A STUDY OF NUMERICAL SEMIGROUPS, MARKOV BASES, AND GAUSSIAN INTEGERS

JON ALLEN

Abstract. In this article will study Markov bases, numerical semigroups and Gaussian integers. We will study the relationship between these objects, and study the usefulness of maps between these objects.

1. Introduction

This paper is broken into four main sections. They are: Numerical Semigroups, Bijections, Markov Bases, Gaussian Integers.

Instead of simply heading straight for a definition of numerical semigroups, we will instead construct them from scratch. It will be necessary to understand the reasoning behind the construction of these groups if we wish to create an analogous construction with Gaussian integers later. After we have constructed this semigroup, we will then define it and show some examples. Finally we will discuss Frobenius numbers, which are related to the fact that numerical semigroups have a finite complement.

After we discuss numerical semigroups, then we will talk about the kinds of things which are in bijection with them. These objects include lattice ideals, and Markov bases. This leads us to ask what exactly Markov Ideals are.

The third section will define Markov bases and present a theorem that is central to the usefulness of these objects. We our better understanding of Markov bases we will revisit the map between these and numerical semigroups before we move onto Gaussian integers.

The cocept of numerical semigroups leads us to ask what kind of other similar constructions we can create. We examine what happens when we extend this object from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$. Here we will encounter an exciting and surpising fact.

We will then touch on Markov bases and their relationships to the numerical semigroups we will be looking at.

We will also look at what numeric semigroups are, along with the logic of their construction. We will later use this information and logic to create a similar construction with the Gaussian integers.

We will finally look the structure of the numerical semigroups and see a surprising result in the Gaussian analogue of these.

2. Numerical Semigroups

We begin with a set of positive integers $A = \{n_1, \ldots, n_k\}$. We can form an additive semigroup $S \subset \mathbb{Z}$ with elements of the form $a_1 n_1 + \cdots + a_k n_k \in S$ where $a_i \in \mathbb{N}$. It is sometimes useful to represent A as a vector $\mathbf{n} \in \mathbb{N}^k$ and S as it's vector space. We say that

$S = \langle A \rangle = \{\mathbf{n} \cdot \mathbf{a} : \forall \mathbf{a} \in \mathbb{N}^k\}$. Suppose that $n_i = 0$ for some i. Then n_i does not contribute to S and $\langle A \rangle \cong \langle A \setminus \{n_i\} \rangle$ as a semigroup. Going forward we assume that $n_i \neq 0$ for all i.

As before, we let $A = \{n_1, \ldots, n_k\}$. We will say $c = \gcd(n_1, \ldots, n_k)$ and $A' = \{n_1/c, \ldots, n_k/c\}$. Consider the following function.

$$\begin{aligned} \varphi : &\langle A \rangle \to \langle A' \rangle \\ &n_i \mapsto \frac{n_i}{c} \end{aligned}$$

Now because φ maps the generators of $\langle A \rangle$ to the generators of $\langle A' \rangle$ and is invertible, we know that $\langle A \rangle \cong \langle A' \rangle$. Further, we know that $\gcd(A') = 1$. Henceforth, we will restrict ourselves to semigroups whose generators have a greatest common denominator of one. This restriction has some interesting consequences.

Lemma 1. *Given $A = \{n_1, \ldots, n_k : n \in \mathbb{N}\}$ with $\gcd(A)$, the set of linear combinations of A is the set of all integers.*

Proof. We say $E = \{a_1 n_1 + \cdots + a_k n_k > 0 : a_i \in \mathbb{Z} \text{ and } n_i \in A\}$. Obviously $n_1 \in E$. Because E has at least one element and a lower bound, there must be a smallest element in E. We say the smallest element of E is $s = a_1 n_1 + \cdots + a_k n_k$. We choose some $n_i \in A$. We note that $s \leq n_i$ and divide n_i by s to obtain $n_i = sq + r$ where $q, r \in \mathbb{N}$ and $0 \leq r < s$. This means that

$$\begin{aligned} r &= n_i - sq \\ &= n_i - (a_1 n_1 + \cdots + a_k n_k)q \\ &= n_i - q a_1 n_1 - \cdots - q a_k n_k \\ &= -q a_1 n_1 - \cdots - q a_i n_i + n_i - \cdots - a_k n_k \\ &= -q a_1 n_1 - \cdots - (q a_i - 1) n_i - \cdots - a_k n_k \end{aligned}$$

