}_{-i}; s + 1 - w_{ij}).$$

Subtracting the two equations, the term $f(\mathbf{a}; s - q) = f\big(\mathbf{a}; s + 1 - (q+1)\big)$ cancels, and we are left with

$$f(\mathbf{a}; s+1) - f(\mathbf{a}; s) = \sum_{i=1}^{n} \sum_{j=0}^{y_i - 1} f(\mathbf{a}_{-i}; s + 1 - w_{ij}) - \sum_{i=1}^{n} \sum_{j=0}^{x_i - 1} f(\mathbf{a}_{-i}; s - u_{ij}),$$

and we want to show that this quantity is (eventually) positive. By Proposition 1.6, $f(\mathbf{a}_{-i}; s)$ is a quasi-polynomial with leading term

$$\frac{1}{(n-2)! \prod_{j \neq i} a_j} s^{n-2}.$$

Therefore $f(\mathbf{a}; s+1) - f(\mathbf{a}; s)$ is a quasi-polynomial with leading coefficient (on s^{n-2})

$$\begin{aligned}
&\sum_{i=1}^{n} \sum_{j=0}^{y_i - 1} \frac{1}{(n-2)! \prod_{j \neq i} a_j} - \sum_{i=1}^{n} \sum_{j=0}^{x_i - 1} \frac{1}{(n-2)! \prod_{j \neq i} a_j} \\
&\quad = \sum_{i=1}^{n} \frac{a_i y_i}{(n-2)! a_1 \cdots a_n} - \sum_{i=1}^{n} \frac{a_i x_i}{(n-2)! a_1 \cdots a_n} \\
&\quad = \frac{1}{(n-2)! a_1 \cdots a_n} \left[\sum_{i=1}^{n} a_i y_i - \sum_{i=1}^{n} a_i x_i \right] \\
&\quad = \frac{1}{(n-2)! a_1 \cdots a_n} \big((q+1) - q \big) \\
&\quad = \frac{1}{(n-2)! a_1 \cdots a_n}.
\end{aligned}$$

Since this is a positive leading term, $f(\mathbf{a}; s+1) - f(\mathbf{a}; s)$ will eventually be positive, as desired.

$\square$

Proof of Theorem 1.12. Let s be sufficiently large. By Theorem 1.8, the set of t with $f(t) = f(sp)$ is exactly

$$\left\{ sp + \sum_i a_i b_i : \ 0 \le b_i < d_i \right\}.$$

The largest element of this set occurs at $b_i = d_i - 1$ for all i, so

$$g_{=f(sp)} = sp + \sum_{i=1}^{n} (d_i - 1) a_i.$$

The smallest element of this set occurs at $b_i = 0$ for all i, so

$$h_{=f(sp)} = sp.$$

The number of elements in this set is

$$c_{=f(sp)} = d_1 \cdots d_n = p.$$

The sum of the elements in this set is

$$\begin{aligned} s_{=f(sp)} &= \sum_{b_1=0}^{d_1-1} \cdots \sum_{b_n=0}^{d_n-1} \left(sp + \sum_{i=1}^{n} a_i b_i \right) \\ &= d_1 \cdots d_n sp + \sum_{i=1}^{n} \left(\prod_{j \ne i} d_j \cdot \sum_{b_i=0}^{d_i-1} a_i b_i \right) \\ &= sp^2 + \sum_{i=1}^{n} \left(\prod_{j \ne i} d_j \cdot \frac{a_i d_i (d_i - 1)}{2} \right) \\ &= sp^2 + \sum_{i=1}^{n} \frac{p a_i (d_i - 1)}{2}. \end{aligned}$$

The generating function for this set is

$$\begin{aligned} F_{=f(sp)}(x) &= \sum_{b_1=0}^{d_1-1} \cdots \sum_{b_n=0}^{d_n-1} x^{sp + \sum_{i=1}^{n} a_i b_i} \\ &= x^{sp} \prod_i \left(1 + x^{a_i} + \cdots + x^{(d_i-1)a_i} \right) \\ &= x^{sp} \prod_i \frac{1 - x^{d_i a_i}}{1 - x^{a_i}}. \end{aligned}$$

