Extending the Linear Diophantine Problem of Frobenius

Curtis Kifer

Version of May 3, 2010

Contents

Chapter 1

Introduction

1.1 The coin exchange problem of Frobenius

According to Alfred Brauer (1894–1985) in his 1942 article [5], it was the German mathematician Ferdinand Georg Frobenius (1849–1917) who would mention occasionally in his lectures the problem of determining the largest integer that cannot be represented as a nonnegative, linear, integral combination of a set of positive, coprime integers. Brauer, a student of Isaac Shur who was a student of Georg Frobenius, was still seeking solutions to this 'problem of Frobenius' more than 10 years later in [6].

By 1972, there were a number of published papers looking into the Frobenius Problem [8], also known as 'the linear diophantine problem of Frobenius', or the 'coin exchange problem of Frobenius'. The last thirty years have seen a lot more research into the problem and its generalizations as witnessed by the 2005 book *The Diophantine Frobenius Problem* [1], the grand compilation of all things Frobenius Problem.

1.2 The Frobenius number is well defined

Given integer-valued relatively prime 'coins' $a_1, a_2, ..., a_k$, the Frobenius number is the largest integer n such that the linear diophantine equation $a_1m_1 + a_2m_2 + ... + a_km_k = n$ has no solution in non-negative integers $m_1, m_2, ..., m_k$. Following [3] we denote by $g(a_1, ..., a_k)$ the largest integer value not attainable by this coin system. That is to say that any integer x greater than the Frobenius number $g(a_1, ..., a_k)$ has a representation $x = a_1x_1+a_2x_2+...+a_kx_k$ by $a_1, a_2, ..., a_k$ for some non-negative integers $x_1, x_2, ..., x_k$. We say x is representable by $a_1, a_2, ..., a_k$.

While it is obvious that there are representable positive integers and non-representable positive integers, must there be a largest non-representable integer? Maybe there are indefintely large non-representable integers for $a_1, a_2, ..., a_k$ with gcd $(a_1, a_2, ..., a_k) = 1$. This notion of whether or not the Frobenius number is well-defined will be the first bit of mathematics we look at in this paper.

Proposition 1.1. *The Frobenius number $g(a_1, ..., a_k)$ is well-defined.*

Proof. Given $a_1, a_2, ..., a_k$ with $\gcd(a_1, a_2, ..., a_k) = 1$, the extended Euclidean algorithm gives that there exist $m_1, m_2, ..., m_k \in \mathbb{Z}$ such that

$$a_1m_1 + a_2m_2 + ... + a_km_k = 1.$$

It follows that we can group the negative terms on the left while grouping the terms that are positive or zero on the right to get

$$a_{k_1}m_{k_1} + a_{k_2}m_{k_2} + ... + a_{k_\alpha}m_{k_\alpha} + a_{k_{\alpha+1}}m_{k_{\alpha+1}} + ... + a_{k_{\alpha+\beta}}m_{k_{\alpha+\beta}} = 1,$$

where $k_1, k_2, ..., k_\alpha$ index the negative coefficients and $k_{\alpha+1}, ..., k_{\alpha+\beta}$ index everything else. Now let

$$x = -(a_{k_1} - 1)(a_{k_1}m_{k_1} + a_{k_2}m_{k_2} + ... + a_{k_\alpha}m_{k_\alpha})$$

and note that x is representable. The above equation equal to one can be added to x yielding a representation of $x + 1$. We can repeat this process $a_{k_1} - 1$ times, producing the list $x, x+1, x+2, ..., x+a_{k_1}-1$. To continue the sequence, we next add a_{k_1} yielding $x + a_{k_1}$ then continue adding ones as before. So we see that every integer greater than or equal to x is representable. □

The Frobenius Problem is in general a two-fold problem: not only do we seek the largest non-representable integer, $g(a_1, ..., a_k)$, but we also want to know how many non-representable integers there are. We denote this quantity by $n(a_1, a_2, ..., a_k)$. In this paper, and in many articles on the subject, authors generally seek insight into both $g(a_1, ..., a_k)$ and $n(a_1, a_2, ..., a_k)$.

1.3 Amitabha Tripathi's results

In Chapter 5, we will see that the main theorem in this paper is an extension of one of two theorems in the 2006 article by Amitabha Tripathi [15] where he, among other things, exploits work by S.M. Johnson in 1960; A. Brauer, J.E. Shockley in 1962; E.S. Selmer in 1977, and O.J. Rödseth in 1978 [4, 11, 9, 10] to prove an explicit closed formula for the Frobenius Number when the 'coins' are constructed in a prescribed manner.

Tripathi begins the paper with two lemmas: the first lemma is in two parts; the first part follows [4]. The second part is due to [11]

Lemma 1.2. *Let $A = \{a_1, a_2, ..., a_k\}$ be a set of positive integers with $\gcd(a_1, a_2, ..., a_k) = 1$ and for each $j \in \{1, ..., a_1-1\}$ let n_j denote the least positive integer congruent to $j \pmod{a_1}$ that is representable by A. Then*

(a) $g(a_1, a_2, ..., a_k) = \max\limits_{1 \le j \le a_1-1} n_j - a_1.$

(b) $n(a_1, a_2, ..., a_k) = \dfrac{1}{a_1}\sum\limits_{j=1}^{a_1-1}(n_j - j) = \dfrac{1}{a_1}\sum\limits_{j=1}^{a_1-1} n_j - \dfrac{a_1-1}{2}.$

In the second lemma the coins are constructed so that all but one have a common divisor. This idea stems from the work in [9]. Then, [10] uses [9] and Lemma 1.2 to prove the following.

Lemma 1.3. *Let* $A = \{a_1, a_2, ..., a_k\}$ *be a set of positive integers with* $\gcd(a_1, a_2, ..., a_k) = 1$*. If* $\gcd(a_2, a_3, ..., a_k) = d$*, let* $a_j = d \cdot a'_j$ *for each* $j \in \{2, ..., k\}$*. Then*

(a) $g(a_1, a_2, ..., a_k) = d \cdot g(a_1, a'_2, a'_3, ..., a'_k) + a_1(d-1)$*.*

(b) $n(a_1, a_2, ..., a_k) = d \cdot n(a_1, a'_2, a'_3, ..., a'_k) + \frac{1}{2}(a_1 - 1)(d-1)$*.*

Now the relevant theorem from Tripathi's paper [15].

Theorem 1.4. *Let* $a_1, a_2, ..., a_k$ *be pairwise coprime positive integers, and for* $i \in \{1, 2, ..., k\}$*, let* $A_i = \frac{a_1 a_2 \cdots a_k}{a_i}$*. Then*

$$g(A_1, A_2, ..., A_k) = (k-1)a_1 a_2 \cdots a_k - (A_1 + A_2 + ... + A_k).$$

1.4 Goal of this paper

The main goal of this paper is to extend Theorem 1.4 to find the largest integer that is s-representable; we will make this definition precise in Chapter 3.

Tripathi's Theorem 1.4 is a corollary to the main theorem of this paper. As already mentioned, Tripathi's Theorem 1.4 used Lemmas 1.2 and 1.3 in its proof. This paper will extend those lemmas to include s-representable integers, so that they, too, can be viewed as corollaries to these results.

Chapter 2

The two-coin problem

Proposition 1.1 assured us what we already knew: the Frobenius number $g(a_1, ..., a_k)$ is well defined. Now let's see if we can find it in the simplest case. Below, we will prove the following classical results:

- *Two-coin Theorem:* For relatively prime positive integers a and b, $g(a, b) = ab - a - b$.
- *Sylvester's Theorem:* For relatively prime positive integers a and b, exactly half of the integers between 1 and $(a-1)(b-1)$ are representable by a and b.

So yes, we can find the Frobenius number, even if only with two coins; moreover, we know exactly how many non-representable integers there are. Alfonsin shows four proofs of the Two-coin Theorem in [1]; Beck–Robins show another in [3]. There may be as-yet undiscovered ways to prove these two theorems. We will provide novel proofs of both these theorems below. The origins of the Two-coin Theorem are lost in history. Quoting from [3]:

> [The two-coin Theorem] is one of the famous folklore results and might be one of the most misquoted theorems in all of mathematics. People usually cite James J. Sylvester's problem in [14], but his paper contains [Sylvester's theorem] rather than [the Two-coin Theorem]. In fact, Sylvester's problem had previously appeared as a theorem in [13]. It is not known who first discovered or proved The two-coin Theorem. It is very conceivable that Sylvester knew about it when he came up with [Sylvester's theorem].

2.1 The Frobenius number for two coins

We begin with a lemma.

Lemma 2.1. *For positive integers a, b with* $\gcd(a, b) = 1$*, then* $0b, 1b, 2b, 3b, ..., (a-1)b$ *form a complete set of residues modulo a.*

Proof. For $i \neq j$ and $i, j \in \{0, 1, 2, ..., a-1\}$, note that

$$\begin{aligned} ib \equiv jb \pmod{a} &\Rightarrow a \mid ib - jb \\ &\Rightarrow a \mid b(i-j) \\ &\Rightarrow a \mid (i-j) \text{ since } \gcd(a, b) = 1 \\ &\Rightarrow i \equiv j \pmod{a}, \end{aligned}$$

which is impossible since $i \neq j$ and $i, j \in \{0, 1, 2, ..., a-1\}$. Thus $0b, 1b, 2b, 3b, ..., (a-1)b$ form a complete set of residues modulo a since the set is composed of a distinct integers modulo a. □

Now we prove the celebrated two-coined theorem of Calavaras County.

