A SEQUENCE OF QUASIPOLYNOMIALS ARISING FROM RANDOM NUMERICAL SEMIGROUPS

CALVIN LENG

Abstract. De Loera, O'Neill, and Wilburne recently proved that the expected number of minimum generators of a randomly generated numerical semigroup can be expressed in terms of a doubly-indexed sequence of integers, denoted $h_{n,i}$, that count generating sets with certain properties. We investigate the values. In particular, we prove a recurrence relation that implies this sequence is eventually quasipolynomial when the second parameter is fixed.

Contents

1. Introduction 1
2. Background 3
3. Random Numerical Semigroups 6
4. Quasipolynomial Pattern/Motivating Overview 8
5. Results on RI-pairs that Correspond to Working Sets 12
6. Proof of Main Results 19
7. Algorithms and Miscellaneous Remarks 24
8. Future Work 26
References 27

1. Introduction

A *numerical semigroup* is a subset of $\mathbb{Z}_{\geq 0}$ containing 0 that is closed under addition. De Loera, O'Neill, and Wilburne [2] introduced a model for random numerical semigroups, and expressed the expected number of minimal generators of producing the resulting numerical semigroup in terms of a sequence of integers, denoted $h_{n,i}$. The values of $h_{n,i}$ for $n = 68$ to $n = 76$ are presented in Figure 1.

Figure 1 is read with the second parameter of $h_{n,i}$ taking $i = 0, 1, 2, \ldots$, e.g. $h_{68,2} = 249$. For all n, the value of $h_{n,i}$ is positive for only a finite number of i's. Thus we denote $d_n = \max\{i : h_{n,i} > 0\} = \deg h_n$ (see (1.1)). From [2, Proposition 4.12.c] we get

Date: June 13, 2018.
Key words and phrases. numerical semigroup; computation; quasipolynomial.

$n = 68$:	1,	29,	249,	888,	1705,	2014,	1599,	888,	347,	91,	14,	1	
$n = 69$:	1,	31,	301,	1181,	2414,	2939,	2365,	1335,	535,	147,	25,	2	
$n = 70$:	1,	28,	248,	1012,	2218,	2873,	2431,	1414,	569,	155,	26,	2	
$n = 71$:	1,	34,	359,	1577,	3615,	4945,	4481,	2878,	1348,	453,	105,	15,	1
$n = 72$:	1,	25,	222,	893,	1923,	2498,	2138,	1267,	526,	147,	25,	2	
$n = 73$:	1,	35,	383,	1764,	4252,	6139,	5883,	4008,	2004,	725,	181,	28,	2
$n = 74$:	1,	34,	337,	1456,	3361,	4694,	4365,	2853,	1345,	453,	105,	15,	1
$n = 75$:	1,	32,	346,	1582,	3810,	5567,	5428,	3758,	1888,	684,	172,	27,	2
$n = 76$:	1,	33,	334,	1448,	3413,	5005,	4992,	3559,	1863,	705,	181,	28,	2

FIGURE 1. Coefficient rows $n = 68$ to $n = 76$. Patterns in the rightmost values apparent mod 3

the formula $d_n = \lfloor (n-1)/2 \rfloor - \lfloor n/3 \rfloor$. For example, $d_{68} = 11$ and $d_{71} = 12$, as seen from the length of each row.

From the proof of [2, Theorem 5.5], a formula for the expected number of minimal generators of a random numerical semigroup, denoted $\mathbb{E}[e(S)]$, is given by

$$\mathbb{E}[e(S)] = \sum_{n=1}^{M} p(1-p)^{\lfloor n/2 \rfloor} \left(h_{n,0} + h_{n,1} p + \dots h_{n,d_n} p^{d_n} \right). \tag{1.1}$$

for fixed input parameters (M, p) (see [2]). Formula (1.1) demonstrates that the expected number of minimal generators is completely determined by the sequence $h_{n,i}$. The details of the aforementioned results will be elaborated on in Section 3.

In the same paper, they prove that $h_{n,i}$ counts the number of numerical semigroups that satisfy certain criteria and use this to obtain upper and lower bounds on $\mathbb{E}[e(S)]$. Currently, computing $h_{n,i}$ is time-intensive: the computation takes 3 days for $n = 89$ on the authors' machines. The results of the computations are provided at

`https://gist.github.com/coneill-math/c2f12c94c7ee12ac7652096329417b7d`.

Not much is known of the values of the coefficients. We summarize the results developed in [2].

- $h_{n,0} = 1$.
- $h_{n,1} = \lfloor (n+1)/2 \rfloor - \tau(n)$ where $\tau(n)$ denotes the number of divisors of n.
- For any $i \geq 1$ and $N \geq 2$, we have

$$\sum_{j=2}^{N} \binom{\lfloor (n-1)/j \rfloor - \lfloor n/(j+1) \rfloor}{i} \leq h_{n,i} \leq \binom{\lceil n/2 \rceil - 2i}{i}.$$

The goal of this paper is to further investigate the sequence $h_{n,i}$, as they encode much information about the expected properties of random numerical semigroups. The main result of this paper is a recurrence relation among h_{n,d_n-k} for k fixed and

n large. With reference to Figure 1, this particular class of coefficients corresponds to the final (asymptotically $d_n/4$) entries of each row.

Theorem 1.1 (Main Theorem). *For each non-negative integers k, we have*

$$h_{n,d_n-k} = \sum_{l=0}^{k} h_{m,d_m-l}\binom{d_n-d_m}{k-l}$$

for all $n \geq m > 24k + 12 - 8b$, where $n, m \equiv b$ mod 3 for $b \in \{0, 1, 2\}$.

Theorem 1.1 implies that h_{n,d_n-k} is eventually quasipolynomial in n, and recover the degree, period, and formula for the leading coefficient.

Corollary 1.2 (Quasipolynomiality). *For fixed k and sufficiently large n, the value h_{n,d_n-k} is a quasipolynomial in n of degree k with period 6 and constant leading coefficient*

$$c_k = \begin{cases} \frac{2}{k!6^k} & n \equiv 0, 1 \ mod\ 3 \\ \frac{1}{k!6^k} & n \equiv 2 \ mod\ 3 \end{cases}.$$

In the development of the proof of Theorem 1.1, we also arrive at an algorithm for computing $h_{n,i}$ among this particular class of indices that is more efficient than the brute force method. Notably, the algorithm computes h_{n,d_n-k} for any sufficiently large n (with respect to k) in $O(2^{4k})$ time. The time complexity is independent of n, providing unexpected results. For example, computing $h_{90,d_{90}-3}$ takes around the same time as computing $h_{90000,d_{90000}-3}$; the only difference in runtime is attributed to computing larger binomial coefficients. Additionally, the implicit constant for the time complexity is small: the algorithm has been successfully run up to $k = 7$ on the author's machine, taking around 6 hours. Moreover, the algorithm is parallelizable, a fact that has yet to be utilized (see Problem 8.3).

The algorithm has obtained $h_{n,i}$ values that were previously unobtainable. As provided in the link earlier, rows of h_n were computed up to $n = 90$. With the improved algorithm and Theorem 1.1, explicit quasipolynomials have been provided for h_{n,d_n-k} up to $k = 4$ in Figure 2 and for $k = 5, 6, 7$ at the link provided in Remark 7.5 (due to lack of spacing). Notably, computing the quasipolynomial for h_{n,d_n-7} entails computing the value of $h_{183,d_{183}-7} = h_{183,23} = 6423209$ without the machinery of Theorem 1.1, a task which would have been outside the reach of computation with the current algorithm.

2. Background

Definition 2.1. A *semigroup* is a group without the criteria of invertability. A *numerical semigroup* is a subsemigroup of $\mathbb{Z}_{\geq 0}$ with the operation of addition. The *numerical semigroup generated by a generating set* $A = \{a_1, a_2, \ldots, a_k\}$ is the set

$$S = \langle A \rangle = \{a_1x_1 + a_2x_2 + \cdots + a_kx_k : x_i \in \mathbb{Z}_{\geq 0}\}.$$

$$h_{n,d_n} = \begin{cases} 2 & n \equiv 0 \bmod 6, n \geq 18 \\ 2 & n \equiv 1 \bmod 6, n \geq 7 \\ 1 & n \equiv 2 \bmod 6, n \geq 2 \\ 2 & n \equiv 3 \bmod 6, n \geq 15 \\ 2 & n \equiv 4 \bmod 6, n \geq 10 \\ 1 & n \equiv 5 \bmod 6, n \geq 5 \end{cases}$$

$$h_{n,d_n-1} = \begin{cases} \frac{1}{3}(n+3) & n \equiv 0 \bmod 6, n \geq 42 \\ \frac{1}{3}(n+11) & n \equiv 1 \bmod 6, n \geq 31 \\ \frac{1}{6}(n+16) & n \equiv 2 \bmod 6, n \geq 26 \\ \frac{1}{3}(n+6) & n \equiv 3 \bmod 6, n \geq 39 \\ \frac{1}{3}(n+8) & n \equiv 4 \bmod 6, n \geq 34 \\ \frac{1}{6}(n+19) & n \equiv 5 \bmod 6, n \geq 23 \end{cases}$$