Thus $r \in E \cup \{0\}$. But $r < s$ and s is the smallest element of E so $r = 0$. This means that $n_i = sq$ for all n_i, but the only number that divides all n_i is 1, and so $s = 1$. And since every multiple of s is a linear combination of the elements of A, we have our result. □

Of course studying a more complicated version of $\mathbb{Z}$ isn't very interesting. This is why we have been limiting the generators of our semigroups to $\mathbb{N}$. There is another much less obvious property that we can obtian from this result however. It will allow us to create an upper bound for the complement in $\mathbb{N}$ of our semigroups. The immediate consequence of this is that the complement in $\mathbb{N}$ of these semigroups is finite.

Theorem 1. *A semigroup generated by a set of positive integers with a greatest common denominator of one has a finite complement in $\mathbb{N}$.*

Proof. Let $A = \{n_1, \ldots, n_k\}$ with $\gcd(A) = 1$ and let $S = \langle A \rangle$. We know from our previous lemma that we can find some $a_1, \ldots, a_k \in \mathbb{Z}$ such that $1 = a_1 n_1 + \cdots + a_k n_k$. Let $\mathbf{a}^+ = \{a_i : a_i > 0\}$ and $\mathbf{a}^- = \{a_j : a_j < 0\}$. Then $1 = \sum_{a_i \in \mathbf{a}^+} a_i n_i + \sum_{a_i \in \mathbf{a}^-} a_j n_j$ or $1 - \sum_{a_j \in \mathbf{a}^-} a_j n_j = \sum_{a_i \in \mathbf{a}^+} a_i n_i$. Now because $a_j < 0$ for all $a_j \in \mathbf{a}^- < 0$ and $a_j < 0$ for all $a_j \in \mathbf{a}^+ > 0$ then $\sum_{a_i \in \mathbf{a}^+} a_i n_i \in \langle A \rangle$ and $-\sum_{a_i \in \mathbf{a}^-} a_i n_i \in \langle A \rangle$. So if we say $c = -\sum_{a_i \in \mathbf{a}^-} a_i n_i$ then we have found c and $c + 1$ which are both elements of $\langle A \rangle$.

We claim that for any $n \geq (c-1)(c+1)$ then $n \in \langle A \rangle$. To verify this claim, we show that $c|n$. Dividing n by c leads us to $n = cq + r$ where $q, r \in \mathbb{N}$ and $0 \leq r < c$. We know that $cq + r \geq (c-1)(c+1) = (c-1)c + (c-1)$. Further $r \geq (c-1)$. This means that $cq \geq (c-1)c$ or $q \geq c - 1 \geq r$. But $n = cq + r = qc + r + rc - rc = (q-r)c + r(c+1)$. We know that $q \geq r \geq 0$ and so $q - r \geq 0$ and $r \geq 0$. We also know that c and $c+1$ are both in $\langle A \rangle$. This means that $n \in \langle A \rangle$. Thus $\mathbb{N} \langle A \rangle \subset \{n \in \mathbb{N} : n < (c+1)(c-1)\}$, which is finite.

□

Definition 1. [7] A numerical semigroup (NSG) is a nonempty subset S of $\mathbb{N}$ that is closed under addition, contains the zero element, and whose complement in $\mathbb{N}$ is finite.

2.1. Examples

Example 1. *The semigroup generated by* $\{1\}$ *is* $\{0, 1, 2, \dots\} = \mathbb{N}$. *Obviously* $\mathbb{N} \setminus \mathbb{N} = \emptyset$ *which is finite, thus* $\mathbb{N}$ *is a NSG.*

Example 2. *The semigroup generated by* $\{2\}$ *is* $\{0, 2, 4, \dots\}$. *The complement of this set is all odd natural numbers. The complement of this semigroup in* $\mathbb{N}$ *is not finite, thus our semigroup is not a NSG.*