Theorem 2.2 (The two-coin Theorem)**.** *For positive integers a, b with* $\gcd(a, b) = 1$*, then* $g(a, b) = ab - b - a$.

Proof. The proof is made easier by assuming (without loss of generality) that $a < b$. To prove the theorem, we'll first show that everything from $(a-1)b$ on is representable, then move backwards down the number line so that the first integer arrived at that is not representable by a and b will be $g(a, b)$.
Claim: For any integer n such that $n > (a-1)b$, n is representable by a and b.
Proof of Claim: Given $n > (a-1)b$, Lemma 2.1 implies that exactly one of $0b, 1b, 2b, 3b, ..., (a-1)b$ is congruent to $n \pmod{a}$; say $tb \equiv n \pmod{a}$ where $t \in \{0, 1, 2, ..., a-1\}$. Note that $tb \leq (a-1)b < n$ since $t \in 0, 1, 2, ..., a-1$. Next, note that adding any multiple of a to an integer that is congruent to n modulo a, will result in another integer congruent to n modulo a. Since $tb < n$ and $tb \equiv n \pmod{a}$, then n equals tb plus some multiple of a. So add the requisite number of multiples of a to tb to realize a representation of n by a and b, say $tb + ua = n$, so the claim is proven.

It has been shown that every integer greater than $(a-1)b = ab - b$ is representable by a and b, so now let's count backwards from $ab - b$ and see who is representable and who is not representable.

Each of $ab - b$, $ab - b - 1$, $ab - b - 2$, $\ldots$, $ab - b - (a-1)$ is distinct modulo a since a consecutive integers are always distinct modulo a. Thus for each $v \in \{0, 1, 2, ..., a-1\}$, $\exists\, w \in \{0, 1, 2, ..., a-1\}$ such that $ab - b - v \equiv wb \pmod{a}$, by Lemma 2.1. Now note that because $[a < b] \Rightarrow [ab - 2b < ab - b - (a-1)]$ then each of $0b, 1b, 2b, 3b, ..., (a-2)b = ab - 2b$ is less than each of $(a-1)b = ab - b$, $ab - b - 1$, $ab - b - 2$, $\ldots$, $ab - b - (a-1)$. Thus, since $wb \equiv ab - b - v \pmod{a}$ and $wb < ab - b - v$, then $ab - b - v$ equals wb plus some multiple of a. So add the requisite number of multiples of a to wb to realize a representation of $ab - b - v$ by a and b, say $wb + xa = ab - b - v$.

It has been shown that every integer greater than or equal to $ab - b - (a-1)$ is representable by a and b. We now arrive at the first integer not representable by a and b which is $ab - b - a$. To see why this is so, suppose that $ab - b - a$ is representable by a and b: so for some $p, q \in \mathbb{N}$, $ab - b - a = pa + qb$. Such a representation demands that $ab - b - a$ is either

1. a multiple of a, or

2. a multiple of b, or

3. a multiple of b plus a multiple of a.

The first two cases will never happen since $ab - b - a = b(a-1) - a$ shows that $ab - b - a$ is not a multiple of b, while $ab - b - a = a(b-1) - b$ shows that $ab - b - a$ is not a multiple of a. So the assumption is that $ab - b - a = pa + qb$ is a multiple of b plus a multiple of a. We will now see that this can't happen since

$$\begin{aligned} & ab - b - a = pa + qb \text{ for positive } p, q \\ \Rightarrow \quad & qb \equiv ab - b - a \pmod{a} \text{ and } qb < ab - b - a, \end{aligned}$$

however $0b, 1b, 2b, 3b, ..., (a-2)b$ are the only multiples of b that are less than $ab - b - a$, and none are congruent modulo a to $ab - b - a = (a-1)b - a \equiv (a-1)b \pmod{a}$, so no such qb can exist. □

2.2 Sylvester's Theorem

Sylvester requires us to see the following counting lemma.

Lemma 2.3. *Let* $\gcd(a, b) = 1$ *and let* $\lfloor x \rfloor$ *be the greatest integer function, then*

$$\sum_{i=1}^{a-1} \left\lfloor \frac{ib}{a} \right\rfloor = \frac{1}{2}(a-1)(b-1).$$

Proof. Call a lattice point in $\mathbb{R}^2$ 'positive-valued' if both its coordinates are positive-valued. Consider counting positive-valued lattice points beneath the line $y = \frac{b}{a}x$ between $x = 1$ and $x = a - 1$:

- When $x = 1$ then $y = \frac{b}{a}$ so there are $\lfloor \frac{b}{a} \rfloor$ positive-valued lattice points beneath the line at $x = 1$
- When $x = 2$ then $y = 2\frac{b}{a}$ so there are $\lfloor 2\frac{b}{a} \rfloor$ positive-valued lattice points beneath the line at $x = 2$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

- When $x = a - 1$ then $y = (a-1)\frac{b}{a}$ so there are $\left\lfloor \frac{(a-1)b}{a} \right\rfloor$ positive-valued lattice points beneath the line at $x = a - 1$

so the number of positive-valued lattice points beneath the line $y = \frac{b}{a}x$ between $x = 1$ and $x = a - 1$ is

$$\sum_{i=1}^{a-1} \left\lfloor \frac{ib}{a} \right\rfloor .$$

Next, let's think geometrically about counting those same lattice points: cut from the plane the rectangle determined by the line $y = \frac{b}{a}x$ from the point $(0, 0)$ to (a, b) – this rectangle is a units wide and b units high – and note that the positive-valued lattice points beneath the line $y = \frac{b}{a}x$ between $x = 1$ and $x = a - 1$ are all contained in this cut-out rectangle; also, the line $y = \frac{b}{a}x$ cuts this rectangle, corner-to-corner, evenly in two.

Now let's trim this a-by-b rectangle evenly around the edges so that it is now $a - 2$ units wide and $b - 2$ units high – the rectangle has been trimmed symmetrically so that the line still cuts this rectangle evenly in half. Now we have an $(a-2)$-by-$(b-2)$ rectangle containing $(a-1)(b-1)$ lattice points that is cut evenly in half by the line $y = \frac{b}{a}x$. Note that the $\sum_{i=1}^{a-1} \left\lfloor \frac{ib}{a} \right\rfloor$ positive-valued lattice points beneath the line are all contained in this rectangle and are the only lattice points remaining beneath the line. Note also that $\gcd(a, b) = 1$ implies that none of the lattice points in this rectangle lie on the line since x would need be a multiple of a in order for $y = \frac{b}{a}x$ to be an integer, but x is at most $a - 1$ in this rectangle.

Since the rectangle contains $(a-1)(b-1)$ lattice points, and the line divides the rectangle evenly in two, and no lattice points lie directly on the line, then the number of lattice points lying beneath the line in this rectangle is $\frac{1}{2}(a-1)(b-1)$. □

Theorem 2.4. *For positive integers a, b with $\gcd(a, b) = 1$, there are exactly $\frac{1}{2}(a-1)(b-1)$ integers not representable by a and b.*

Proof. Theorem 2.2 showed that all integers greater than $ab - b - a$ are representable by a and b, so we must sort out who is representable and who is not representable only for integers in the interval $[1, ab - b - a]$.

Claim: For each $k \in \{1, 2, ..., a-1\}$, $\exists$ t_k such that every member of the list of non-negative integers $ab - kb - a$, $ab - kb - 2a$,..., $ab - kb - t_k a$ is not representable by a and b, where t_k is maximal so that we stay non-negative.

Proof of Claim: Suppose not: so for some $k \in \{1, 2, ..., a-1\}$, $\exists x, y \in \mathbb{N}$, $\exists q \in \{1, 2, ..., t_k\}$ such that $xa + yb = ab - kb - qa$. Now,

$$\begin{aligned} & xa + yb = ab - kb - qa \\ \Rightarrow \quad & yb = (a-k)b - (q+x)a, \end{aligned}$$

which implies

1. $yb < (a-k)b$, so y is equal to exactly one of $0, 1, 2, ..., a-k-1$, and
2. $yb \equiv (a-k)b \pmod{a}$.

However none of $0, 1, 2, ..., a-k-1$ are congruent modulo a to $a-k$ thus no such $y \in \mathbb{Z}_{\geq 0}$, $q \in \{1, 2, ..., t\}$ can exist such that $xa + yb = ab - kb - qa$ so the claim is proven, though the size of t_k still needs to be determined.