$$h_{n,d_n-2} = \begin{cases} \frac{1}{36}(n^2+108) & n \equiv 0 \bmod 6, n \geq 66 \\ \frac{1}{36}(n^2+16n+19) & n \equiv 1 \bmod 6, n \geq 55 \\ \frac{1}{72}(n^2+26n+160) & n \equiv 2 \bmod 6, n \geq 50 \\ \frac{1}{36}(n^2+6n+117) & n \equiv 3 \bmod 6, n \geq 63 \\ \frac{1}{36}(n^2+10n-20) & n \equiv 4 \bmod 6, n \geq 58 \\ \frac{1}{72}(n^2+32n+247) & n \equiv 5 \bmod 6, n \geq 47 \end{cases}$$

$$h_{n,d(n)-3} = \begin{cases} \frac{1}{648}(n^3-9n^2+342n-3240) & n \equiv 0 \bmod 6, n \geq 90 \\ \frac{1}{648}(n^3+15n^2-69n+5885) & n \equiv 1 \bmod 6, n \geq 79 \\ \frac{1}{1296}(n^3+30n^2+264n-1952) & n \equiv 2 \bmod 6, n \geq 74 \\ \frac{1}{648}(n^3+315n-2268) & n \equiv 3 \bmod 6, n \geq 87 \\ \frac{1}{648}(n^3+6n^2-132n+6200) & n \equiv 4 \bmod 6, n \geq 82 \\ \frac{1}{1296}(n^3+39n^2+471n-863) & n \equiv 5 \bmod 6, n \geq 71 \end{cases}$$

$$h_{n,d_n-4} = \begin{cases} \frac{1}{15552}(n^4-24n^3+828n^2-17280n+419904) & n \equiv 0 \bmod 6, n \geq 114 \\ \frac{1}{15552}(n^4+8n^3-282n^2+24728n+413225) & n \equiv 1 \bmod 6, n \geq 103 \\ \frac{1}{31104}(n^4+28n^3+204n^2-10256n+454912) & n \equiv 2 \bmod 6, n \geq 98 \\ \frac{1}{15552}(n^4-12n^3+666n^2-12852n+374949) & n \equiv 3 \bmod 6, n \geq 111 \\ \frac{1}{15552}(n^4-4n^3-300n^2+26528n-490112) & n \equiv 4 \bmod 6, n \geq 106 \\ \frac{1}{31104}(n^4+40n^3+510n^2-8168n+426817) & n \equiv 5 \bmod 6, n \geq 95 \end{cases}$$

FIGURE 2. Quasipolynomial formulas for h_{n,d_n-k} up to $k=4$.

A generating set A is *minimal* if for all $x \in A$, we have $\langle A \rangle \neq \langle A \setminus \{x\} \rangle$. The *embedding dimension* of a numerical semigroup S is the size of a set that minimally generates S. Every numerical semigroup has a unique minimal generating set (see [1]).

Example 2.2. The numerical semigroup S generated by $A = \{6, 9, 20\}$ is the set

$$S = \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, 24, 26, 27, 29, 30, 32, 33, 35, 36, 38, 39, 40, 41, 42, 44, 45, 46, \dots\}.$$

One can think of S as the non-negative integral span of A. We see that the set A minimally generates S since if we removed any element from A, the resulting set will no longer generate S. Therefore the embedding dimension of S is $e(S) = 3$.

Let $B = \{6, 9, 15, 20\}$ be a generating set. We see that B also generates S, i.e. $\langle B \rangle = S$. However, we see that $B \setminus \{15\}$ also generates S, as demonstrated in the previous paragraph. Hence B does not minimally generate S. This demonstrates the notion that one can think of the embedding dimension of a numerical semigroup as the number of "non-redundant generators" needed. In fact, a generating set minimally generates a numerical semigroup if no generator is a sum of the other generators.

We can also explain the idea of a numerical semigroup with a familiar analogy. Consider a McDonald's menu that sells McNuggets only in boxes of 6, 9, and 20. Then, S would be every possible quantities of McNuggets one could purchase given the menu.

Definition 2.3. Given $k \in \mathbb{Z}_{\geq 1}$ and $n \in \mathbb{Z}$, the *binomial coefficient* $\binom{n}{k}$ is the integer

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{k!}.$$

Remark 2.4. Definition 2.3 coincides with the usual binomial coefficient for $n \in \mathbb{Z}_{\geq 1}$, which is defined as

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

and only takes in inputs $n \geq k$. We see the usual binomial coefficient is a special case of the generalized binomial coefficient. We use the generalized binomial coefficient in this paper as we often want to use the binomial coefficients with inputs n not necessarily greater or equal than k.

Example 2.5. We have

$$\binom{5}{2} = \frac{5 \cdot 4}{2!} = 10$$

$$\binom{k}{k+1} = \frac{k \cdot (k-1) \cdot (k-2) \cdots 0}{(k+1)!} = 0$$

$$\binom{-5}{2} = \frac{(-5) \cdot (-6)}{2!} = 15.$$

Notation 2.6. The *floor* of a real number x is the integer part of x, denoted $\lfloor x \rfloor$. In other words,

$$\lfloor x \rfloor = \max\{l \in \mathbb{Z} : l \leq x\}.$$

Notation 2.7. We denote $\delta(x, y)$ as the function on $\mathbb{Z} \to \mathbb{Z}$ such that

$$\delta(x, y) = \begin{cases} 1 & x \equiv y \bmod 2 \\ 0 & x \not\equiv y \bmod 2 \end{cases}.$$

In other words, $\delta(x, y)$ is the indicator function for the event that x and y maintain the same parity.

Definition 2.8. A *quasipolynomial* is a function $q : \mathbb{Z} \to \mathbb{Z}$ such that

$$q(x) = c_0(x) + c_1(x)x + c_2(x)x^2 + \cdots + c_d(x)x^d$$

where each $c_i(x)$ is periodic function of integral period. The *degree* of q is the integer d, denoted $\deg q$. The *period* of q is the lowest common multiple of the periods of all the c_i. The *leading coefficient* of q is $c_d(x)$.

Remark 2.9. Quasipolynomials are simply polynomials where coefficients are periodic functions. Quasipolynomials are widely used in combinatorics when a polynomial can be expressed only in specific residue classes modulo n.

3. Random Numerical Semigroups

The authors of [2] provide a model of randomly generating a numerical semigroup that is similar to the Erdos-Renyi model for random graphs. We now make this formal.

Definition 3.1 ([2, Chapter 1])**.** Fix as input a non-negative integer M and a probability $p \in [0, 1]$. Generate a numerical semigroup S according to the following procedure:

- initialize a set of generators $A = \{\}$ for S;
- independently choose with probability p whether to include each $n \leq M$ in A.

A numerical semigroup $S = \langle A \rangle$ produced by this model is indicated by $S \sim S(M, p)$.

Example 3.2. Let $M = 40$ and $p = 0.05$. To produce a random numerical semigroup S by this method: for each value of x include $x \in A$ with probability 0.05. An example is $A = \{8, 16, 20, 23\}$. Since 16 is redundant, the minimal generating set produced by this procedure is $A' = \{8, 20, 23\}$. Our resulting semigroup is $S = \langle A' \rangle = \langle A \rangle$. Notice that some of the generators in the generating set produced by this method were redundant. This is what makes characterizing the expected embedding dimension of a numerical semigroup produced by $S(M, p)$ an interesting question.

From [2] we have the following results on the expected embedding dimension of a random numerical semigroup with parameters (M, p).

Theorem 3.3 ([2, Theorem 1.1, Corollary 4.10])**.** *If $S \sim (M, p)$, then*

$$\mathbb{E}[e(S)] = \sum_{n=1}^{M} p(1-p)^{\lfloor n/2 \rfloor} \left(h_{n,0} + h_{n,1}p + \dots h_{n,d_n}p^{d_n}\right)$$

where $h_{n,i}$ counts the number of generating sets A such that

- $|A| = i$;
- $x < n/2$ *for all* $x \in A$;
- *A minimally generates a numerical semigroup; and*
- $n \notin \langle A \rangle$.

Therefore the more values of $h_{n,i}$ we can compute, the better we can approximate the expected behavior of numerical semigroups sampled with this model. The general goal of this paper is to better understand $h_{n,i}$ to allow for more efficient computation. We urge the reader to take a look at the table of coefficients $h_{n,i}$ that have been computed at the link provided in Section 1. To read the data, the first integer in each line corresponds to the value of n. Every integer afterwards corresponds to $i = 0$, then $i = 1$, and so on until $i = d_n$. Notably, h_{n,d_n} refers to the final entry of the n-th row, and h_{n,d_n-k} refers to the $(k+1)$-th to last entry of the n-th row. An excerpt is presented in Figure 1.

We now introduce some of the more striking patterns among the coefficients.