Example 3. *The semigroup generated by* $\{2, 3\}$ *is* $A = \{0, 2, 3, 4, \dots\}$. *Obviously* $\mathbb{N} \setminus A = \{1\}$ *which is finite, thus* A *is a NSG.*

Example 4. *The semigroup generated by* $\{6, 10, 15\}$ *is* $B = \{0, 6, 10, 12, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, \dots\}$. $\mathbb{N} \setminus B = \{1, 2, 3, 4, 7, 8, 9, 11, 13, 14, 17, 19, 23, 29\}$ *is finite, and* B *is a NSG.*

2.2. Frobenius Numbers

The fact that NSGs have a finite complement in $\mathbb{N}$ has a consequence. Namely that for any semigroup S there exists some minimal natural number $F(S)$ such that if $n > F(S)$ then $n \in S$. In words, this number $F(S)$ is the largest natural number that is not in our semigroup. This is called the Frobenius number, while the number $F(S) + 1$ is referred to as the conductor[7].

We take a numerical semigroup S generated by the set $A = \{n_1, \dots, n_k\}$. We let $m = \min(A)$ and $M = \max(A)$. As we saw in the proof for Theorem 1, if we have two consecutive numbers $c, c+1 \in S$ then $c^2 - 1$ provides an upper bound for $F(S)$. How much better can we do? There are formulas for some specific cases, but there are no known formulas for every case. Here we present an algorithm for finding the Frobenius number of any NSG.

The structure of an NSG has some trivial but very useful properties. The first thing of note, is that if we find the conductor than we have found the Frobenius number and vice versa. If we choose some $s_1 \in S$, then there exists at least one s_2 such that $s_1 < s_2 \leq s_2 + M$. In fact, for any $n_i \in A, s_1 \in S$ we know that $s_1 < s_1 + n_i \leq s_1 + M$. We use this fact to provide a working interval for our algorithm of $[s_i, s_i + M]$.

Let us suppose we have found m sequential elements in S starting with $s_1 \in S$. We know that $s_1 + i \in S$ for all $0 \leq i \leq m - 1$. Choose any $s_2 > s_1$. Then $s_2 = s_1 + j$ for some $j \in \mathbb{N}$. If we divide j by $\min A$ then we obtain $j = q \cdot \min(A) + r$ where $0 \leq r < \min A$. From the definition of a semigroup, we know that if $s_1 \in S$ then $s_1 + q \cdot \min(A) \in S$. It also follows that $s_1 + r \in S$. Putting thse two facts together, we have $(s_1 + r) + q \cdot \min(A) \in S$. This means that $s_2 \in S$.

Thus the smallest number in A which begins a consecutive sequence of m elements in A is the conductor. Our algorithm begins with a known lower bound for our conductor. We increase this bound until we find a sequence of $\min A$ consecutive elements in S will. This reveals our conductor.

We know that every NSG contains zero. Zero is also the smallest element of any NSG and so it is our first candidate for the conductor. We say $c_1 = 0$ and begin our algorithm by constructing a working set $F_1 = \{c_1 + n_1, \ldots, c_1 + n_k\}$.

We say $c_i = c_1$ and $F_i = F_1$ and we begin iterating our algorithm. As we iterate we will seek to ensure that $|F_i| \leq \max A$.

We check to see if the smallest $\min A$ elements of F_i are sequential. If they are, then we have met our termination criteria, and $F(S) = c_i - 1$. If we have not met the termination criteria, then we choose our next conductor candidate. We know that we have accounted for all elements in our semigroup at this point up to $c_i + \min A$. It is then safe to discard any elements of our semigroup below $\min F_i$. We choose our next lower bound for our conductor to be $c_{i+1} = \min F_i$ and define $F_i' = F_i \setminus \{\min F_i\}$.