To determine the magnitude of t_k in $ab-kb-a$, $ab-kb-2a$,..., $ab-kb-t_k a$, we ask how big can t_k get so that $ab-kb-t_k a$ remains non-negative? Note that $ab-kb-t_k a = (a-k)b-t_k a$ so we want to subtract the maximal multiple of a from $(a-k)b$ and still have a non-negative integer remaining. The question is then, how many a fit into $(a-k)b$? This is the non-negative integer $\left\lfloor \frac{(a-k)b}{a} \right\rfloor$. Thus for each $k \in \{1, 2, ..., a-1\}$ the list of non-representable integers $ab-kb-a$, $ab-kb-2a$,..., $ab-kb-t_k a$ has $\left\lfloor \frac{(a-k)b}{a} \right\rfloor$ members. Thus the number of non-representable integers is at least

$$\begin{aligned}
&\left\lfloor \frac{(a-1)b}{a} \right\rfloor + \left\lfloor \frac{(a-2)b}{a} \right\rfloor + ... + \left\lfloor \frac{(a-(a-1))b}{a} \right\rfloor \\
= \ & \left\lfloor \frac{b}{a} \right\rfloor + \left\lfloor \frac{2b}{a} \right\rfloor + ... + \left\lfloor \frac{(a-1)b}{a} \right\rfloor \\
= \ & \sum_{i=1}^{a-1} \left\lfloor \frac{ib}{a} \right\rfloor \\
= \ & \frac{1}{2}(a-1)(b-1) \text{ by Lemma 2.1.}
\end{aligned}$$

To see that there are no more non-representable integers, note that we have looked at all non-representable integers congruent modulo a to $(a-1)b, (a-2)b, ..., (a-(a-1))b = 1b, 2b, ..., (a-1)b$ since we looked at all non-representable integers equal to $ab-kb-qa = (a-k)b-qa \equiv (a-k)b \pmod{a}$ for each $k \in \{1,2,...,a-1\}$, and for each $q \in \{1,2,...,t_k\}$ (where t_k is maximal). That is to say we have looked at all the non-representable non-negative integers that are less than or equal to $ab-b-a$ since every non-representable non-negative integer need be congruent modulo a to one of $1b, 2b, ..., (a-1)b$ by Lemma 2.1. □

2.3 More coins

For k greater than two coins, the Frobenius problem becomes way more difficult! Quoting Beck–Robins in [3]:

> ...the Frobenius problem for $k \geq 3$ is much harder than the case $k = 2$ that we have discussed. Certainly beyond $k = 3$, the Frobenius problem is wide open, though much effort has been put into its study. The literature on the Frobenius problem is vast, and there is still much room for improvement. The interested reader might consult the comprehensive monograph [1], which surveys the references to almost all articles dealing with the Frobenius problem and gives about 40 open problems and conjectures related to the Frobenius problem.

Chapter 3

More than one representation

3.1 s-representable integers

Now we ask how many representations a nonnegative integer has. For this we next define a partition function. Let $A = \{a_1, a_2, ..., a_k\}$ be a set of positive integers and for any nonnegative integer n, denote by

$$p_A(n) := \#\{(m_1, m_2, ..., m_k) \in \mathbb{Z}^k : \text{all } m_j \geq 0,\ m_1a_1 + ... + m_ka_k = n\}$$

the number of partitions of n into parts of sizes $a_1, a_2, ..., a_k$. Note n is non-negative so anytime we speak of partitioning an integer, it is understood that the integer is non-negative.

We say that $p_A(n)$ is the number of representations of n by $A = \{a_1, a_2, ..., a_k\}$. When $p_A(n) = s$, we say that n is s-representable by $A = \{a_1, a_2, ..., a_k\}$, or just that n is s-representable when it is already understood that the parts of each partition are of sizes $a_1, a_2, ..., a_k$. When an integer n has at most s representations by A, we'll say n is $\leq s$-representable; less than s representations is $<s$-representable; when n has at least s representations, we'll say n is $\geq s$-representable; greater than s representations is $>s$-representable.

For $A = \{a_1, a_2, ..., a_k\}$ with $\gcd(a_1, a_2, ..., a_k) = 1$ and $s \in \mathbb{N}_{\geq 0}$, is there a largest s-representable integer? Theorem 2.2 showed us that for $s = 0$, the answer is 'yes'. Is the same true for $s \geq 1$? We will show that, in general, the answer is yes but we have to be careful with our terminology. We will show that there always exists a largest $<s$-representable integer. Intuition dictates that this would be the largest $(s-1)$-representable integer. However, there exist some $s \in \mathbb{Z}_{>0}$ and some concoction of coin values $a_1, a_2, ..., a_k$ with $\gcd(a_1, ..., a_k) = 1$ for which there are no $(s-1)$-representable integers!

Definition 3.1. Let $\gcd(a_1, a_2, ..., a_k) = 1$.

(a) Denote by $g_s(a_1, a_2, ..., a_k)$ the greatest integer such that $p_A(g_s) < s$.

(b) Denote by $n_s(a_1, a_2, ..., a_k)$ the number of positive integers that are $<s$-representable by $A = \{a_1, a_2, ..., a_k\}$.

We need to show that these notions are well defined.

Proposition 3.1. *$g_s(a_1, a_2, ..., a_k)$ is well defined.*

Proof. We show that for each $s \in \mathbb{N}$ there exists an integer that is $\geq s$-representable and every integer greater than it is $\geq s$-representable.

For $A = \{a_1, a_2, ..., a_k\}$ and $\gcd(a_1, a_2, ..., a_k) = 1$, Euclid's algorithm asserts the existence of integers $m_1, m_2, ..., m_k$ such that $a_1 m_1 + ... + a_k m_k = 1$. Obviously not all the m_j are zero, and some are negative while some are positive. Let's rewrite this equation separating the negative terms from the non-negative terms by regrouping:

$$1 = (a_{k_1} m_{k_1} + a_{k_2} m_{k_2} + ... + a_{k_\alpha} m_{k_\alpha}) + (a_{k_{\alpha+1}} m_{k_{\alpha+1}} + ... + a_{k_{\alpha+\beta}} m_{k_{\alpha+\beta}}) \tag{3.1}$$

so that $1, 2, ..., \alpha$ index all the negative terms while $\alpha+1, ..., \alpha+\beta$ index all the non-negative terms.
Now let's play with (3.1):

$$\begin{aligned} 1 &= (a_{k_1} m_{k_1} + a_{k_2} m_{k_2} + ... + a_{k_\alpha} m_{k_\alpha}) + (a_{k_{\alpha+1}} m_{k_{\alpha+1}} + ... + a_{k_{\alpha+\beta}} m_{k_{\alpha+\beta}}) \\ 0 &= a_{k_1}(a_{k_1} m_{k_1} - 1) + ... + a_{k_\alpha}(a_{k_1} m_{k_\alpha}) + a_{k_{\alpha+1}}(a_{k_1} m_{k_{\alpha+1}}) + ... + a_{k_{\alpha+\beta}}(a_{k_1} m_{k_{\alpha+\beta}}). \end{aligned} \tag{3.2}$$

Let

$$\begin{aligned} x = -s \cdot (a_{k_1}(a_{k_1} m_{k_1} - 1) + ... + a_{k_\alpha}(a_{k_1} m_{k_\alpha})) \\ - (a_{k_1} - 1) \cdot (a_{k_1} m_{k_1} + a_{k_2} m_{k_2} + ... + a_{k_\alpha} m_{k_\alpha}) \end{aligned}$$

so x is composed of $-s$ factors of the negative terms from (3.2) plus $-(a_{k_1} - 1)$ factors of the negative terms from (3.1).

- Note that x is ≥ 1-representable.

- Next, note that x is $\geq s$-representable since (3.2) can be added to x without sending any of the terms of x to the negative, and this process can be repeated s times, each time yielding a new representation of x. Thus, x has been shown to be $\geq s$-representable.

- Similarly, (3.1) can be added to x without sending any of the terms of x to the negative, and this process can be repeated $a_{k_1} - 1$ times. To continue adding ones, add the $a_{k_1}^{\text{th}}$ one by merely adding a_{k_1}, then continue adding ones as before.

Clearly, one can keep being added indefinitely with each addition of a one resulting in an integer that is $\geq s$-representable. Thus x is $\geq s$-representable and every integer greater than x is $\geq s$-representable so the claim is proved. □

Now we are sure that $g_s(a_1, a_2, ..., a_k)$ is a well-defined object, so we can start discovering some things about it. Realize that the Frobenius number which we have already seen denoted $g(a_1, a_2, ..., a_k)$, can now be denoted by $g_1(a_1, a_2, ..., a_k)$ – the largest integer that is <1-representable. Also, anything we discover to be true concerning a generic 'largest s-representable integer', had better be true for our old friend, the Frobenius number.

3.2 Beck–Robins, 2003

In [2], Beck–Robins define s-representable integers and discover some things about s-representable integers under two coins.

We compare our definition of $g_s(a_1, ..., a_k)$ with that of Beck–Robins.

- Under Beck–Robins, the Frobenius number is denoted $g_0(a_1, ..., a_k)$ – the least integer beyond which every integer is represented more than 0 times.
  Under the definition we developed, the Frobenius number is denoted $g_1(a_1, ..., a_k)$. We think of it as the largest integer that is <1-representable.