Remark 3.4. For all sufficiently large $n \geq 0$ we have

$$h_{n,d_n} = \begin{cases} 2 & n \equiv 0, 1 \bmod 3 \\ 1 & n \equiv 2 \bmod 3 \end{cases}.$$

In other words, the last entry of each row follows a recurring 1, 2, 2 pattern. This follows from Theorem 1.1 alongside direct computations. We also give an example of a linear quasipolynomial.

$$h_{n,d_n-1} = \tfrac{1}{3}(n+8) \qquad \text{for all } n \equiv 4 \bmod 6, n \geq 34.$$

Notation 3.5. We introduce notation that will be used throughout the rest of the paper.

$$\begin{aligned} b_n &: \text{ the unique integer in } \{0,1,2\} \text{ such that } n \equiv b_n \bmod 3 \\ kA &: \text{ the set } \{x_1 + x_2 + \cdots + x_k : x_i \in A\} = A + A + \cdots + A \\ P(\alpha) &: \text{ the set } \{(y, \alpha - y) \in \mathbb{Z}^2_{\geq 1} : 1 \leq y < \alpha - y\} \\ p_n(k) &: \text{ the integer } b_n - 2k - 1 \\ X_n &: \text{ the set } \left(\frac{n}{3}, \frac{n}{2}\right) \cap \mathbb{Z}. \end{aligned}$$

Example 3.6. The set kA can be thought of as the set of integers that can be summed to by k (not necessarily distinct) elements of A. The notation $P(\cdot)$ will generally be used with input $b_n - \alpha$ and is first used in Theorem 5.5. For example,

$$P(8) = \{(1,7),(2,6),(3,5)\}.$$

In other words $P(\alpha)$ is the set of ordered pairs of positive integers that sum to α such that the first element is strictly lesser. The notation $p_n(k)$ will be used as a lower bound in Theorem 5.15. Each X_n is one of the sets counted by h_{n,d_n}.

We now overview some preliminary results on the value of $h_{n,i}$. Since the following conditions occur many times later in the paper, we give them a name.

Definition 3.7. Fix a set A. We say A *works* for n if

- $n \notin \langle A \rangle$;
- $x < n/2$ for all $x \in A$;
- A minimally generates a numerical semigroup.

In other words, $h_{n,i}$ counts sets of size i that work for n. We say A is *strongly n-bounded* if $n/4 < x < n/2$ for all $x \in A$.

4. Quasipolynomial Pattern/Motivating Overview

When we computed values of $h_{n,i}$, we noticed a pattern. For large n, the k-th to last entry of each row formed a quasipolynomial of degree k. What is meant by this is that the last coefficient of each row forms a periodic sequence, the second to last form a quasilinear function of n, the third to last coefficient are quasiquadratic, etc. In particular, the formulas in Figure 2 hold for all known coefficients for all sufficiently large n. Moreover, the value of n where the formulas begin to hold appear to follow an arithmetic pattern: the formula for h_{n,d_n-k} is valid for $n \geq 24k + c_n$ where c_n is a constant depending only on n modulo 6. In this section and the next, we develop theory that explains the above two phenomena, both of which are encapsulated by the recurrence relation in Theorem 1.1.

To motivate the numerous definitions and lemmas introduced later, we provide an overview of how the proof developed behind the scenes. The first question we tackled was an explanation for why

$$h_{n,d_n} = \begin{cases} 2 & n \equiv 0,1 \bmod 3 \\ 1 & n \equiv 2 \bmod 3 \end{cases}. \tag{4.1}$$

In other words, an explanation for why the final entry of each row forms a 1-2-2 pattern.

We first noticed that the set X_n was always counted by h_{n,d_n}. Then, from the form of h_{n,d_n} given in (4.1), we had to answer two questions:

- what is the extra set that is counted by h_{n,d_n} for $n \equiv 0,1 \bmod 3$, and
- why is there no extra set that is counted by h_{n,d_n} for $n \equiv 2 \bmod 3$?

Before proceeding, let us denote $E_{0,n}$ as the extra set counted by h_{n,d_n} for $n \equiv 0 \bmod 3$ and likewise for $E_{1,n}$.

We knew that the set X_n is counted by h_{n,d_n} for every n as proven in [2]. Also, it felt intuitive that small changes to X_n would result in small changes to its additive structure, i.e. for integers x that are close to X_n (i.e. $|X_n - x|$ is close to 0), the semigroup $\langle X_n \cup \{x\}\rangle$ should not be too different from $\langle X_n\rangle$. For these reasons, we attacked the problem of finding sets counted by h_{n,d_n-k} by constructing sets from X_n.

We remark that for all n,

$$X_n = \left\{ \left\lfloor \frac{n}{3} \right\rfloor + 1, \left\lfloor \frac{n}{3} \right\rfloor + 2, \dots, \left\lfloor \frac{n}{3} \right\rfloor + d_n \right\}. \tag{4.2}$$

Since X_n contains every integer in the interval $(n/3, n/2)$, if we wanted to construct counted sets from X_n, we could only adjoin elements from $\{1, 2, \dots, \lfloor n/3 \rfloor\}$ to X_n. Thus we thought of $\lfloor n/3 \rfloor$ as a sort of cutoff point. From this, it felt natural to express sets in terms of how offset the elements are from $\lfloor n/3 \rfloor$. This motivates the following.

Definition 4.1. The *offset form* of a set $A = \{x_1, x_2, \dots, x_k\}$ is the set

$$A_{(n)} = \{x_1 - \lfloor n/3 \rfloor, x_2 - \lfloor n/3 \rfloor, \dots, x_k - \lfloor n/3 \rfloor\} = A - \lfloor n/3 \rfloor.$$

Remark 4.2. We then computed some sets that were counted by h_{n,d_n} and noticed that if we expressed the sets in offset form, they were always the same. An obvious first example if the set X_n since it is always counted by h_{n,d_n}. From (4.2), we see that

$$(X_n)_{(n)} = \{1, 2, \dots, d_n\}$$

for all n. More notably, we noticed that for all sufficiently large n, we have

$$(E_{0,n})_{(n)} = \{-1, 1, 3, 4, \dots, d_n\}$$
$$(E_{1,n})_{(n)} = \{0, 2, 3, \dots, d_n\}.$$

To demonstrate this more concretely, one may compute that

$$E_{0,30} = \{9, 11, 13, 14\}$$
$$E_{0,36} = \{11, 13, 15, 16, 17\}.$$

Taking the offset form, we have:

$$(E_{0,30})_{(30)} = \{-1, 1, 3, 4\}$$
$$(E_{0,36})_{(36)} = \{-1, 1, 3, 4, 5\}.$$

After expressing the sets we computed in offset form, we noticed that we could go one step further. We noticed that if we instead expressed sets in terms of how different they are from X_n and then take the offset form of the result, the expressions would be equal. This motivates the following.

Definition 4.3. Let n be the integer implicitly declared throughout the paper. A set $I \subseteq \mathbb{Z}$ is an *inserting set* for n if

$$I_{(n)} \subseteq \{-\lfloor n/3 \rfloor, \dots, -1, 0\},$$

and a set $R \subseteq \mathbb{Z}$ is a *removing set* for n if

$$R_{(n)} \subseteq \{1, 2, \dots, d_n\}.$$

An ordered pair (R, I) is an *RI-pair* for n if R is a removing set and I is an inserting set.

There is a natural bijection between RI-pairs for n and the powerset of $\{1, 2, \dots, d_n\}$ given by the map, denoted φ_n, such that

$$(R, I) \mapsto (X_n \setminus R) \cup I.$$

The inverse map is given by

$$A \mapsto (X_n \setminus A, A \setminus X_n).$$

Since φ_n gives a bijection between the two objects, we say the set *corresponding to* an RI-pair (R, I) is the set $\varphi_n(R, I)$, and vice-versa.

Remark 4.4. Definition 4.3 makes precise the notion of "constructing sets from X_n". An inserting set is simply the set of elements we want to insert into X_n, and a removing set is simply the set of elements we want to remove from X_n.

Since there is a bijection between RI-pairs and sets potentially counted by $h_{n,i}$, we can rephrase our goal as counting RI-pairs, which turn out to be much easier to analyze, as demonstrated by Theorem 5.5.

From the fact that R and I must be disjoint, we have $|\varphi_n(R, I)| = d_n - |R| + |I|$.

Example 4.5. In order to build intuition, we first demonstrate the notion of an RI-pair before applying it to our ongoing example of $E_{0,n}$ and $E_{1,n}$.

Let $n = 43$ and let $A = \{6, 9, 20\}$. We will find the RI-pair corresponding to A, then express it in offset form.

We use the inverse map given by

$$A \mapsto (X_n \setminus A, A \setminus X_n).$$

We see that

$$X_n = \{15, 16, 17, 18, 19, 20, 21\}.$$

Therefore we have

$$(R, I) = (\{15, 16, 17, 18, 19, 21\}, \{6, 9\}).$$

Expressed in offset form, we have

$$(R_{(n)}, I_{(n)}) = (\{1, 2, 3, 4, 5, 7\}, \{-8, -5\})$$

since $\lfloor n/3 \rfloor = 14$.

Example 4.6. We now apply Definition 4.3 to our ongoing example of $E_{0,n}$ and $E_{1,n}$. Let $(R_{0,n}, I_{0,n})$ and $(R_{1,n}, I_{1,n})$ be the RI-pairs corresponding to $E_{0,n}$ and $E_{1,n}$, respectively. From the expressions in Remark 4.2 we deduce that when expressed in offset form, we have

$$(R_{0,n})_{(n)} = \{2\} \qquad (I_{0,n})_{(n)} = \{-1\}$$
$$(R_{1,n})_{(n)} = \{1\} \qquad (I_{1,n})_{(n)} = \{0\}.$$

Note that this holds for all n. Thus, the main pattern we noticed was that for all sufficiently large n, the extra set counted by h_{n,d_n} for $n \equiv 0 \bmod 3$ and $n \equiv 1 \bmod 3$ was always of the form

$$E_{0,n} = X_n \setminus \{\lfloor n/3 \rfloor + 2\} \cup \{\lfloor n/3 \rfloor - 1\}$$
$$E_{1,n} = X_n \setminus \{\lfloor n/3 \rfloor + 1\} \cup \{\lfloor n/3 \rfloor\}.$$

In order to illustrate this more concretely, let $(R_{0,30}, I_{0,30})$ and $(R_{0,36}, I_{0,36})$ be the RI-pairs that correspond to $E_{0,30}$ and $E_{0,36}$, respectively. Then, we see that

$$R_{0,30} = \{12\} \qquad I_{0,30} = \{9\}$$
$$R_{0,36} = \{14\} \qquad I_{0,36} = \{11\}$$

and thus we conclude that

$$E_{0,30} = X_{30} \setminus \{12\} \cup \{9\}$$
$$E_{0,36} = X_{36} \setminus \{14\} \cup \{11\}.$$

Therefore, we have answered the first question of determining the extra set that is counted by $h_{n.d_n}$ for $n \equiv 0, 1 \bmod 3$. We then moved on to the second question of: why doesn't $E_{2,n}$ exist?