We have assumed that $c_i + \min A$ elements are accounted for, and so we need to ensure this for the next iteration. Thus we say $F_{i+1} = F_i' \cup \{\min F_i + n_j : \forall n_j \in A\}$. Now we are ready to iterate again, and so go to the termination criteria step for F_{i+1}

The maximum time this algorithm takes to find the Frobenius number is a linear multiple of the number of elements in the semigroup and the size of the Frobenius number. There may be faster ways of finding this number, but for our purposes, it is simple to implement and lends itself to a great deal of optimization when run on binary computer system.[2]

The following is a pseudocode implementation of the algorithm. Given a numerical semigroup $S = \langle A \rangle$ where $A = \{n_1, \ldots, n_k\}$, the algorithm takes A as input and produces the conductor c of the NSG as output.

```
INPUT: A = {n_1, ..., n_k} where gcd(n_1, ..., n_k) = 1

  c := 0
  F := A
  WHILE [c + 1, c + min(A) − 1] ⊄ F
    c := min(F)
    F := F \ {min(F)}
    F := F ∪ {c + n_i : ∀n_i ∈ A}
  ENDWHILE

OUTPUT: The conductor of ⟨A⟩ is c
```

Example 5. *We let* $\langle A \rangle = \langle 5, 7, 9 \rangle$. *Then* $c_1 = 0$ *and* $F_1 = \{5, 7, 9\}$ *while* $\min(A) = 5$. *We iterate our algorithm in the table below:*

Conductor	*Working NSG Window*	*Termination*
$c_1 = 0$	$F_1 = \{5, 7, 9\}$	$\{1, 2, 3, 4\} \not\subset F_1$
$c_2 = 5$	$F_2 = \{7, 9, 10, 12, 14\}$	$\{6, 7, 8, 9\} \not\subset F_2$
$c_3 = 7$	$F_3 = \{9, 10, 12, 14, 15\}$	$\{8, 9, 10, 11\} \not\subset F_3$
$c_4 = 9$	$F_4 = \{10, 12, 14, 15, 16, 18\}$	$\{10, 11, 12, 13\} \not\subset F_4$
$c_5 = 10$	$F_5 = \{12, 14, 15, 16, 17, 18, 19\}$	$\{11, 12, 13, 14\} \not\subset F_5$
$c_6 = 12$	$F_6 = \{14, 15, 16, 17, 18, 19, 21\}$	$\{12, 13, 14, 15\} \not\subset F_6$
$c_7 = 14$	$F_7 = \{15, 16, 17, 18, 19, 21, 23\}$	$\{15, 16, 17, 18\} \subset F_7$

And so we see that 13 *is the Frobenius number for* $\langle 5, 7, 9\rangle$

3. Markov Bases

The semigroups that we have been examining are relatively simple objects. In the upcoming section on bijections we will see how we can relate them to less straightforward algebraic and combinatorial objects. However in order to have that discussion we will need to understand a tool called the Markov basis.

Markov bases play a central role in the recent field of algebraic statistics. A seminal paper[4] on this field introduced the idea of a Markov basis for log linear statistical models and related them to commutative algebra. This work has been applied in many fields and has been particularly active in computational biology[5]. However, we will be glossing over the statistical role of these bases and will instead focus on their algebraic properties. First we need to get a few definitions and some notation out of the way.

We can represent a numerical semigroup $S = \langle n_1, \ldots, n_k\rangle$ as a matrix $A = \begin{bmatrix} n_1 & \cdots & n_k \end{bmatrix}$. Then for every element $s \in S$ we can say $s = Au$ for some $u \in \mathbb{N}^k$.

Definition 2. [5] The set of tables

$$\mathcal{F}(u) = \Big\{v \in \mathbb{N}^k : Av = Au\Big\}$$

is called the *fiber* of a contingency table $u \in \mathcal{T}(n)$ with respect to the model $\mathcal{M}_A$

Contingency tables and matrix models are specific to statistics. The thing we should take from this definition, is that a fiber $\mathcal{F}(u)$ of an element Au of our semigroup A is the set of vectors $\big\{v \in \mathbb{N}^k : Av = Au\big\}$

Example 6. *For the numerical semigroup* $A = \begin{bmatrix} 3 & 4 & 5 \end{bmatrix}$ *we will find the fiber corresponding to the element* $Au = 8$.

We need to find all solutions to the equation $\begin{bmatrix} 3 & 4 & 5 \end{bmatrix}\begin{bmatrix} x, y, z \end{bmatrix} = 8$ *or* $3x+4y+5z = 8$ *where* $x, y, z \in \mathbb{N}$. *We find that* $3 + 5$ *and* $4 \cdot 2$ *are the only two possible solutions, and so for* $Au = 8$ *we see that* $\mathcal{F}(u) = \{(1, 0, 1), (0, 2, 0)\}$.