- Under Beck–Robins, $g_s(a_1, ..., a_k)$ is the least integer beyond which every integer is represented more than s times. (This is the largest s-representable integer whenever it exists.)
  Under the definition we developed, $g_s(a_1, ..., a_k)$ is the largest integer that is $<s$-representable.

3.3 Brown et al, 2010

In [7], Brown et al show the first part of Lemma 4.1 of this paper to be a result of Brauer-Shockley in 1962 [4]. Brown et al define the greatest integer with exactly j representations and denote it $g_j(x_1, x_2, ..., x_n)$. The authors also show some results with two coins.

Also due to these authors, as observed by Shallit–Stankewicz [12] in their 2010 article:

> [Brown et al] observed that, for a fixed n-tuple $(x_1, x_2, ..., x_n)$, the function $g_j(x_1, x_2, ..., x_n)$ need not be increasing (considered as a function of j). For example, they gave the example $g_{35}(4, 7, 19) = 181$ while $g_{36}(4, 7, 19) = 180$. They asked if there are examples for which $g_1 < g_0$.

3.4 Shallit–Stankewicz, 2010

The 2010 article [12] by Jeffrey Shallit and James Stankewicz continues the research of Brown et al [12]. The authors adopt the notation used by Brown et al by denoting $g_j(x_1, x_2, ..., x_n)$ the greatest integer with exactly j representations.

> In this note, we show that the answer to the question of Brown et al is yes, even for [tuples whose coordinates x_i can be written as a non-negative integer linear combination of the others]. For example, it is easy to verify that $g_0(8, 9, 11, 14, 15) = 21$, while $g_1(8, 9, 11, 14, 15) = 20$. But we prove much more...

and they do! They show that for any $k > 0$, and $n = 5$, the quantity $g_0 - g_k$ is unbounded. They then provide examples with $g_0 > g_1$ for $n \geq 6$.

3.5 Our contribution

As stated in the introduction, the goal of this paper is to extend Theorem 1.4 to find the largest s-representable integer under the same conditions that Tripathi set up.

Our work will be shown to extend Lemma 1.2, Lemma 1.3, and Theorem 1.4.

The extension of the two-coin problem found by [2] and [7] is discovered in a novel way in the next section.

3.6 s-representable integers under two coins

We have seen that for $a, b \in \mathbb{Z}_{>0}$ and $\gcd(a, b) = 1$ then $g_1(a, b) = ab - b - a$. Next we will see that $g_s(a, b) = sab - b - a$.

Lemma 3.2. *Let $a, b \in \mathbb{Z}_{>0}$ and $\gcd(a, b) = 1$. Adding ab to a non-negative integer that is s-representable by a and b yields an $(s+1)$-representable integer; subtracting ab yields an $(s-1)$-representable integer. (We will assume that subtracting ab yields a non-negative integer.)*

Proof. Let m be a s-representable non-negative integer and rank its representations

$$\begin{aligned} m &= ax_1 + by_1 \\ &= ax_2 + by_2 \\ &\vdots \quad \vdots \\ &= ax_s + by_s \end{aligned}$$

so that $x_1 < x_2 < ... < x_s$ and $y_1 > y_2 > ... > y_s$. We can view the pairs (x_i, y_i) above as the s non-negative lattice points along the line $ax + by = m$ with slope $-\frac{a}{b}$ and y-intercept $\frac{m}{b}$. Since $\gcd(a, b) = 1$, results from elementary algebra and our ordering of the representations dictate that we 'rise' $-a$ and 'run' b to get from (x_i, y_i) to (x_{i+1}, y_{i+1}) so for $2 \leq i \leq s$

$$ax_i + by_i = a(x_1 + (i-1)b) + b(y_1 - (i-1)a).$$

Thus our ranked list of representations of m above looks like

$$\begin{aligned} m &= ax_1 + by_1 \\ &= a(x_1 + b) + b(y_1 - a) \\ &\vdots \qquad \vdots \qquad \vdots \\ &= a(x_1 + (s-1)b) + b(y_1 - (s-1)a). \end{aligned}$$

Now we add ab to m and so also to each of the representations above. To keep track of things, we'll make two lists of s representations each: we compose the first list of s representations by adding the ab into the first term of each representation of the above list; we compose the second list of s representations by adding the ab into the second term.

$$\begin{array}{rlrl}
 & \underline{\text{First List}} & & \underline{\text{Second List}} \\
 & a(x_1+b)+by_1 & & ax_1+b(y_1+a) \\
= & a(x_1+2b)+b(y_1-a) & = & a(x_1+b)+by_1 \\
= & a(x_1+3b)+b(y_1-2a) & = & a(x_1+2b)+b(y_1-a) \\
 & \vdots \qquad \vdots \qquad \vdots & & \vdots \qquad \vdots \qquad \vdots \\
= & a(x_1+(s-1)b)+b(y_1-(s-2)a) & = & a(x_1+(s-2)b)+b(y_1-(s-3)a) \\
= & a(x_1+sb)+b(y_1-(s-1)a). & = & a(x_1+(s-1)b)+b(y_1-(s-2)a).
\end{array}$$

Each list has s representations; however, representations 1 through $s-1$ of the first list exactly equal representations 2 through s of the second list. All in all, there are these $s-1$ representations, plus the last representation from the first list; plus the first representation of the second list. Thus $m+ab$ has $s+1$ representations,

$$\begin{aligned}
m+ab &= ax_1+b(y_1+a) \\
&= a(x_1+b)+by_1 \\
&= a(x_1+2b)+b(y_1-a) \\
& \quad \vdots \qquad \vdots \qquad \vdots \\
&= a(x_1+sb)+b(y_1-(s-1)a),
\end{aligned}$$

and it has been shown that adding ab to an s-representable integer yields an $(s+1)$-representable integer.

What if we had subtracted ab instead of adding it? We start with some s-representable integer n and rank its representations by increasing x_i and decreasing y_i

$$\begin{aligned}
n &= ax_1+by_1 \\
&= a(x_1+b)+b(y_1-a) \\
&= a(x_1+2b)+b(y_1-2a) \\
& \quad \vdots \qquad \vdots \qquad \vdots \\
&= a(x_1+(s-1)b)+b(y_1-(s-1)a).
\end{aligned}$$

We than subtract ab from the first term making a first list, and from the second term producing a second list, making two lists for the integer $n-ab$.

$$\begin{array}{rlrl}
 & \underline{\text{First List}} & & \underline{\text{Second List}} \\
 & a(x_1-b)+by_1 & & ax_1+b(y_1-a) \\
= & ax_1+b(y_1-a) & = & a(x_1+b)+b(y_1-2a) \\
= & a(x_1+b)+b(y_1-2a) & = & a(x_1+2b)+b(y_1-3a) \\
 & \vdots \qquad \vdots & & \vdots \qquad \vdots \\
= & a(x_1+(s-3)b)+b(y_1-(s-2)a) & = & a(x_1+(s-2)b)+b(y_1-(s-1)a) \\
= & a(x_1+(s-2)b)+b(y_1-(s-1)a). & = & a(x_1+(s-1)b)+b(y_1-sa).
\end{array}$$

- The second through the s^{th} representations of the first list exactly equal the first through the $(s-1)^{st}$ representations of the second list, so we thus far have $s-1$ representations of $n-ab$.

- The first 'representaion' of the first list is not a representation at all since if $x_1 - b$ were positive then the list of representations of n should have had $a(x_1 - b) + b(y_1 + a) = n$ as its first representation.

- The last item of the second list is not a representation of $n - ab$ since if $y_1 - sa$ were positive then the list of representations of n was missing the representation $a(x_1 + sb) + b(y_1 - sa) = n$.

- The three bulleted items above show that $n - ab$ is $(s-1)$-representable.

Now we know that subtracting ab from an s-representable integer yields an $(s-1)$-representable integer, and that this process can be repeated indefinitely so long as we deal only with non-negative integers. □

Theorem 3.3. *For positive integers a, b with* $\gcd(a,b) = 1$, *then* $g_s(a,b) = sab - b - a$.

Proof. We induct on s. The base case is Theorem 2.2. We assume the theorem is true for the first $s-1$ positive integers, so assume $g_{s-1}(a,b) = (s-1)ab - b - a$.

Claim: $sab - b - a$ is $<s$-representable.

Proof of Claim: Suppose not, so suppose $sab - b - a$ is $\geq s$-representable. But this is impossible since $(s-1)ab - b - a$ is $<(s-1)$-representable and adding ab to an integer that is $<(s-1)$-representable results in an integer that is $<s$-representable is a result of Lemma 3.2.

Claim: If $x > sab - b - a$ then x is $\geq s$-representable.

Proof of Claim: Assume not so assume that x is $<s$-representable. Lemma 3.2 gives that $x - ab$ is $<(s-1)$-representable. So we have that $x - ab > (s-1)ab - b - a$ and $s - ab$ is $<(s-1)$-representable, but this is a contradiction to the fact that $(s-1)ab - b - a$ is the largest integer that is $<(s-1)$-representable.