To answer this question, we noticed another pattern. When we expressed counted sets in terms of the offset form of the corresponding RI-pair, we noticed that as $\min I$ became smaller, the size of R became larger. This makes intuitive sense in that as we adjoin smaller elements to our generating set, the resulting numerical semigroup will have more elements, meaning a higher chance of having $n \in \langle A \rangle$. This idea motivates Definition 5.6. It turns out that for $n \equiv 2 \bmod 3$, for any non-empty inserting set I with $|I| \geq 1$, we have $|R| \geq 1 + |I|$. Thus, it follows that no set counted by h_{n,d_n} asides from X_n will have size d_n for $n \equiv 2 \bmod 3$. This is proven in Example 5.14.

Now that we had an explanation for pattern (4.1), we extended the argument to coefficients of the form h_{n,d_n-k}. The key observation we noticed was that for a fixed k, we only had to adjoin elements from a fixed interval into X_n to acquire every set counted by h_{n,d_n-k}. More precisely, every set counted by h_{n,d_n-k} had a corresponding RI-pair (R, I) that satisfied $I_{(n)} \subseteq \{0, -1, \ldots, p_n(k)\}$. This is proven in Theorem 5.15. Turns out, it also follows from this that we only had to remove elements from a fixed interval. Together, this means that for a fixed k, if we vary the value of n, all of the sets counted by h_{n,d_n-k} will lie in the same interval when expressed as the offset form of the corresponding RI-pair. Hence, as we vary n, the only thing that varies is the value of d_n. From these facts, the proof of the main theorem follows.

5. Results on RI-pairs that Correspond to Working Sets

In this section, we prove results on the definitions introduced in the previous section.

Proposition 5.1. *For any strongly n-bounded set A, the following are equivalent:*

1. *A works for n;*
2. *$n \notin \langle A \rangle$;*
3. *$n \notin 3A$; and*
4. *$b_n \notin 3A_{(n)}$.*

Proof. (1) $\iff$ (2): If A works for n, then $n \notin \langle A \rangle$ by definition. Conversely, suppose $n \notin \langle A \rangle$. Since A is strongly n-bounded, we have

$$x + y > \frac{n}{2} > z \quad \text{for all } x, y, z \in A.$$

Since no two elements of A sum to another element of A, that means A minimally generates a numerical semigroup, meaning A works for n.

(2) $\iff$ (3): If $n \notin \langle A \rangle$, then $n \notin 3A$ by definition. Conversely, suppose $n \notin 3A$. Since A is strongly n-bounded, we have that

$$x < n < y \quad \text{for all } x \in 2A \text{ and } y \in 4A.$$

Therefore, $n \in \langle A \rangle$ if and only if $n \in 3A$, which means that $n \notin \langle A \rangle$.

(3) $\iff$ (4): Follows from the fact that $n = 3\lfloor n/3 \rfloor + b$. □

The significance of Proposition 5.1 is that if we restrict to only strongly n-bounded sets, we can determine if a set works for n by simply analyzing $3A_{(n)}$. Although the criteria of strong n-boundedness appears to be rather strict, this obstacle is later alleviated by Lemma 6.1. Specifically, if n is sufficiently large (with respect to k), then we can guarantee that every set counted by h_{n,d_n-k} is strongly n-bounded.

Example 5.2. Continuing notation from Section 4, we prove that $E_{0,36}$ works for 36 (as it should be, since it is counted by $h_{36,d_{36}}$). We computed that

$$E_{0,36} = \{11, 13, 15, 16, 17\}.$$

Since $E_{0,36}$ is strongly 36-bounded, we simply need to show that $0 \notin 3(E_{0,36})_{(36)}$. We have

$$(E_{0,36})_{(36)} = \{-1, 1, 3, 4, 5\}.$$

We will later develop methods to show that $0 \notin 3\{-1, 1, 3, 4, 5\}$. For now, it is not hard to convince oneself that it is true.

We now provide an equivalent condition for an RI-pair to correspond to a set A such that $b_n \notin 3A_{(n)}$. This condition will prove to be much easier to work with. In particular, this condition follows from a classification of every way for three integers to sum to $b_n \in \{0, 1, 2\}$.

Lemma 5.3. *Let $b_n \in \{0, 1, 2\}$. Fix integers $\alpha \leq y \leq z$ such that $\alpha + y + z = b_n$ such that not all of b_n, y, z equal 0. Then, we have that $\alpha \leq 0$ and that (y, z) must take on exactly one of the following forms:*

1. *(Form 1) $(\alpha, b_n - 2\alpha)$;*
2. *(Form 2) $((b_n - \alpha)/2, (b_n - \alpha)/2)$ where $\alpha \equiv b_n \bmod 2$;*
3. *(Form 3) $(\beta, b_n - \alpha - \beta)$ where $\beta \leq 0$ and $\alpha \neq \beta$; or*
4. *(Form 4) $(y, b_n - \alpha - y)$ where $1 \leq y < b_n - \alpha - y$.*

Proof. Since $b_n \in \{0, 1, 2\}$, we must have $\alpha \leq 0$ as α, y, z are each integers where α is the smallest of the three.

Let $S = \{\alpha, y, z\}$. We see that either $|S| = 2$ or $|S| = 3$. We see that $|S| \neq 1$ as the only case of that occurring is if $\alpha = y = z = b_n = 0$, which we discarded in the hypothesis of the statement of the claim.

Additionally, we see that either 1 or 2 of α, y and z must be less than or equal to 0. We cannot have 3 as the only case of that is again $\alpha = y = z = b_n = 0$. Therefore we have either $\alpha \leq y \leq 0$ and $z > 0$ or $\alpha \leq 0$ and $y, z > 0$. We split into these four cases.

Suppose $|S| = 2$. If $\alpha \leq y \leq 0$ and $z > 0$, then we must have $y = \alpha$, which corresponds to Form 1.

Otherwise, $\alpha \leq 0$ and $y, z > 0$, so we must have $y = z$, which corresponds to Form 2.

Suppose $|S| = 3$. If $\alpha \leq y \leq 0$ and $z > 0$, then we must have $\alpha \neq y$, which corresponds to Form 3.

Otherwise, $\alpha \leq 0$ and $y, z > 0$, so we must have $y \neq z$, which corresponds to Form 4.

It is easy to check that each of these forms are distinct. □

Lemma 5.4. *Let A be a set with a corresponding RI-pair (R, I). Then $n \notin 3A$ if and only if for all $\alpha \in I_{(n)}$ and all $y, z \in (X_n \cup I)_{(n)}$ such that $x + y + z = b_n$, we have either $y \in R_{(n)}$ or $z \in R_{(n)}$.*

Proof. The statement $n \notin 3A$ is equivalent to $b_n \notin 3A_{(n)}$, so we prove the claim with the latter statement.

$(\implies)$: Suppose for the sake of contradiction that $b_n \notin 3A_{(n)}$ and suppose that there exists $\alpha \in I_{(n)}$ and $y, z \in (X_n \cup I)_{(n)}$ that satisfy $\alpha + y + z = b_n$ such that $y, z \notin R_{(n)}$. Since $y, z \notin R_{(n)}$ and $\alpha \in I_{(n)}$, that means that $x, y, z \in A_{(n)}$ since $A = (X_n \setminus R) \cup I$. Since $x + y + z = b_n$, this contradicts with the fact that $b_n \notin 3A_{(n)}$.

($\Longleftarrow$) : Suppose for the sake of contradiction that $b_n \in 3A_{(n)}$ and that for all $\alpha \in I_{(n)}$ and all $y, z \in (X_n \cup I)_{(n)}$, we have either $y \in R_{(n)}$ or $z \in R_{(n)}$. Since $b \in 3A_{(n)}$, that means that $x + y + z = b_n$ for some $x, y, z \in A_{(n)}$. We also have

$$A_{(n)} = ((X_n)_{(n)} \setminus R_{(n)}) \cup I_{(n)} = ((X_n)_{(n)} \cup I_{(n)}) \setminus R_{(n)}$$

because $I_{(n)}$ and $R_{(n)}$ are disjoint. Together, that means that there exists $x, y, z \in (X_n \cup I)_{(n)}$ such that $x + y + z = b$ from basic set theoretic arguments. That means that either $y \in R_{(n)}$ or $z \in R_{(n)}$ by hypothesis. This contradicts with the fact that $y, z \in A_{(n)}$. $\square$

Theorem 5.5. *Let A be a set with a corresponding RI-pair (R, I). Then $n \notin 3A$ if and only if for all $\alpha \in I_{(n)}$ the following hold:*

(i) $b_n - 2\alpha \in R_{(n)}$;
(ii) $(b_n - \alpha)/2 \in R_{(n)}$ if $\alpha \equiv b$ mod 2;
(iii) $b_n - \alpha - \beta \in R_{(n)}$ for all $\beta \in I_{(n)}$ not equal to α; and
(iv) $y \in R_{(n)}$ or $z \in R_{(n)}$ for all $(y, z) \in P(b_n - \alpha)$.