Since $f(sp)$ is an increasing function of s (for sufficiently large s), we have that $g_{\le f(sp)} = g_{=f(sp)}$ and $h_{\ge f(sp)} = h_{=f(sp)}$. To compute $c_{\le f(sp)}$, we must compute

$$\sum_{k=0}^{f(sp)} c_{=k}.$$

The values of $c_{=k}$ may disagree with our above formula (which is only valid for sufficiently large k) for a fixed set of k, but this can only change the sum by a constant amount, so

$$c_{\leq f(sp)} = C_1' + \sum_{r=0}^{s} c_{=f(rp)} = sp + C_1,$$

where C_1' and C_1 are constants. Similarly, we may compute

$$\begin{aligned} s_{\leq f(sp)} &= C_2' + \sum_{r=0}^{s} \left(rp^2 + \sum_{i=1}^{n} \frac{pa_i(d_i-1)}{2} \right) \\ &= C_2' + \frac{s^2p^2 + sp^2}{2} + (s+1)\sum_{i=1}^{n} \frac{pa_i(d_i-1)}{2} \\ &= \frac{1}{2}(sp)^2 + \left(\frac{p + \sum_{i=1}^{n} a_i(d_i-1)}{2} \right) sp + C_2, \end{aligned}$$

where C_2' and C_2 are constants. Finally,

$$\begin{aligned} F_{\geq f(sp)}(x) &= \sum_{r=s}^{\infty} F_{=f(rp)}(x) \\ &= \sum_{r=s}^{\infty} x^{rp} \prod_i \frac{1-x^{d_i a_i}}{1-x^{a_i}} \\ &= \frac{x^{sp}}{1-x^p} \prod_i \frac{1-x^{d_i a_i}}{1-x^{a_i}}. \end{aligned}$$

□

Proof of Proposition 1.16. Note that the d_i as defined in the proposition are indeed $d_i = \gcd(\mathbf{a}_{-i})$, as required to apply Theorem 1.12. Let $t = \sum_{i=1}^{n} a_i x_i$, for some $x_i \in \mathbb{Z}_{\geq 0}$, be any number with at least one representation by $\mathbf{a}$. Letting $b_i = x_i \bmod d_i$ (so $0 \leq b_i < d_i$), and, noting that $a_i d_i = p$, we get that there exists $s \in \mathbb{Z}_{\geq 0}$ such that

$$t = sp + \sum_i a_i b_i.$$

In particular, $f(t) = f(sp)$ with $s \geq 0$. and so such a t will be counted when we look at $g_{=f(sp)}$. Note that t such that $f(t) = 0$ will *not* be counted; such t will correspond to negative s.

So let $s \in \mathbb{Z}_{\geq 0}$ be given, and let $k = \binom{s+n-1}{n-1}$. We have (in the notation of Theorem 1.8(3))

$$a_i' = \frac{a_i}{\prod_{j \neq i} d_i} = 1,$$

for all i. Then by Theorem 1.8(3),

$$f(\mathbf{a}; sp) = f(\mathbf{a}'; s) = f\big((1, \ldots, 1); s\big) = \binom{s+n-1}{n-1} = k$$