□

Chapter 4

Two propositions

On the way to generalizing Theorem 5.4 from Tripathi's article [15], we discovered extensions for the two lemmas due to [4] and [11]. Tripathi used these lemmas in one of his proofs of Theorem (1.4) in his article [15]. We will not use them in the proof of our main theorem, but include them here because they might be of independent interest.

Proposition 4.1. *Let* $A = \{a_1, a_2, ..., a_k\}$ *be a set of positive integers with* $\gcd(a_1, a_2, ..., a_k) = 1$ *and for each* $j \in \{0, 1, ..., a_1 - 1\}$ *let* $n_{j,s}$ *denote the least non-negative integer congruent to* $j \pmod{a_1}$ *such that* $p_A(n_{j,s}) \geq s$. *Then*

(a)
$$g_s(a_1, a_2, ..., a_k) = \max_{0 \leq j \leq a_1 - 1} n_{j,s} - a_1.$$

(b)
$$n_s(a_1, a_2, ..., a_k) = \frac{1}{a_1} \sum_{j=0}^{a_1 - 1} (n_{j,s} - j) = \frac{1}{a_1} \sum_{j=0}^{a_1 - 1} n_{j,s} - \frac{a_1 - 1}{2}.$$

Proof. (a) It must be shown that $\max\limits_{0 \leq j \leq a_1 - 1} n_{j,s} - a_1$ is $<s$-representable and that any integer greater than $\max\limits_{0 \leq j \leq a_1 - 1} n_{j,s} - a_1$ is $\geq s$-representable.

For the first part, $\max\limits_{0 \leq j \leq a_1 - 1} n_{j,s} - a_1$ is $<s$-representable since $n_{j,s} - a_1$ is $<s$-representable for each $j \in \{0, 1, ..., a_1 - 1\}$, because $n_{j,s}$ is the least non-negative integer congruent to j $(\text{mod } a_1)$ that is $\geq s$-representable.

For the second part, take any $x > \max\limits_{0 \leq j \leq a_1 - 1} n_{j,s} - a_1$ and note that x is congruent modulo a_1 to one of the $n_{i,s}$ since there is one $n_{i,s}$ for each $i \in \{0, 1, ..., a_1 - 1\}$. There are two possibilities: either x equals this $n_{i,s}$ or x is greater than this $n_{i,s}$.

- If $x = n_{i,s}$ for some $i \in \{0, 1, ..., a_1 - 1\}$, then x is $\geq s$-representable since each $n_{i,s}$, $i \in \{0, 1, ..., a_1 - 1\}$, is defined to be $\geq s$-representable.

- If x does not equal any of the $n_{i,s}$, note that x is still congruent modulo a_1 to one of the $n_{i,s}$ so $x = n_{i,s} + ta_1$ for one of the $n_{i,s}$ and some positive integer t, thus x is $\geq s$-representable since adding ta_1 to an integer that is $\geq s$-representable yields an integer that is $\geq s$-representable.

This proves part (a) of the proposition.

To prove part (b) of the proposition: given $j \in \{0, 1, ..., a_1 - 1\}$, note that $n_{j,s}$ is the least non-negative integer congruent to $j \pmod{a_1}$ such that $n_{j,s}$ is $\geq s$-representable by $A = \{a_1, a_2, ..., a_k\}$, thus all positive integers that are less than $n_{j,s}$ and congruent to $j \pmod{a_1}$ are $<s$-representable and so must be counted.

For each $j \in \{0, 1, ..., a_1 - 1\}$, count the number of integers between zero and $n_{j,s}$ that are congruent to $j \pmod{a_1}$ by noting that since $n_{j,s}$ is congruent to $j \pmod{a_1}$, then $n_{j,s} = pa_1 + j$ for some non-negative integer p, and so $n_{j,s}$ is the $(p+1)^{th}$ non-negative integer congruent to $j \pmod{a_1}$ since:

the 1^{st} non-negative integer integer congruent to $j \pmod{a_1}$ is j and $j = 0 \cdot a_1 + j$;

the 2^{nd} non-negative integer integer congruent to $j \pmod{a_1}$ equals $1 \cdot a_1 + j$;

the 3^{rd} non-negative integer integer congruent to $j \pmod{a_1}$ equals $2a_1 + j$;

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

the $(p+1)^{th}$ non-negative integer integer congruent to $j \pmod{a_1}$ equals $pa_1 + j = n_{j,s}$.

Since $n_{j,s}$ is the $(p+1)^{th}$ integer congruent to $j \pmod{a_1}$, then there are p integers congruent to $j \pmod{a_1}$ that are less than $n_{j,s}$. Thus we have that $p = \dfrac{n_{j,s} - j}{a_1}$; in other words, the number of non-negative integers congruent to $j \pmod{a_1}$ that are $<s$-representable is $\dfrac{n_{j,s} - j}{a_1}$. To complete the proof, sum the $\dfrac{n_{j,s} - j}{a_1}$ non-negative integers that are $<s$-representable for each $j \in \{0, 1, ..., a_1 - 1\}$ which gives that $n_s(a_1, a_2, ..., a_k) = \dfrac{1}{a_1} \displaystyle\sum_{j=0}^{a_1-1} n_{j,s} - j$. Next, remember that $\displaystyle\sum_{j=0}^{a_1-1} j = \dfrac{a_1(a_1-1)}{2}$ and part (b) of the proposition has been shown. □

Proposition 4.2. *Let* $A = \{a_1, a_2, ..., a_k\}$ *be a set of positive integers with* $\gcd(a_1, a_2, ..., a_k) = 1$. *If* $\gcd(a_2, a_3, ..., a_k) = d$, *let* $a_j = d \cdot a'_j$ *for each* $j \in \{2, ..., k\}$. *Then*

(a) $g_s(a_1, a_2, ..., a_k) = d \cdot g_s(a_1, a'_2, a'_3, ..., a'_k) + a_1(d-1)$.

(b) $n_s(a_1, a_2, ..., a_k) = d \cdot n_s(a_1, a'_2, a'_3, ..., a'_k) + \frac{1}{2}(a_1 - 1)(d-1)$.

Proof. (a) As in Proposition 4.1, for each $j \in \{0, 1, ..., a_1 - 1\}$ denote $n_{j,s}$ as the least nonnegative integer congruent to $j \pmod{a_1}$ such that $n_{j,s}$ is $\geq s$ representable by $A = \{a_1, a_2, ..., a_k\}$. Denote $n'_{j,s}$ similarly: $n'_{j,s}$ is the least non-negative integer congruent to $j \pmod{a_1}$ that is $\geq s$-representable by $A' = \{a_1, a'_2, a'_3, ..., a'_k\}$.

The result will follow easily after it is shown that $\{n_{i,s}\}_{i=0}^{a_1-1} = d \cdot \{n'_{j,s}\}_{j=0}^{a_1-1}$ which will be clear after the next several claims:

Claim: $n_{j,s}$ always has at least one of its representations $n_{j,s} = a_1m_1 + a_2m_2 + ... + a_km_k$ with $m_1 = 0$.

Proof of Claim: By definition, $n_{j,s}$ has at least s representations each of which is congruent to $j \pmod{a_1}$. The list of the representations of $n_{j,s}$ looks like

$$\begin{aligned} n_{j,s} &= a_1m_1 + a_2m_2 + ... + a_km_k \\ &= a_1\breve{m}_1 + a_2\breve{m}_2 + ... + a_k\breve{m}_k \\ &\vdots \qquad\quad \vdots \qquad\quad \vdots \\ &= a_1\grave{m}_1 + a_2\grave{m}_2 + ... + a_k\grave{m}_k \end{aligned}$$

for some non-negative integers $m_i, \breve{m}_i, ..., \grave{m}_i$. Now suppose that $m_1 \neq 0, \breve{m}_1 \neq 0, ..., \grave{m}_1 \neq 0$, thus at least one a_1 can be subtracted from each side of the above list of the representations of $n_{j,s}$ yielding

$$\begin{aligned} n_{j,s} - a_1 &= a_1(m_1 - 1) + a_2m_2 + ... + a_km_k \\ &= a_1(\breve{m}_1 - 1) + a_2\breve{m}_2 + ... + a_k\breve{m}_k \\ &\vdots \qquad\quad \vdots \qquad\quad \vdots \\ &= a_1(\grave{m}_1 - 1) + a_2\grave{m}_2 + ... + a_k\grave{m}_k. \end{aligned}$$

However, now the non-negative integer $n_{j,s} - a_1$ is $\geq s$-representable and is congruent to j (mod a_1) contradicting the definition of $n_{j,s}$. Thus at least one of $m_1, \breve{m}_1, ..., \grave{m}_1$ is equal to zero.

Now it is known that at least one representation of $n_{j,s}$ has $m_1 = 0$ so the list of representations of $n_{j,s}$ looks like

$$\begin{aligned} n_{j,s} &= a_2m_2 + ... + a_km_k \\ &= a_1\breve{m}_1 + a_2\breve{m}_2 + ... + a_k\breve{m}_k \\ &\vdots \qquad\quad \vdots \qquad\quad \vdots \\ &= a_1\grave{m}_1 + a_2\grave{m}_2 + ... + a_k\grave{m}_k. \end{aligned}$$

Note that any of $\breve{m}_1, ..., \grave{m}_1$ may also be zero.