Proof. Lemma 5.4 asserts $n \notin 3A$ if and only if for all $\alpha \in I_{(n)}$ and $y, z \in (X_n \cup I)_{(n)}$ such that $\alpha + y + z = b_n$, we have either y or z in $R_{(n)}$. Lemma 5.3 classifies every way for three integers to sum to b_n. Applying it to this case, we see that each of Form 1, Form 2, Form 3, and Form 4 corresponds to precisely each of the conditions given in the statement of the claim. $\square$

Theorem 5.5 provides an equivalent, but much easier to work with condition than $n \notin 3A$. Thus we give the condition a name.

Definition 5.6. An *RI*-pair (R, I) is *compatible* for n if (R, I) satisfies the conditions given in Theorem 5.5. We say in this case that R is *compatible with I*.

We define the *removal degree* of an inserting set I, denoted $r(I)$, as

$$r(I) = \min\{|R| : (R, I) \text{ is compatible}\}.$$

Similarly, we define the *removal degree* of an integer $\alpha \leq 0$ as

$$r(\alpha) = r(J)$$

where J is the inserting set such that $J_{(n)} = \{\alpha\}$.

Remark 5.7. Although the definition of "compatible" technically needs to depend on b_n, this will not prove to be a problem as we will always be working with a fixed residue class mod 3, meaning b_n will always be fixed from the implicit integer n that is declared throughout the paper.

Remark 5.8. Given an inserting set I, Theorem 5.5 provides a systematic way to construct a removing set R such that the set A corresponding to (R, I) satisfies $n \notin 3A$. This will be explored in Example 5.10. Moreover, the theorem admits a better-than-brute-force method of computing h_{n,d_n-k}, which we make explicit in Algorithm 7.3.

Intuitively, given a set of integers I that we want to adjoin to X_n, Theorem 5.5 provides a method to systematically determine which elements R from X_n we must remove in order to have $n \notin 3A$ where A is the set corresponding to (R, I). Therefore later in the paper, we often will informally refer to this inserting and removing notion when applying Theorem 5.5. Most applications of the theorem will involve starting with a set $R = \emptyset$ and systematically putting elements into R. Additionally, we will refer to items 1-4 of Theorem 5.5 when explaining which elements we must put into R given an inserting set I. We provide examples that exemplify this notion.

Example 5.9. Continuing from Example 5.2, we now prove that $0 \notin 3(E_{0,36})_{(36)}$. Theorem 5.5 asserts that the above is equivalent to showing that (R, I) is compatible where (R, I) is the RI-pair corresponding to $E_{0,36}$. From Example 4.6, we have that

$$R_{(36)} = \{2\} \qquad\qquad I_{(36)} = \{-1\}.$$

We now check the four items of Theorem 5.5 for (R, I). Let $\alpha = -1$.

From Theorem 5.5(i), we must have $b_n - 2\alpha = 0 - 2(-1) = 2 \in R_{(n)}$, which is indeed satisfied.

From Theorem 5.5(ii), since $\alpha \neq b_n \bmod 2$, we have nothing to check.

From Theorem 5.5(iii), since there are no other elements of $I_{(n)}$, we have nothing to check.

From Theorem 5.5(iv), we have $P(b_n - \alpha) = \emptyset$, thus we have nothing to check.

Therefore, (R, I) is indeed compatible, meaning $0 \notin 3(E_{0,36})_{(36)}$. Since $E_{0,36}$ is strongly 36-bounded, that means the set works for 36. Since $|R| = |I|$, that means that $|E_{0,36}| = d_{36}$. Together, that means $E_{0,36}$ is counted by $h_{36,d_{36}}$.

Example 5.10 provides a basis for how Algorithm 7.3 works, as well as intuition for several upcoming proofs.

Example 5.10. Suppose $n = 60$ and we wanted to adjoin $I = \{17, 18\}$ to X_n. Theorem 5.5 provides a systematic method of constructing a removing set R such that $n \notin 3\varphi_n(R, I)$. Since $I > n/4$, the resulting set will be strongly n-bounded. This implies the resulting set will work for n.

We check every item of Theorem 5.5 with every element $\alpha \in I_{(n)}$ to construct $R_{(n)}$.

We first compute the offset form

$$I_{(n)} = \{-3, -2\}$$

and initialize $R_{(n)} = \emptyset$. Note that $b_n = b_{60} = 0$ since $60 \equiv 0 \bmod 3$.

- Let $\alpha = -2$. From Theorem 5.5(i), we must put $b_n - 2\alpha = 4$ into R. From Theorem 5.5(ii), since $\alpha \equiv b_n \bmod 2$, we must put $(b_n - \alpha)/2 = 1$ into R. From Theorem 5.5(iii), the only case is $\beta = -3$, so we put $b_n - \alpha - \beta = 5$ into R. We deal with Theorem 5.5(iv) later. We conclude this iteration with $R_{(n)} = \{1, 4, 5\}$.

- Let $\alpha = -3$. From Theorem 5.5(i), we must put $b_n - 2\alpha = 6$ into R. From Theorem 5.5(ii), since $\alpha \not\equiv b_n \bmod 2$, we do not put anything into R. From Theorem 5.5(iii), the only case is $\beta = -2$ which we have already dealt with. We again deal with Theorem 5.5(iv) later. We conclude this iteration with $R_{(n)} = \{1, 4, 5, 6\}$.

We now deal with Theorem 5.5(iv). We see that

$$P(b_n - 2) = \emptyset$$
$$P(b_n - 3) = \{(1, 2)\}.$$

The pair $(1, 2)$ is the only pair we must consider. We already have $1 \in R_{(n)}$, thus we do nothing.

We are now finished with the criteria of compatibility. Therefore, we conclude that the RI-pair

$$R_{(n)} = \{1, 4, 5, 6\} \implies R = \{21, 24, 25, 26\}$$
$$I = \{17, 18\}$$

corresponds to a set that works for 60. We compute the corresponding set

$$A = \varphi_{60}(R, I) = \{17, 18, 22, 23, 27, 28, 29\}.$$

Lemma 5.11. *We have*

$$r(\alpha) = 1 + \delta(\alpha, b_n) + \left\lfloor \frac{b_n - \alpha - 1}{2} \right\rfloor$$

for any integer $\alpha \leq 0$.

Proof. The proof follows from performing the same process used in Example 5.10 on the single element set $\{\alpha\}$. A subtle note is the fact that each item of Theorem 5.5 guarantees a unique element to put into $R_{(n)}$ from the distinctness of forms in Lemma 5.3. We elaborate below.

Fix $\alpha \leq 0$, let $I = \{\alpha\}$, and suppose R is a removing set that is maximally compatible with I. We must show that

$$|R| = 1 + \delta(\alpha, b_n) + \left\lfloor \frac{b_n - \alpha - 1}{2} \right\rfloor.$$

The set R must satisfy all four items of Theorem 5.5 as it is compatible. Additionally, the set R must not contain any element not specified by an item of Theorem 5.5 because it is maximally compatible.

We initialize $R_{(n)} = \emptyset$. For each item of the theorem, we will add elements into $R_{(n)}$. Since each item guarantees distinct elements from the distinctness of forms in Lemma 5.3, $|R|$ increases by exactly the number of elements added at each item.

- From Theorem 5.5(i), we must have $b_n - 2\alpha \in R_{(n)}$. Therefore $|R| = 1$.

- From Theorem 5.5(ii), we must have $(b_n - \alpha)/2 \in R_{(n)}$ if $\alpha \equiv b \bmod 2$. Therefore $|R| = 1 + \delta(\alpha, b_n)$.
- From Theorem 5.5(iii), we remove nothing else since there is no $\beta \in I_{(n)}$ not equal to α.
- From Theorem 5.5(iv), we remove $|P(b_n - \alpha)|$ elements.

Therefore,

$$|R| = 1 + \delta(\alpha, b_n) + |P(b_n - \alpha)| = 1 + \delta(\alpha, b_n) + \left\lfloor \frac{b_n - \alpha - 1}{2} \right\rfloor,$$

as desired. □

Example 5.12. Let $n = 30$. Suppose we want to construct a working set by adjoining an element $x = 9$ into the set $X_n = \{11, 12, 13, 14\}$. What is the minimum number of elements that must be removed so that the resulting set works for n?

We apply Lemma 5.11 to answer our question. We have that the corresponding value for α is $\alpha = -1$ because if $J = \{x\} = \{9\}$, then $J_{(n)} = \{-1\}$. Applying the formula given in the lemma, we have

$$r(\alpha) = 1 + \delta(-1, b_n) + \left\lfloor \frac{0 - (-1) - 1}{2} \right\rfloor = 1.$$

Note that $b_n = 0$ since $n \equiv 0 \bmod 3$. Although the formula does not tell us what elements we must remove, we can instead use Theorem 5.5, which tells us that we must remove 12. Therefore the set

$$\{11, 12, 13, 14\} \setminus \{12\} \cup \{9\} = \{9, 11, 13, 14\}$$

works for 30. This precisely matches with our previous discussions on $E_{0,30}$.