(this calculation is a classical combinatorics problem about compositions). Now we may simply apply Theorem 1.12 and using that $p = a_i d_i$:

$$\begin{aligned}
g_{=f(sp)} = g_{\leq f(sp)} &= sp + \sum_{i=1}^{n} (d_i - 1) a_i \\
&= sp + \sum_{i=1}^{n} (p - a_i) \\
&= (s+n)p - \sigma, \\
h_{=f(sp)} = h_{\geq f(sp)} &= sp, \\
c_{=f(sp)} &= p, \\
s_{=f(sp)} &= sp^2 + \sum_{i=1}^{n} \frac{p a_i (d_i - 1)}{2} \\
&= sp^2 + \sum_{i=1}^{n} \frac{p^2 - p a_i}{2} \\
&= \frac{2sp^2}{2} + \frac{np^2 - p\sigma}{2} \\
&= \frac{p\big((2s+n)p - \sigma\big)}{2}, \\
F_{=f(sp)}(x) &= x^{sp} \prod_i \frac{1 - x^{d_i a_i}}{1 - x^{a_i}} \\
&= \frac{x^{sp} \left(1 - x^p\right)^n}{\left(1 - x^{a_1}\right) \cdots \left(1 - x^{a_n}\right)}, \\
F_{\geq f(sp)}(x) &= \frac{x^{sp}}{1 - x^p} \prod_i \frac{1 - x^{d_i a_i}}{1 - x^{a_i}} \\
&= \frac{x^{sp} \left(1 - x^p\right)^n}{\left(1 - x^p\right)\left(1 - x^{a_1}\right) \cdots \left(1 - x^{a_n}\right)} \\
&= \frac{x^{sp} \left(1 - x^p\right)^{n-1}}{\left(1 - x^{a_1}\right) \cdots \left(1 - x^{a_n}\right)}.
\end{aligned}$$

Finally, using that $c_{=0} = \frac{(n-1)p-\sigma+1}{2}$ from Tripathi [19],

$$\begin{aligned}
c_{\le k} &= \sum_{j=0}^{k} c_{=j} \\
&= c_{=0} + \sum_{r=0}^{s} c_{=\binom{r+n-1}{n-1}} \\
&= \frac{(n-1)p-\sigma+1}{2} + \sum_{r=0}^{s} p \\
&= (s+1)p + \frac{(n-1)p-\sigma+1}{2}.
\end{aligned}$$

□

Proof of Proposition 1.19. We will be brief, since much of this is classical; see Wilf's text [20, Section 3.15], for example. Define $G(x) = \sum_{t=0}^{\infty} f(\mathbf{a};t)x^t$. We see that

$$G(x) = (1 + x^{a_1} + x^{2a_1} + \cdots)\cdots(1 + x^{a_n} + x^{2a_n} + \cdots) = \frac{1}{\prod_i (1 - x^{a_i})}.$$

All of the poles of G are mth roots of unity, where $m = \operatorname{lcm}(\mathbf{a})$. One pole is $x = 1$, of order n. Label the other roots of unity by ζ_j, for $1 \le j < m$, and suppose ζ_j is a pole of order b_j. Then the partial fraction expansion of $G(x)$ yields that there exist $C_\ell, D_{j\ell} \in \mathbb{Q}$ such that

$$G(x) = \sum_{\ell=1}^{n} \frac{C_\ell}{(1-x)^\ell} + \sum_{j=1}^{m-1}\sum_{\ell=1}^{b_j} \frac{D_{j\ell}}{(1-x/\zeta_j)^\ell}.$$

Suppose ζ_j is a primitive rth root of unity. Then a term $\frac{D_{j\ell}}{(1-x/\zeta_j)^\ell}$, if expanded out as a product of geometric series, contributes a degree $\ell - 1$ quasi-polynomial of period r to $f(t)$. Summed together, we will have a period m quasi-polynomial. We can see that ζ_j is a root of exactly those $1 - x^{a_i}$ such that r divides a_i; therefore, it will be a pole of order $b_j = |i : \ r \text{ divides } a_i|$.

Since $\gcd(\mathbf{a}) = 1$, we must have $b_j \le n-1$, and so the only degree $n-1$ piece will come from

$$C_n/(1-x)^n = \sum_{t=0}^{\infty} C_n \binom{t+n-1}{n-1} x^t$$

(the tth coefficient in the power series will be the number of ways to write $t = c_1 + \cdots + c_n$ with $c_i \in \mathbb{Z}_{\ge 0}$, again a classical combinatorics problem).