Next, as a result of the above claim, realize that $d \mid n_{j,s}$ by recalling that $\gcd(a_2, a_3, ..., a_k) = d$ and $a_j = d \cdot a'_j$ so the first equation in the above list of representations of $n_{j,s}$ can be rewritten with d factored out:

$$\begin{aligned} n_{j,s} &= a_2m_2 + ... + a_km_k \\ &= d \cdot (a'_2m_2 + ... + a'_km_k), \end{aligned}$$

so $d \mid n_{j,s}$ and $\dfrac{n_{j,s}}{d}$ is a positive integer; also, d divides every representation of $n_{j,s}$. Further, for those representations of $n_{j,s}$ in which $\breve{m}_1$ is not zero, then $d \mid \breve{m}_1$ as the following claim shows:

Claim: Those representations of $n_{j,s}$ in which $\breve{m}_1$ is not zero are such that $d \mid \breve{m}_1$.

Proof of Claim: Take a representation of $n_{j,s}$ in which $\breve{m}_1$ is not zero and divide it by d:

$$\begin{aligned}\frac{n_{j,s}}{d} &= \frac{(a_1\breve{m}_1 + a_2\breve{m}_2 + ... + a_k\breve{m}_k)}{d} \\ &= \frac{(a_1\breve{m}_1)}{d} + \frac{(a_2\breve{m}_2)}{d} + ... + \frac{(a_k\breve{m}_k)}{d} \\ &= \frac{(a_1\breve{m}_1)}{d} + \frac{(da_2'\breve{m}_2)}{d} + ... + \frac{(da_k'\breve{m}_k)}{d} \qquad \text{(since } a_i = da_i' \text{ for } i \in \{2, ..., k\} \\ &= \frac{(a_1\breve{m}_1)}{d} + (a_2'\breve{m}_2) + ... + (a_k'\breve{m}_k)\end{aligned}$$

This last equality shows that $d \mid \breve{m}_1$ since $\frac{a_1\breve{m}_1}{d}$ is an integer and $\gcd(a_1, d) = 1$, so the claim is proved.

Thus $\frac{\breve{m}_1}{d} = \breve{m}_1{}'$ is an integer and $\frac{n_{j,s}}{d}$ is $\geq s$-representable by $A' = \{a_1, a_2', a_3', ..., a_k'\}$. The list of at least s representations of $\frac{n_{j,s}}{d}$ looks like

$$\begin{aligned}\frac{n_{j,s}}{d} &= a_2'm_2 + ... + a_k'm_k \\ &= a_1\breve{m}_1{}' + a_2'\breve{m}_2 + ... + a_k'\breve{m}_k \\ &\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \\ &= a_1\grave{m}_1{}' + a_2'\grave{m}_2 + ... + a_k'\grave{m}_k.\end{aligned}$$

Now we will prove that $\frac{n_{j,s}}{d} \in \{n_{i,s}'\}_{i=0}^{a_1-1}$. In other words, $\frac{n_{j,s}}{d}$ is the least integer congruent to some $i \pmod{a_1}$ that is $\geq s$-representable by $A' = \{a_1, a_2', a_3', ..., a_k'\}$. Suppose $\frac{n_{j,s}}{d} \equiv i$ (mod a_1), then any positive integer congruent to $i \pmod{a_1}$, when multiplied by d, will yield an integer congruent to $j \pmod{a_1}$. To see this, note that $n_{j,s}$ is congruent to $j \pmod{a_1}$ so $n_{j,s} = a_1W + j$. Also, $\frac{n_{j,s}}{d} \equiv i \pmod{a_1}$ so

$$\begin{aligned}&\frac{a_1W + j}{d} = a_1X + i \\ \Rightarrow \quad & a_1W + j = d \cdot (a_1X + i) \\ \Rightarrow \quad & a_1W + j = d \cdot a_1X + d \cdot i \\ \Rightarrow \quad & a_1(W - dX) + j = d \cdot i\end{aligned}$$

shows that $d \cdot i \equiv j \pmod{a_1}$.

That $\frac{n_{j,s}}{d}$ is the least integer congruent to $i \pmod{a_1}$ that is $\geq s$-representable will be demonstrated in the following claim.

Claim: $\frac{n_{j,s}}{d}$ is the least integer congruent to $i \pmod{a_1}$ that is $\geq s$-representable by $A' = \{a_1, a_2', a_3', ..., a_k'\}$.

Proof of Claim: That $\dfrac{n_{j,s}}{d}$ is congruent to $i \pmod{a_1}$ and is $\geq s$-representable has already been determined; all that is needed is to show that $\dfrac{n_{j,s}}{d}$ is the least such integer: suppose that x is a lesser integer that is congruent to $i \pmod{a_1}$ and is $\geq s$-representable, so $x < \dfrac{n_{j,s}}{d}$ with $x \equiv i \pmod{a_1}$. x is $\geq s$-representable by $A' = \{a_1, a'_2, a'_3, ..., a'_k\}$ and so has a list of at least s representations that looks like

$$\begin{aligned} x &= a'_2 x_2 + ... + a'_k x_k \\ &= a_1 \breve{x}_1 + a'_2 \breve{x}_2 + ... + a'_k \breve{x}_k \\ &\vdots \qquad\quad \vdots \qquad\quad \vdots \\ &= a_1 \grave{x}_1 + a'_2 \grave{x}_2 + ... + a'_k \grave{x}_k \end{aligned}$$

This list can now be multiplied by d resulting in a list congruent to $j \pmod{a_1}$. Further, since $x < \dfrac{n_{j,s}}{d}$, then $dx < n_{j,s}$. In other words dx is $\geq s$-representable by $A = \{a_1, a_2, ..., a_k\}$ and $dx \equiv j \pmod{a_1}$, a contradiction to the fact that $n_{j,s}$ is, by definition, the least non-negative integer congruent to $j \pmod{a_1}$ that is $\geq s$-representable. Thus no such x exists so the claim is proved.

Note that the claim shows $\left\{\dfrac{n_{j,s}}{d}\right\}_{j=0}^{a_1-1} \subset \{n'_{i,s}\}_{i=0}^{a_1-1}$ since for each $j \in \{0, 1, ..., a_1 - 1\}$, $\dfrac{n_{j,s}}{d}$ has been shown to be an element of $\{n'_{i,s}\}_{i=0}^{a_1-1}$. Note, also, that $\left\{\dfrac{n_{j,s}}{d}\right\}_{j=0}^{a_1-1} \subset \{n'_{i,s}\}_{i=0}^{a_1-1}$ implies $\{n_{j,s}\}_{j=0}^{a_1-1} \subset \{d \cdot n'_{i,s}\}_{i=0}^{a_1-1}$ is realized by multiplying every element in both sets by d.

The inclusion in the other direction – that $\{d \cdot n'_{i,s}\}_{i=0}^{a_1-1} \subset \{n_{j,s}\}_{j=0}^{a_1-1}$ - can be realized similarly: start with a $n'_{i,s} \in \{n'_{i,s}\}_{i=0}^{a_1-1}$; multiply all of its representations – there are at least s of them and represented by $A' = \{a_1, a'_2, a'_3, ..., a'_k\}$ – by d resulting in an element $n_{j,s}$, congruent to $j \pmod{a_1}$ and represented at least s times by $A = \{a_1, a_2, ..., a_k\}$. If there were a lesser element in $\{n_{j,s}\}_{j=0}^{a_1-1}$ congruent to $j \pmod{a_1}$ then d could be divided out, resulting in an integer $\geq s$-representable by $A' = \{a_1, a'_2, a'_3, ..., a'_k\}$, congruent to $i \pmod{a_1}$, and less than $n'_{i,s}$ contradicting the definition of the $n'_{i,s}$. Thus, $\{d \cdot n'_{i,s}\}_{i=0}^{a_1-1} \subset \{n_{j,s}\}_{j=0}^{a_1-1}$. Now inclusion has been shown in both directions, thus $\{n_{i,s}\}_{i=0}^{a_1-1} = \{d \cdot n'_{j,s}\}_{j=0}^{a_1-1}$, and the maximal element of one set equals the maximal element of the other.

Now the desired result for part (a) of Proposition 4.2 follows from Proposition 4.1:

$$\begin{aligned} g_s(a_1, a_2, ..., a_k) &= \max_{0 \leq j \leq a_1 - 1} n_{i,s} - a_1 && \text{(by Lemma 4.1)} \\ &= \max_{0 \leq j \leq a_1 - 1} d \cdot n'_{j,s} - a_1 && (\text{since } \{n_{i,s}\}_{i=0}^{a_1-1} = \{d \cdot n'_{j,s}\}_{j=0}^{a_1-1}) \\ &= d \cdot (\max_{0 \leq j \leq a_1 - 1} n'_{j,s} - a_1) + a_1(d-1) \\ &= d g_s(a_1, a'_2, a'_3, ..., a'_k) + a_1(d-1) && \text{(by Proposition 4.1).} \end{aligned}$$

To prove part (b) of the proposition, apply Proposition 4.1:

$$\begin{aligned}
n_s(a_1, a_2, ..., a_k) &= \frac{1}{a_1}\sum_{j=0}^{a_1-1} n_{j,s} - \frac{a_1-1}{2} \qquad \text{(by Proposition 4.1)} \\
&= d \cdot (\frac{1}{a_1}\sum_{j=0}^{a_1-1} n'_{j,s} - \frac{a_1-1}{2}) + \frac{1}{2}(a_1-1)(d-1) \\
&= d \cdot n_s(a_1, a'_2, a'_3, ..., a'_k) + \frac{1}{2}(a_1-1)(d-1).
\end{aligned}$$

□

Chapter 5

The Main Theorem

5.1 Tripathi's Theorem

Let's be reminded of Tripathis's Theorem (1.4) and one of his two proofs found in [15].