Lemma 5.13. *If $n \notin 3A$, then we have*

$$|A| \leq d_n + 1 - r(m)$$

where $m = \min I_{(n)}$ and (R, I) is the RI-pair corresponding to A.

Proof. Since $n \notin 3A$, (R, I) is compatible. Let $m = \min I_{(n)}$. Let J be the set such that $I_{(n)} = \{m\} \cup J_{(n)}$. Similar to the proof of Lemma 5.11, since (R, I) is compatible, we will check that it satisfies the four items of Theorem 5.5. Initialize $Q_{(n)} = \emptyset$. Let $\alpha = m$. From the distinctness of forms in Lemma 5.3, $|Q|$ increases by exactly the number of elements added at each item, but only for a single iteration of $\alpha \in I_{(n)}$.

- From Theorem 5.5(i), we must have $b_n - 2\alpha \in Q_{(n)}$. Therefore $|Q| = 1$.
- From Theorem 5.5(ii), we must have $(b_n - \alpha)/2 \in Q_{(n)}$ if $\alpha \equiv b_n \bmod 2$. Therefore $|Q| = 1 + \delta(\alpha, b_n)$.
- From Theorem 5.5(iii), we remove $|J|$ elements as $J_{(n)}$ is the set of elements of $I(n)$ not equal to m. Therefore $|Q| = 1 + \delta(\alpha, b_n) + |J|$
- From Theorem 5.5(iv), we remove $|P(b_n - \alpha)|$ things.

Hence at the end of this iteration, we have

$$|Q| = r(m) + |J| = r(m) + |I| - 1.$$

Since this procedure will only increase the size of Q, and since R must be constructed by this procedure, we have that

$$|R| \geq |Q| = r(m) + |I| - 1.$$

Therefore,

$$|A| = d_n + |I| - |R| \geq d_n + |I| - r(m) - |I| + 1 = d_n + 1 - r(m),$$

as desired. □

Example 5.14. Fix $n \equiv 2 \bmod 3$. Continuing from Section 4, we prove here that no additional set counted by h_{n,d_n}, denoted $E_{2,n}$, exists.

Fix $n \equiv 2 \bmod 3$. Let A be a set that works for n with a corresponding RI-pair (R, I) such that $A \neq X_n$. Denote $m = \min I_{(n)}$. From Lemma 5.13 we have

$$\begin{aligned} |A| &\leq d_n + 1 - r(m) \\ &= d_n + 1 - \left(1 + \delta(m,2) + \left\lfloor \frac{2-m-1}{2} \right\rfloor\right) \\ &= d_n - \delta(m,2) - \left\lfloor \frac{2-m-1}{2} \right\rfloor. \end{aligned}$$

Suppose $m \leq -2$. Then we have

$$\begin{aligned} |A| &\leq d_n - d(m,2) - \left\lfloor \frac{2-m-1}{2} \right\rfloor \\ &\leq d_n - \left\lfloor \frac{2-(-2)-1}{2} \right\rfloor \\ &= d_n - 1, \end{aligned}$$

meaning A is not counted by h_{n,d_n}.

Suppose $m = -1$. Then we have

$$\begin{aligned} |A| &\leq d_n - d(-1,2) - \left\lfloor \frac{2+1-1}{2} \right\rfloor \\ &= d_n - 1, \end{aligned}$$

meaning A is not counted by h_{n,d_n}.

Suppose $m = 0$. Then we have

$$\begin{aligned} |A| &\leq d_n - d(0,2) - \left\lfloor \frac{2-1}{2} \right\rfloor \\ &= d_n - 1, \end{aligned}$$

meaning A is not counted by h_{n,d_n}.

Since $\min I_{(n)} \leq 0$ by definition, we have exhausted every case. Therefore, no set asides from X_n is counted by h_{n,d_n} for $n \equiv 2 \bmod 3$.

Theorem 5.15. *Let $k \geq 0$ be an integer. If A is a set that satisfies $|A| \geq d_n - k$ and $n \notin 3A$, then*

$$I_{(n)} \subseteq \{p_n(k), p_n(k)+1, \ldots, -1, 0\}$$

where (R, I) is the RI-pair corresponding to A.

Proof. Suppose A satisfied $|A| \geq d_n - k$ and $n \notin 3A$. Denote $m = \min I_{(n)}$ where I is the corresponding inserting set. By Lemma 5.13, we have

$$d_n - k \leq |A| \leq d_n + 1 - r(m).$$

Therefore $-k \leq 1 - r(m)$ which is equivalent to $k \geq r(m) - 1$.

Our goal is to solve for m. From Lemma 5.11, we expand $r(m)$ to get

$$\begin{aligned} k &\geq 1 + \delta(m, b_n) + \left\lfloor \frac{b_n - m - 1}{2} \right\rfloor - 1 \\ &= \delta(m, b) + \frac{b_n - m - 1 - \delta(m, b_n)}{2} \\ &= \frac{1}{2}\left(\delta(m, b_n) + b_n - m - 1\right). \end{aligned}$$

With algebraic manipulations, we arrive at

$$m \geq \delta(m, b_n) + b_n - 2k - 1 \geq -2k - 1 + b_n = p_n(k),$$

meaning $\min I_{(n)} \geq p_n(k)$.

□

6. Proof of Main Results

With the results on RI-pairs developed, we now prove the main theorem and Corollary 1.2.

Lemma 6.1. *If $n > 24k + 12 - 8b_n$, then every set counted by h_{n,d_n-k} is strongly n-bounded.*

Proof. Let A be a set counted by h_{n,d_n-k} and let (R, I) be its corresponding RI-pair. From Theorem 5.15 we have

$$\min I_{(n)} \geq p_n(k).$$

From the above inequality, the sets A that correspond to RI will have $\min A \geq p_n(k) + \lfloor n/3 \rfloor$. Since we want $\min A > n/4$ for the set to be strongly n-bounded, we shall solve for n in the inequality $p_n(k) + \lfloor n/3 \rfloor > n/4$.

We see that

$$\begin{aligned} p_n(k) + \left\lfloor \frac{n}{3} \right\rfloor > \frac{n}{4} &\iff -2k - 1 + b_n + \left\lfloor \frac{n}{3} \right\rfloor > \frac{n}{4} \\ &\iff -2k - 1 + b_n + \frac{n - b_n}{3} > \frac{n}{4} \\ &\iff \frac{n}{12} > 2k + 1 - \frac{2}{3} b_n \\ &\iff n > 24k + 12 - 8b_n. \end{aligned}$$

□

Corollary 6.2. *For $n > 24k + 12 - 8b_n$, the sets counted by $h_{n,d(n)-k}$ have a corresponding inserting set I that satisfies $\min I_{(n)} \geq p_n(k)$. In particular, the lower bound is independent of n.* □

We now have enough machinery to prove the main theorem and Corollary 1.2.

Proof of Main Theorem. First, we denote $n\mathcal{RI}$ as the set of all RI-pairs with n as the implicit integer. We denote

$$n\mathcal{RI}_{m_1,m_2} = \left\{ (R, I) \in n\mathcal{RI} : I_{(n)} \subseteq \{0, -1, \dots, m_1\} \text{ and } R_{(n)} \subseteq \{1, 2, \dots, m_2\} \right\}.$$

Let n and m be integers that satisfy $n \equiv m \bmod 3$ and $n \geq m > 24k + 12 - 8b_n$. Denote $\mathcal{S}_k$ as the set of k-subsets of $\{d_m + 1, d_m + 2, \dots, d_n\}$.

We prove the claim combinatorially. We show that there is a bijection between

$$\mathcal{A} := \{A : A \text{ is counted by } h_{n,d_n-k}\}$$

and

$$\mathcal{B} := \bigcup_{l=0}^{k} \left(\{A : A \text{ is counted by } h_{m,d_m-l}\} \times \mathcal{S}_{k-l} \right).$$

From Lemma 6.1, the sets we count in $\mathcal{A}$ and $\mathcal{B}$ will be strongly n-bounded and strongly m-bounded, respectively. From Theorem 5.15 and the fact that the lower bound on I is independent of value in the same residue class mod 3, it is sufficient to find a bijection $f : \mathcal{A}' \to \mathcal{B}'$ where

$$\mathcal{A}' = \#\{(R, I) \in n\mathcal{RI}_{p_m(k),d_n} : (R, I) \text{ is compatible}, |R| - |I| = k\}$$

$$\mathcal{B}' = \#\bigcup_{l=0}^{k} \left(\{(R, I) \in m\mathcal{RI}_{p_m(k),d_m} : (R, I) \text{ is compatible}, |R| - |I| = l\} \times S_{k-l} \right).$$

This is sufficient because

$$|\mathcal{A}'| = h_{n,d_n-k}$$

$$|\mathcal{B}'| = \sum_{l=0}^{k} h_{m,d_m-l} \binom{d_n - d_m}{k - l}.$$

To define f, for every $(R, I) \in \mathcal{A}'$, we split R into R_1 and R_2 such that

$$(R_1)_{(n)} = \{\alpha \in R_{(n)} : 1 \leq \alpha \leq d_m\}$$
$$(R_2)_{(n)} = \{\alpha \in R_{(n)} : d_m + 1 \leq \alpha \leq d_n\}.$$

With this splitting, we define f as

$$(R, I) \mapsto ((R_1, I), R_2) \text{ for all } (R, I) \in \mathcal{A}'.$$

We first show that f is well-defined. Denote $l = |R_1| - |I|$. In particular, we must show that

- (R_1, I) is compatible;
- $l \leq k$; and
- $R_2 \in \mathcal{S}_{k-l}$.