Furthermore, if $d_i = 1$ for all i, then no $r > 1$ can divide $n-1$ of the a_i, and so $b_j \le n-2$, and the only degree $n-1$ and $n-2$ pieces will come from

$$C_n/(1-x)^n + C_{n-1}/(1-x)^{n-1} = \sum_{t=0}^{\infty} \left(C_n \binom{t+n-1}{n-1} + C_{n-1}\binom{t+n-2}{n-2} \right) x^t.$$

Noting that

$$C_n = (1-x)^n G(x)\Big|_{x=1} \quad \text{and} \quad C_{n-1} = \frac{d}{dx}(1-x)^n G(x)\Big|_{x=1},$$

we compute that

$$C_n = \frac{1}{a_1 \cdots a_n} \quad \text{and} \quad C_{n-1} = \frac{a_1 + \cdots + a_n - n}{2a_1 \cdots a_n},$$

and we can compute that

$$\begin{aligned} &C_n \binom{t+n-1}{n-1} + C_{n-1}\binom{t+n-2}{n-2} \\ &= \frac{1}{(n-1)!a_1 \cdots a_n} t^{n-1} + \frac{a_1 + \cdots + a_n}{2(n-2)!a_1 \cdots a_n} t^{n-2} + \text{ lower order terms.} \end{aligned}$$

This gives the first leading term of $f(t)$, in general, and the first two leading terms when $d_i = 1$ for all i, and so Parts (1) and (2) are proved.

To prove Part (3), Theorem1.12(3) allows us to assume without loss of generality that $d_i = 1$ for all i, and we want to prove that $f(s+1) > f(s)$ for sufficiently large s. Indeed, the leading term of $f(s+1) - f(s)$, when expanded out as a quasi-polynomial using Part (2), is

$$\frac{1}{(n-2)!a_1 \cdots a_n} s^{n-2}.$$

Since this is a positive leading term, $f(s+1) - f(s)$ must eventually be positive, as desired. □

3 Open Questions

Question 3.1. We have made no effort to quantify what *sufficiently large* means in any of these theorems, but probably one can, since $f(t)$ is so "well-behaved" here. What bounds can we give for when the results hold?

Question 3.2. The $n = 2$ case is well understood (see Proposition 1.15), and finding formulas for $n \geq 4$ seems very difficult even in the $k = 0$ case. It seems possible that there are interesting formulas when $n = 3$, however. For example, when $n = 3$ and $k = 0$, there are reasonable formulas (see Ramírez Alfonsín [15, Chapter 2], and, for a generating function approach, see Denham [10]). Are there interesting formulas for $n = 3$ and general k?

Question 3.3. Let $P \subseteq \mathbb{R}^n$ be a d-dimensional polytope whose vertices are rational, and let m be the smallest integer such that the vertices of mP (P dilated by a factor of m) are integers. Then Ehrhart [11] proves that $f(t) = |tP \cap \mathbb{Z}^n|$ is a quasi-polynomial of period m (see the Beck and Robins text [8] for many more details). This is a generalization of our problem, as taking P to be the convex hull of $\mathbf{e}_i/a_i$ ($1 \leq i \leq n$), where $\mathbf{e}_i$ is ith standard basis vector, yields the Frobenius $f(t)$. One can define $g_{\leq k}$, and so forth, using this f, and Aliev, De Loera, and Louveaux [1] study structural and algorithmic results related to this. Do some of the results of this current paper generalize to that more general setting?

Question 3.4. What can we say about the computational complexity of computing $g_{\leq k}$, $c_{\leq k}$, and so forth? If n is not fixed, then Ramírez Alfonsín [14] shows that even computing $g_{=0}$ is NP-hard. On the other hand, if n is fixed, then Kannan [13] shows that $g_{=0}$ can be computed in polynomial time, and Barvinok and Woods [4] show that $c_{=0}$ and other quantities can be computed in polynomial time. Generalizing, Aliev, De Loera, and Louveaux [1] show that, for fixed n and k, $g_{\leq k}$ and other quantities can be computed in polynomial time.