Theorem 5.1. *Let $a_1, a_2, ..., a_k$ be pairwise coprime positive integers with product Π . For $i \in \{1, 2, ..., k\}$, let $A_i = \frac{\Pi}{a_i}$ and denote by Σ the sum $A_1 + A_2 + ... + A_k$. Then*

$$g_1 = g(A_1, A_2, ..., A_k) = (k-1)\Pi - \Sigma.$$

To prove the theorem, we will need the following

Lemma 5.2. *Any positive integer x can be written as*

$$x = A_1x_1 + A_2x_2 + ... + A_kx_k$$

with $0 \leq x_i \leq (a_i - 1)$ for every $i \in \{1, ..., k-1\}$.

Proof. If A_ix_i is negative then add a multiple of a_i to this term to make it positive yielding $A_i(x_i + Ta_i)$. Because $A_ia_i = A_ka_k$, we can keep the representation equal to x by simultaneously subtracting Ta_k from the term A_kx_k possibly rendering it negative, so

$$x = A_1x_1 + ... + A_i(x_i + Ta_i) + ... + A_k(x_k - Ta_k)$$

with only x_k possibly negative. Note that negative A_ix_i means x_i is negative, and since $x_i \equiv h \pmod{a_i}$ for some $h \in \{1, ..., a_i - 1\}$, then $x_i = -Ta_i + h$ for some positive T. It follows that $x_i + Ta_i = h$. □

Proof of Theorem 5.1. We need to see both that $(k-1)\Pi - \Sigma$ is not representable by $A_1, A_2, ..., A_k$, and that any integer greater than $(k-1)\Pi - \Sigma$ is representable.

For the first part, suppose that $(k-1)\Pi - \Sigma$ is representable so

$$A_1x_1 + A_2x_2 + ... + A_kx_k = (k-1)\Pi - \Sigma$$

with $x_j \geq 0 \ \forall \ j \in \{1, ..., k\}$.

- For each $j \in \{1, ..., k\}$, the left-hand side of the above equation is congruent to $A_j x_j$ modulo a_j since every $A_i = \frac{\Sigma}{a_i}$ is a multiple of a_j when $i \neq j$.
- The right hand side is congruent to $-A_j$ modulo a_j since $\Pi \equiv 0 \pmod{a_j}$ and $-\Sigma \equiv -A_j \pmod{a_j}$.
- Thus $A_j x_j \equiv -A_j \pmod{a_j}$ so

$$\begin{aligned} & a_j \mid A_j(x_j+1) \\ \Rightarrow\ & a_j \mid (x_j+1) \ (\text{since} \gcd(a_j, A_j) = 1) \\ \Rightarrow\ & a_j \leq (x_j+1) \ \Rightarrow\ x_j \geq (a_j - 1) \text{ for each } j \in \{1, ..., k\}. \end{aligned}$$

However this is impossible since then

$$\begin{aligned} (k-1)\Pi - \Sigma = A_1x_1 + A_2x_2 + ... + A_kx_k &\geq A_1(a_1-1) + A_2(a_2-1) + ... + A_k(a_k-1) \\ &= A_1a_1 - A_1 + A_2a_2 - A_2 + ... + A_ka_k - A_k \\ &= k\Pi - \Sigma \end{aligned}$$

so the first part of the proof is complete.

For the second part, first note that we can rewrite

$$\begin{aligned} & (k-1)\Pi - \Sigma \\ = \ & a_1A_1 + a_2A_2 + ... + a_{k-1}A_{k-1} - A_1 - A_2 - ... - A_{k-1} - A_k \\ = \ & A_1(a_1-1) + A_2(a_2-1) + ... + A_{k-1}(a_{k-1}-1) - A_k, \end{aligned} \tag{5.1}$$

and choose $N > (k-1)\Pi - \Sigma$. Write $N = A_1w_1 + ... + A_kw_k$ within the constraints of Lemma 5.2 so that only w_k may be negative. We then have

$$\begin{aligned} A_1w_1 + ... + A_kw_k &> (k-1)\Pi - \Sigma \\ A_1w_1 + ... + A_kw_k &> A_1(a_1-1) + A_2(a_2-1) + ... + A_{k-1}(a_{k-1}-1) - A_k \\ A_kw_k &> -A_k \quad (\text{since } (a_i - 1) \geq w_i) \\ A_k(w_k+1) &> 0. \end{aligned}$$

So we have $w_k + 1 > 0 \ \Rightarrow \ w_k > -1 \ \Rightarrow \ w_k \geq 0$, thus Tripathi's Theorem is proved. □

5.2 Extending Tripathi's Theorem

Theorem 5.3. *For the A_i as defined in Theorem 5.1,*

$$k\Pi - \Sigma = g_1 + \Pi = g_2 = g_3 = g_4 = ... = g_k.$$

In other words, $k\Pi - \Sigma$ is exactly 1-representable and every integer greater than $k\Pi - \Sigma$ is $\geq k$-representable.

Proof. For the first part, note that $g_1 + \Pi$ is representable; to see that $g_1 + \Pi$ has no more than one representation, first note that we already saw in equation (5.1)

$$g_1 = A_1(a_1 - 1) + A_2(a_2 - 1) + ... + A_{k-1}(a_{k-1} - 1) - A_k,$$

so

$$\begin{aligned} g_1 + \Pi &= A_1(a_1 - 1) + A_2(a_2 - 1) + ... + A_{k-1}(a_{k-1} - 1) - A_k + \Pi \\ &= A_1(a_1 - 1) + A_2(a_2 - 1) + ... + A_{k-1}(a_{k-1} - 1) + A_k(a_k - 1) \end{aligned}$$

reveals the unique representation for $g_1 + \Pi$:

- Any other representation of $g_1 + \Pi$ would have some of the above terms increase while some decrease.

- If $A_i(a_i - 1 + t_i)$ is one of the increased terms then it follows that $(a_i - 1 + t_i) \geq a_i$.

- Thus $A_i(a_i - 1 + t_i) = A_i(a_i + c_i)$ for some nonnegative integer c_i.

- Now subtracting $\Pi = A_i a_i$ from both sides of the above representation for $g_1 + \Pi$ reveals $g_1 = A_1 m_1 + ... + A_i c_i + ... + A_k m_k$ — where the m_j are the other coefficients that were increased or decreased — contrary to the fact that g_1 is not representable.

Thus it has been shown that $g_1+\Pi$ is 1-representable so the first part of the proof is complete.

Next, choose any integer x greater than $g_1+\Pi$, and we will see that x is $>$1-representable — in fact, we will show that x is $\geq k$-representable. Note that there exists some positive integer U such that

$$g_1 + U\Pi \ < \ x \ \leq \ g_1 + (U + 1)\Pi$$

thus, we may subtract from x some multiple of Π so that

$$g_1 \ < \ x - U\Pi \ \leq \ g_1 + \Pi.$$

Note that $x - U\Pi > g_1$ and so is representable, say

$$x - U\Pi = A_1x_1 + A_2x_2 + ... + A_kx_k.$$

Thus

$$x = A_1x_1 + ... + A_i(x_i + Ua_i) + ... + A_kx_k$$

for each $i \in \{1, ..., k\}$ shows that x is $\geq k$-representable. □

5.3 The Main Theorem

For the main theorem, we will need to know something of binomial coefficients, $\binom{n}{k}$, also known as the choose function. Recall that $\binom{n}{k}$ can be viewed as the number of ways to distribute k objects into n slots when repetitions are not allowed. Now we will use the choose function to designate the number of ways to distribute k objects into n slots when repetitions are allowed and see that this number is $\binom{n+k-1}{k}$.

Looking at a concrete example will help: suppose we want to distribute two objects into the first slot, two objects into the second slot, etc, until we run out of objects or have to put all remaining objects in the last slot. We can visualize lining up in a row the k objects to be distributed, and putting two aside to reserve them for the first slot, then two more aside for the next slot, etc, until we have n piles ready for the n appropriate slots. Now note that there are $n-1$ spaces between the n piles, thus our problem has become determining the number of ways to label $n-1$ 'spaces' out of a total of $n-1+k$ items (which are the $n-1$ spaces plus the k objects). This number is $\binom{n-1+k}{n-1}$. Next we apply a common identity for the choose function, that $\binom{a}{b} = \binom{a}{a-b}$ to see that $\binom{n-1+k}{n-1} = \binom{n-1+k}{k}$.