The key to showing that (R_1, I) is compatible is from the fact that for a given inserting set J, the largest element that the four bullets of Theorem 5.5 requires to be in the removing set is $b_n - 2 \min J_{(n)}$. What this means is that if an RI-pair (Q, J) is compatible, then $(Q \setminus \{x + \lfloor n/3 \rfloor\}, J)$ is also compatible for all $x > b_n - 2 \min J_{(n)}$. Since the statement of Theorem 5.5 enacts criteria only on the offset form of RI-pairs, that means we can effectively disregard the fact that $\mathcal{A}'$ takes RI-pairs from $n\mathcal{RI}$ while $\mathcal{B}'$ takes RI-pairs from $m\mathcal{RI}$. Since $(R_1)_{(n)}$ can be constructed by iteratively removing elements $x > d_m$ from $R_{(n)}$, it is sufficient to show that $d_m \geq b_n - 2p_n(k)$. From Lemma 6.1, h_{m,d_m-k} counts only strongly m-bounded sets. Hence, we have that

$$\min I > \frac{m}{4}.$$

Following a chain of equivalent inequalities, we have

$$\begin{aligned}
m - 2\min I < \frac{m}{2} &\iff m - 2\left(\min I_{(n)} + \left\lfloor \frac{m}{3} \right\rfloor\right) < \frac{m}{2} \\
&\iff m - 2\left(p_n(k) + \left\lfloor \frac{m}{3} \right\rfloor\right) < \frac{m}{2} \\
&\iff m - 2p_n(k) - 2\left\lfloor \frac{m}{3} \right\rfloor < \frac{m}{2} \\
&\iff m - 2p_n(k) - 3\left\lfloor \frac{m}{3} \right\rfloor < \frac{m}{2} - \left\lfloor \frac{m}{3} \right\rfloor \\
&\iff \left(m - 3\left\lfloor \frac{m}{3} \right\rfloor\right) - 2p_n(k) < \frac{m}{2} - \left\lfloor \frac{m}{3} \right\rfloor \\
&\iff b_m - 2p_n(k) < \frac{m}{2} - \left\lfloor \frac{m}{3} \right\rfloor < d_m \\
&\iff b_n - 2p_n(k) < \frac{m}{2} - \left\lfloor \frac{m}{3} \right\rfloor < d_m.
\end{aligned}$$

The fact that $l \leq k$ trivially follows from the fact that $|R| = k$ and $|R_1| \leq k$. Similarly, $R_2 \in S_{k-k}$ follows from the fact that R_2 contains only elements in $\{d_m + 1, d_m + 2, \ldots, d_n\}$ and from the fact that $|R_2| = |R| - |R_1| = k - k$.

Hence f is well-defined.

Now, we prove f is injective. Suppose $(A_1, I) \times A_2, (B_1, I) \times B_2 \in \mathcal{B}'$ and that

$$(A_1, I) \times A_2 = (B_1, I) \times B_2.$$

From basic set theory alongside the aforementioned equality, we see that we must have $A_1 = B_1$ and $A_2 = B_2$. Therefore we have that

$$A_1 \cup A_2 = B_1 \cup B_2.$$

This means that

$$(A_1 \cup A_2, I) = (B_1 \cup B_2, I).$$

Therefore f is injective.

Given the injection f defined above, we see that there exists a well-defined inverse map f^{-1} given by

$$((R_1, I), R_2) \mapsto (R_1 \cup R_2, I),$$

which proves that f is bijective. □

Proof of Corollary 1.2. Fix a residue class b_n mod 3 for n, m. Let $m = \min\{x \in \mathbb{Z}_{\geq 0} : x > 24k + 12 - 8b_n\}$. We see that m is constant for a fixed equivalence class $\overline{b}_n \in \mathbb{Z}/3\mathbb{Z}$. That means h_{m,d_m-k} is also constant. Write $c_i = h_{m,d_m-(k-i)}$ as a sequence of constants for $i = 0, \ldots, k$, so that

$$h_{n,d_n-k} = c_0 \binom{d_n - d_m}{0} + c_1 \binom{d_n - d_m}{1} + \cdots + c_k \binom{d_n - d_m}{k}$$

by Theorem 1.1. Since

$$\binom{n}{k} \text{ is a polynomial of degree } k \text{ in } n,$$

we have that

$$h_{n,d_n-k} \text{ is a polynomial of degree } k \text{ in } d_n$$

from the fact that the highest degree term of h_{n,d_n-k} is $\binom{d_n-d_m}{k}$.

Observe that d_n is a linear function if n is fixed mod 6 with leading coefficient 1/6. Since d_n is a linear function if n is fixed mod 6, that means that h_{n,d_n-k} is a degree k quasi-polynomial of period 6.

As for determining the leading coefficient, we see that the highest degree term of the quasi-polynomial is given by

$$h_{m,d_m} \binom{d_n - d_m}{k} = h_{m,d_m} \frac{(d_n - d_m) \cdot (d_n - d_m - 1) \cdots (d_n - d_m - k)}{k!}.$$

Since d_n has a leading coefficient of $1/6$ and since there are k terms in the numerator of the fraction, we have that the leading coefficient is precisely

$$\frac{h_{m,d_m}}{k!6^k},$$

which proves the claim by Remark 3.4. □

Example 6.3. Here we show how to apply the main theorem to determine an expression for h_{n,d_n-3} for all sufficiently large $n \equiv 0 \bmod 3$ and provide the values of n for which the expression is valid.

From the main theorem, we acquire an expression that is valid for

$$n > 24k + 12 - 8b_n = 24 \cdot 3 + 12 - 8 \cdot 0 = 48 + 12 - 16 = 84.$$

Let $m = \min\{x \equiv 0 \bmod 3 : x > 24k + 12 - 8b_n = 84\} = 87$. Appealing to computations, we see that

$$h_{87,d_{87}-0} = 2, \qquad h_{87,d_{87}-1} = 31, \qquad h_{87,d_{87}-2} = 228, \qquad \text{and } h_{87,d_{87}-3} = 1055.$$

Therefore by the main theorem:

$$\begin{aligned} h_{n,d_n-2} = 2 \cdot \binom{d_n - d_{87}}{3} + 31 \cdot \binom{d_n - d_{87}}{2} \\ + 228 \cdot \binom{d_n - d_{87}}{1} + 1055 \cdot \binom{d_n - d_{87}}{0} \end{aligned}$$

for all $n \equiv 0 \bmod 3$ such that $n \geq 87$. We expand binomial coefficients to acquire:

$$h_{n,d_n-3} = \frac{1}{6}(2d_n^3 + 3d_n^2 + 19d_n - 12).$$

We further note that since we consider $n \equiv 0 \bmod 3$, we may write

$$\begin{aligned} d_n &= \left\lfloor \frac{n-1}{2} \right\rfloor - \left\lfloor \frac{n}{3} \right\rfloor \\ &= \begin{cases} \frac{1}{6}n - 1 & n \equiv 0 \bmod 6 \\ \frac{1}{6}n - \frac{1}{2} & n \equiv 3 \bmod 6 \end{cases}. \end{aligned}$$

Substituting into the expression for h_{n,d_n-3}, we arrive at

$$h_{n,d_n-3} = \begin{cases} \frac{1}{648}(n^3 - 9n^2 + 342n - 3240) & n \equiv 0 \bmod 6, n \geq 87 \\ \frac{1}{648}(n^3 + 315n - 2268) & n \equiv 3 \bmod 6, n \geq 90 \end{cases}.$$

We reiterate that these expressions are valid for all $n \geq 87$, which gives us $n \geq 87$ for $n \equiv 0 \bmod 6$ and $n \geq 90$ for $n \equiv 3 \bmod 6$.

Observe that this is already better than what our current computational methods give us! We only have values of h_n computed for $n = 1, 2, \ldots, 90$. Since the polynomial pattern occurs only after $n \geq 87$, this would require us knowing the values of h_{87}, h_{93}, and h_{99} to create the correct cubic polynomial plot fit. Now, we only need to know the value of h_{87}.

Another surprising is that we could have chosen any value for m in place of $\min\{x \equiv 2 \bmod 3 : x > 24k + 12 - 8b_n = 84\} = 87$; as long as $m > 84$, the formula holds even for lesser values of n. For example, if we instead chose $m = 93$ and applied the main theorem, we would acquire the same formula after expanding out binomial coefficients and expanding out d_n by cases.

7. Algorithms and Miscellaneous Remarks

Now that we have a recurrence relation for h_{n,d_n-k}, we return to the question of computing h_{m,d_m-k} where $m = \min\{x \in \mathbb{Z} : x > 24k + 12 - 8b_m\}$. Using the theory developed in Section 5, we provide a better-than-brute-force algorithm to compute h_{n,d_n-k} for $n > 24k + 12 - 8b_n$.