This leaves the open question: Can these quantities be computed in polynomial time if n is fixed, but $a_1, \ldots, a_n$ and k are the input? When k is sufficiently large, Theorem 1.12 applies: For any given t, we can compute $f(t)$ in polynomial time, using the result of Barvinok [5] that $|P \cap \mathbb{Z}^n|$ can be computed in polynomial time for fixed n; then binary search allows us to find s such that $f(sp) \leq k < f\big((s+1)p\big)$, and Theorem 1.12 gives us $g_{=k}$. But what if k is bigger than a constant but not "sufficiently large" for Theorem 1.12 to hold?

References

[1] Iskander Aliev, Jesús A. De Loera, and Quentin Louveaux. Parametric polyhedra with at least k lattice points: their semigroup structure and the k-Frobenius problem. In *Recent trends in combinatorics*, volume 159 of *IMA Vol. Math. Appl.*, pages 753–778. Springer, 2016.

[2] Iskander Aliev, Lenny Fukshansky, and Martin Henk. Generalized Frobenius numbers: bounds and average behavior. *Acta Arith.*, 155(1):53–62, 2012.

[3] Leonardo Bardomero and Matthias Beck. Frobenius coin-exchange generating functions. *Amer. Math. Monthly*, 127(4):308–315, 2020.

[4] Alexander Barvinok and Kevin Woods. Short rational generating functions for lattice point problems. *J. Amer. Math. Soc.*, 16(4):957–979, 2003.

[5] Alexander I. Barvinok. A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed. *Math. Oper. Res.*, 19(4):769–779, 1994.

[6] Matthias Beck and Curtis Kifer. An extreme family of generalized Frobenius numbers. *Integers*, 11:A24, 6, 2011.

[7] Matthias Beck and Sinai Robins. A formula related to the Frobenius problem in two dimensions. In *Number theory (New York Seminar 2003)*, pages 17–23. Springer, New York, 2004.

[8] Matthias Beck and Sinai Robins. *Computing the continuous discretely*. Undergraduate Texts in Mathematics. Springer, New York, 2007.

[9] Tom C. Brown and Peter Jau-Shyong Shiue. A remark related to the Frobenius problem. *Fibonacci Quart.*, 31(1):32–36, 1993.

[10] Graham Denham. Short generating functions for some semigroup algebras. *Electron. J. Combin.*, 10:R36, 2003.

[11] Eugene Ehrhart. Sur les polyedres homothetiques bordes a n dimensions. *Comptes Rendus Hebdomadaires des seances de l'academie des sciences*, 254(6):988, 1962.

[12] Lenny Fukshansky and Achill Schürmann. Bounds on generalized Frobenius numbers. *European J. Combin.*, 32(3):361–368, 2011.

[13] Ravi Kannan. Lattice translates of a polytope and the Frobenius problem. *Combinatorica*, 12(2):161–177, 1992.

[14] Jorge L. Ramírez Alfonsín. Complexity of the Frobenius problem. *Combinatorica*, 16(1):143–147, 1996.

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

[16] Jeffrey Shallit and James Stankewicz. Unbounded discrepancy in Frobenius numbers. *Integers*, 11:A2, 8, 2011.

[17] James J Sylvester. Mathematical questions with their solutions. *Educational times*, 41(21):171–178, 1884.

[18] Lázló A. Székely and Nicholas C. Wormald. Generating functions for the Frobenius problem with 2 and 3 generators. *Math. Chronicle*, 15:49–57, 1986.

[19] Amitabha Tripathi. On a linear Diophantine problem of Frobenius. *Integers*, 6:A14, 6, 2006.

[20] Herbert S. Wilf. *generatingfunctionology*. Academic Press, Inc., Boston, MA, second edition, 1994.