We will also need $\binom{a}{b} = 0$ when $b < 0$, so that our extension merges seamlessly with Tripathi's Theorem 5.1, rendering it a corollary to our results.

Theorem 5.4. *For $T \geq 0$,*

$$(k+T-1)\Pi - \Sigma = g_1 + T\Pi = g_{\binom{k+T-2}{T-1}+1} = g_{\binom{k+T-2}{T-1}+2} = ... = g_{\binom{k+T-1}{T}}.$$

Further, when $T > 0$, $g_1 + T\Pi$ has exactly $\binom{k+T-2}{T-1}$ representations. These $\binom{k+T-2}{T-1}$ representations are realized as

$$A_1(a_1 - 1 + t_1a_1) + A_2(a_2 - 1 + t_2a_2) + ... + A_k(a_k - 1 + t_ka_k), \tag{5.2}$$

with the sum of the t_i equal to $T-1$.

It will be handy later if we note now that the coefficient of A_i in (5.2) satisfies

$$a_i - 1 + t_ia_i \equiv a_i - 1 \pmod{a_i}. \tag{5.3}$$

Note also that Theorem 5.1 is the special case $T = 0$.

Proof. We induct on T. We have seen that the theorem is true for $T = 0$ which was Tripathi's Theorem 5.1. We then saw the theorem true for $T = 1$ in Theorem 5.3. Assume the theorem is true for $T = 0$, $T = 1$,...,$T = I - 1$. So

$$(k + (I-1) - 1)\Pi - \Sigma = g_1 + (I-1)\Pi = g_{\binom{k+I-3}{I-2}+1} = ... = g_{\binom{k+I-2}{I-1}}$$

and this number has exactly $\binom{k+I-3}{I-2}$ representations of the form (5.2) with $t_1 + t_2 + ... + t_k = I - 2$, and let

$$x = (k + I - 1)\Pi - \Sigma.$$

We show that x is exactly $\binom{k+I-2}{I-1}$-representable and that any integer greater than x is $\geq\binom{k+I-1}{I}$-representable thus showing $x = g_{\binom{k+I-2}{I-1}+1} = ... = g_{\binom{k+I-1}{I}}$.

To see that x is exactly $\binom{k+I-2}{I-1}$-representable, we will show that x is both $\geq\binom{k+I-2}{I-1}$-representable and $\leq\binom{k+I-2}{I-1}$-representable.

Claim: x is $\geq\binom{k+I-2}{I-1}$-representable

Proof of Claim: First note that, by the induction hypothesis, $x - \Pi$ has exactly $\binom{k+I-3}{I-2}$ representations, each of which looks like

$$A_1(a_1 - 1 + t_1a_1) + ... + A_i(a_i - 1 + t_ia_i) + ... + A_k(a_k - 1 + t_ka_k), \tag{5.4}$$

with the sum of the t_i equal to $I-2$. The $\binom{k+I-3}{I-2}$ representations of $x-\Pi$ are found by the $\binom{k+I-3}{I-2}$ ways to distribute $I-2$ among the t_i's in (5.4). Now add $\Pi = A_j a_j$ to $x-\Pi$ to see that x's list of representations has at least as many members as there are ways to distribute $I-1$ into the t_i's in (5.4). Thus there are at least $\binom{k+I-2}{I-1}$ representations for x.

Denote by $\mathcal{L}$ the list of $\binom{k+I-2}{I-1}$ representations for x found by distributing $I-1$ into the t_i's in (5.4).

Claim: x is $\leq\binom{k+I-2}{I-1}$-representable.

Proof of Claim: Seeking contradiction, assume x is $>\binom{k+I-2}{I-1}$-representable, and let X be a representation not a member of $\mathcal{L}$. X looks like

$$A_1x_1 + ... + A_jx_j + ... + A_kx_k.$$

Let's compare X to a representation, U of $\mathcal{L}$. U looks like

$$A_1(a_1 - 1 + t_1a_1) + ... + A_j(a_j - 1 + t_ja_j) + ... + A_k(a_k - 1 + t_ka_k). \tag{5.5}$$

Note that the t_i sum to $I-1$, and for each $i \in \{1, ..., k\}$, the coefficient of A_i is congruent to $a_i - 1$ modulo a_i as noted in (5.3). At least one term, say A_jx_j, of X, is not of the form in U, and so $x_j \not\equiv a_j - 1 \pmod{a_j}$. Thus

$$x_j = d + \alpha a_j \tag{5.6}$$

for some $\alpha \geq 0$ and $0 \leq d < a_j - 1$. We have two cases:

- If, in equation (5.6), $\alpha > 0$, then $X - \Pi$ looks like

  $$A_1x_1 + ... + A_j(d + (\alpha - 1)a_j) + ... + A_kx_k.$$

  However, this is impossible since then $x - \Pi$ has A_j with its coefficient not congruent to $a_j - 1$ modulo a_j, contradicting (5.3).

- If, in equation (5.6), $\alpha = 0$, then $x_j = d$, so $A_jx_j < A_j(a_j - 1 + ta_j)$, and $\exists\ i$ with $A_ix_i > A_i(a_i - 1 + ta_i)$. We split into two cases: either (1) $x_i \equiv a_i - 1 \pmod{a_i}$ or (2) $x_i \not\equiv a_i - 1 \pmod{a_i}$.

  - If (1) then $x_i = (a_i - 1 + t_ia_i + ca_i)$ for some positive c, so $X - \Pi$ looks like

    $$A_1x_1 + ... + A_i(a_i - 1 + t_ia_i + (c-1)a_i) + ... + A_jd + ... + A_kx_k.$$

    However this is impossible since the coefficient of A_j does not satisfy (5.3).

  - If (2), that $x_i \not\equiv a_i - 1 \pmod{a_i}$, then $x_i = (a_i - 1 + t_ia_i + c)$ for some positive c not a multiple of a_i, but then we play the same game as above to see that $X - \Pi$ looks like

    $$A_1x_1 + ... + A_i(t_ia_i + c - 1) + ... + A_jd + ... + A_kx_k.$$

    However this is impossible since now there are at least two coefficients not satisfying (5.3).

Thus no such X can exist, so the claim is proved.

Claim: If $N > x$, then N is $\geq\binom{k+I-1}{I}$-representable.
Proof of Claim: N is greater than $x = g_1 + I\Pi$, so $N - I\Pi > g_1$ has a representation

$$N - I\Pi = A_1y_1 + A_2y_2 + ... + A_ky_k. \tag{5.7}$$

At least how many representations must N have? To answer this, we add the $I\Pi$ to equation (5.7) and note that $I\Pi = IA_ja_j$ for every $j \in \{1, ..., k\}$, thus our question asks how many ways there are to distribute I A_ja_j's into the k summands of equation (5.7). This number is $\binom{k+I-1}{I}$, thus we have that N is $\geq\binom{k+I-1}{I}$-representable. □

Bibliography

[1] J.L.R. Alfonsin, *The diophantine Frobenius problem*, Oxford University Press, 2005.

[2] Matthias Beck and Sinai Robins, *An extension of the frobenius coin-exchange problem*, online at http://arxiv.org/abs/math/0204037 (2003).

[3] Matthias Beck and Sinai Robins, *Computing the Continuous Discretely*, Springer, 2007.

[4] A. Brauer and J.E. Shockley, *On a problem of Frobenius*, J. reine angew. Math **211** (1962), 215–220.

[5] Alfred Brauer, *On a problem of partitions*, American Journal of Mathematics **64** (1942), no. 1, 299–312.

[6] Alfred Brauer and B. M. Seelbinder, *On a problem of partitions ii*, American Journal of Mathematics **76** (1954), no. 2, 343–346.

[7] A. Brown, E. Dannenberg, J. Fox, J. Hanna, K. Keck, A. Moore, Z. Robbins, B. Samples, and J. Stankewicz, *On a Generalization of the Frobenius Number*, Journal of Integer Sequences **13** (2010), 10.1.4.

[8] P. Erdös and E.L. Graham, *On a linear diophantine problem of Frobenius*, Acta Arithmetica (1972), 399–408.

[9] S.M. Johnson, *A Linear Diophantine Problem*, Canad. J. Math **12** (1960), 390–398.

[10] O.J. Rödseth, *On a Linear Diophantine Problem of Frobenius*, J. reine angew. Math **301** (1978), 171–178.

[11] E. S. Selmer, *On the linear Diophantine problem of Frobenius*, J. reine angew. Math **293** (1977), 1–17.

[12] Jeffrey Shallit and James Stankewicz, *Unbounded discrepancy in frobenius numbers*, online at http://arxiv.org/abs/1003.0021v1 (2010).

[13] James J. Sylvester, *On Subvariants, i.e. Semi-Invariants to Binary Quantics of an Unlimited Order*, American Journal of Mathematics **5** (1882), 79–136.

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

[15] Amitabha Tripathi, *On a Linear Diophantine Problem of Frobenius*, Integers: Electronic Journal of Combinatorial Number Theory **6, A14** (2006).