Notation 7.1. Denote

$$\begin{aligned} A(I) &= \{b_n - 2\alpha : \alpha \in I_{(n)}\} \\ B(I) &= \{(b_n - \alpha)/2 : \alpha \in I_{(n)}, \alpha \equiv b_n \bmod 2\} \\ C(I) &= \{b_n - \alpha - \beta : \alpha, \beta \in I_{(n)}, \alpha \neq \beta\} \\ P(I, R) &= \{(x, y) : (x, y) \in P(b_n - \alpha) \text{ for some } \alpha \in I, x \notin R, y \notin R\}. \end{aligned}$$

Remark 7.2. The set $A(I)$ is the set of elements removed from Theorem 5.5(i), the set $B(I)$ is the set of elements removed from Theorem 5.5(ii), the set $C(I)$ is the set of elements removed from Theorem 5.5(iii), and the set $P(I, R)$ is the set of pairs to consider for removal from Theorem 5.5(iv).

Algorithm 7.3. Given $k \geq 0$ and $n > 24k + 12 - 8b_n$, computes, h_{n,d_n-k}. Denote $\mathcal{P}(\cdot)$ as the powerset of a set.

function ComputeCoefficient(n, k)
    $h_{n,d_n-k} \leftarrow 0$
    for all $I \in \mathcal{P}(\{p_n(k), p_n(k) + 1, \ldots, -1, 0\})$ **do**
        $R \leftarrow A(I) \cup B(I) \cup C(I)$
        $R_c \leftarrow \{x \in \mathbb{Z} : 1 \leq x \leq b_n - 2\min I\} \setminus R$
        for all $S \in \mathcal{P}(R_c)$ **do**
            if $x \in S$ or $y \in S$ for all $(x, y) \in P(I, R)$ **then**
                $h_{n,d_n-k} \leftarrow h_{n,d_n-k} + \binom{d_n - (b_n - 2\min I)}{k - |R| - |S| + |I|}$
            end if
        end for
    end for
    return h_{n,d_n-k}
end function

Theorem 7.4. *ComputeCoefficients(n, k) returns* h_{n,d_n-k}.

Proof. In essence, this algorithm is computing

$$h_{n,d_n-k} = \#\{(R,I) \in n\mathcal{RI}_{p_n(k),d_n} : (R,I) \text{ is compatible and } |R| - |I| = k\}$$

with many optimizations where $n\mathcal{RI}_{p_n(k),d_n}$ is defined as in the proof of the main theorem. The bulk of the optimizations is that it uses Theorem 5.5 to determine which elements of X_n must be removed given an inserting set I (see Remark 7.2).

From Theorem 5.15, it is sufficient to iterate through

$$I \in \mathcal{P}(\{p_n(k), p_n(k)+1, \ldots, -1, 0\}).$$

Given I, the first three items of Theorem 5.5 requires R to be a superset of $A(I) \cup B(I) \cup C(I)$. The set R_c is every element not in R that is considered for removal by Theorem 5.5 given the inserting set I (i.e. the integers in $[1, b_n - 2\min I]$). Every subset S of R_c such that $x \in S$ or $y \in S$ for all $(x,y) \in P(I,R)$ lets $(R \cup S, I)$ satisfy Theorem 5.5(iv). Let $l = |R|+|S|-|I|$ be the size of the set that the RI-pair currently corresponds to. If $l > k$, then we do not increment h_{n,d_n-k}, which matches the effect of the binomial coefficient. If $l \le k$, we can freely remove $k-l$ elements from the elements not considered by Theorem 5.5. There are precisely $d_n - (b_n - 2\min I)$ elements not considered by Theorem 5.5. Hence, we increment h_{n,d_n-k} by

$$\binom{d_n - (b_n - 2\min I)}{k-l}.$$

A subtle note that may not be clear is that each iteration of $S \in \mathcal{P}(R_c)$ guarantees sets that have not been counted before. This is due to the fact that the RI-pair is unique among other iterations of

$$I \in \mathcal{P}(\{p_n(k), p_n(k)+1, \ldots, -1, 0\})$$

as no other iteration contains the current value of I; and the RI-pair is unique among other iterations of $S \in \mathcal{P}(R_c)$ due to the fact that we are essentially counting removing sets with

$$(R \cup S) \times (k-l)\text{-subsets of } \{b_n - 2\min I + 1, \ldots, d_n\}.$$

Hence, the second slot guarantees uniqueness. □

Remark 7.5. We make the following remarks about Algorithm 7.3.

(i) The time complexity is $O(2^{4k-b_n})$.

(ii) The only difference in running the algorithm with n and $n+3$ is the value of d_n. Since the value of d_n does not contribute to the dominant term of the time complexity of the algorithm, the time complexity of the algorithm is independent of n in the same residue class $\mathbb{Z}/3\mathbb{Z}$. For example, the algorithm takes 62 ms to compute $h_{90,d_{90}-3}$ and 62 ms to compute $h_{9000,d_{9000}-3}$ on the author's machine.

(iii) A C++ implementation is provided at:
`https://github.com/calvinleng97/senior_thesis_random_nmsg`.

Remark 7.6. When we were first developing the Algorithm 7.3, our original program took in integers $m \leq 0$ and $b \in \{0, 1, 2\}$ and then computed the number of compatible RI-pairs that corresponded to a size k set for every $k \geq 0$ where

$$I_{(n)} \subseteq \{0, -1, \dots, -m\}$$
$$R_{(n)} \subseteq \{1, 2, \dots, b + 2m\}.$$

In other words, we provided the option to choose the lowerbound on $I_{(n)}$ so we could observe what patterns occurred.

Denote $A(m, b)_l$ as the output of the aforementioned algorithm for corresponding sets of size l, let $k = \max\{x \in \mathbb{Z} : p_b(x) \geq m\}$, and let $n = \min\{x \in \mathbb{Z} : x > 24k + 12 - 8b\}$.

Clearly, for all $l \leq k$, $A(m, b)_l = h_{n,d_n - l}$ since the aforementioned algorithm would perform the same task as Algorithm 7.3.

However for some reason, even for $l > k$ we noticed that $A_(m, b)_l$ still matched extremely closely to h_{n,d_n-l}. In fact, it even very closely predicted the value of $h_{n,1}$, and maintained the same unimodal pattern as the n-th row of computations given in the precomputed values of $h_{n,i}$ given in [2].

In other words, if we list outputs like so:

$$A(m, b)_{d_n}, A(m, b)_{d_n-1}, \dots, A(m, b)_2, A(m, b)_1, A(m, b)_0, \tag{7.1}$$

it turns out that (7.1) was an extremely good approximation of the n-th row of the precomputed $h_{n,i}$ values given at the link in Section 1.

We provide an example. For $A(4, 2)$, we have

$$1, 23, 166, 543, 951, 990, 656, 284, 79, 13, 1$$

while the value of the 59-th row of the precomputed $h_{n,i}$ values is

$$1, 28, 228, 733, 1186, 1115, 684, 283, 79, 13, 1.$$

8. Future Work

If we could compute $r(I)$ in polynomial time (with respect to I and $\min I$) given any inserting set I, then we could determine whether an inserting set I will have any removing set R at all from the fact that the corresponding set will have size

$$|A| = d_n + |I| - |R| \leq d_n + |I| - r(I).$$

This could then be used as a check in each iteration of Step 2 in Algorithm 7.3 to quickly determine whether it is necessary to go into the later steps.

Problem 8.1. *Obtain a bound on $r(I)$ for each inserting set I.*

In Algorithm 7.3, we satisfy bullet four of Theorem 5.5 by brute-force (i.e. by iterating through every subset T of S). If we could provide a systematic way of finding valid fixations of $P(I, R)$, then runtimes would be reduced drastically.

Problem 8.2. *Investigate the structure of $P(I, R)$.*

In Section 1, we mentioned the possibility of parallelizing Algorithm 7.3. This is possible as the work can be split for each iteration of $I \in \mathcal{P}(\{p_n(k), p_n(k)+1, \ldots, -1, 0\})$.

Problem 8.3. *Write a parallelized algorithm for Algorithm 7.3.*

Note that in order to determine a formula for h_{n,d_n-k} for a fixed $k \geq 0$ and residue class $\overline{b} \in \mathbb{Z}/3\mathbb{Z}$, one simply needs to run ComputeCoefficients(m, k) with $m = \min\{x : x > 24k + 12 - 8b\}$ (by using the main theorem). As a result, the author compiled a database with many of these values and plugged them into the Online Encyclopedia of Integer Sequences at `https://oeis.org/`. We noticed that the values for $b = 2$ matches very closely to `https://oeis.org/A224274`.

Conjecture 8.4. *If* $m_k = \min\{x : x > 24k + 12 - 8 \cdot 2\}$*, then*

$$h_{m_k, d_{m_k}-k} \approx \frac{1}{4}\binom{4k}{k}.$$

The following conjecture arises from empirical results. If true, this would allow for the runtime of Algorithm 7.3 to be cut by a factor of two.

Conjecture 8.5. *All sets counted by* h_{n,d_n-k} *have a corresponding inserting set satisfying* $|I| \leq k+1$.

References

[1] J.C. Rosales, P.A. Garcia-Snchez *Numerical Semigroups,* Springer New York, 2009.

[2] J. De Loera, C. O'Neill, Wilburne *Random Numerical Semigroups and a Simplicial Complex of Irreducible Semigroups*. arXiv, 1710.00979 (2017).

Mathematics Department, University of California Davis, Davis, CA 95616

Email address: `calleng@ucdavis.edu`