Before we give the definiton of a Markov basis, we note that the literature often refers to the elements of a Markov basis as *moves*[5, p.16]

Definition 3. [5] Let $\mathcal{M}_A$ be the log-linear model associated with a matrix A whose integer kernel we denote by $\ker_{\mathbb{Z}}(A)$. A finite subset $\mathcal{B} \subset \ker_{\mathbb{Z}}(A)$ is a *Markov basis* for $\mathcal{M}_A$ if for all $u \in \mathcal{T}(n)$ and all pairs $v, v' \in \mathcal{F}(u)$ there exists a sequence $u_1, \ldots, u_L \in \mathcal{B}$ such that

$$v' = v + \sum_{k=1}^{L} u_k \text{ and } v + \sum_{k=1}^{l} u_k \geq 0 \text{ for all } l = 1, \ldots, L.$$

Now that we have some more insight as to what a Markov basis is, the process in example 8 should make more sense.

Example 7. *We will find the Markov basis which corresponds to the numerical semigroup* $A = \langle 3, 4, 5\rangle$*. First we generate the fibers which correspond to the elements of our NSG.*

$$\left[\begin{array}{c|ccc} & 3 & 4 & 5 \\ \hline 3 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 \\ 5 & 0 & 0 & 1 \\ 6 & 2 & 0 & 0 \\ 7 & 1 & 1 & 0 \\ 8 & 1 & 0 & 1 \\ 8 & 0 & 2 & 0 \\ 9 & 3 & 0 & 0 \\ 9 & 0 & 1 & 1 \\ 10 & 2 & 1 & 0 \\ 10 & 0 & 0 & 2 \end{array}\right]$$

We are particularly interested in fibers with more than one element. These are the fibers associated with the elements $8, 9$ *and* 10*. From the definition of the Markov basis, we know that the product of* A *and an element of the Markov basis is* 0*. Furthermore, we know that we can add a sequence of elements of the Markov basis to any of the elements of a fiber to obtain any other element of that fiber. Taking the difference of two elements from the same fiber will meet both of these criteria.*

Thus if $Au = 8$ *then* $\mathcal{F}(u) = \{(1, 0, 1), (0, 2, 0)\}$ *and so* $(-1, 2, -1) \in \mathcal{B}$*. If* $Av = 9$ *then* $\mathcal{F}(v) = \{(3, 0, 0), (0, 1, 1)\}$ *and so* $(3, -1, -1) \in \mathcal{B}$*. And if* $Aw = 10$ *then* $\mathcal{F}(w) = \{(2, 1, 0), (0, 0, 2)\}$ *and so* $(-2, -1, 2) \in \mathcal{B}$*. And so we have built our Markov basis.*

$$\mathcal{B} = \begin{bmatrix} 3 & -1 & -1 \\ -1 & 2 & -1 \\ -2 & -1 & 2 \end{bmatrix}$$

We also have the fundamental theorem of Markov bases which provides a direct relation to a lattice ideal.

Theorem 2. [3, p. 54] *A finite set of moves* $\mathcal{B}$ *is a Markov basis for* A *if and only if the set of binomials* $\{p^{\mathbf{z}^+} - p^{\mathbf{z}^-} | \mathbf{z} \in \mathcal{B}\}$ *generates the toric ideal* I_A*.*

4. Bijections

As we mentioned in the last section, NSGs are simple to study. It would be useful if we could consider more complicated objects as NSGs. To this end, we will describe some bijections between NSGs and other objects. To start, consider $\varphi : \mathbb{N}^n \to k[x_1, \ldots, x_k]$ given by $\alpha \mapsto \mathbf{x}^\alpha$.

Lemma 2. *Let* S *be a NSG. Then* $\varphi(S)$ *is the set of monic monomials of a monomial ideal of* $k[x]$*, where* φ *is as above.*

Proof. Let $S = \langle n_1, \ldots, n_k \rangle$ and let $I = \langle x^{n_1}, \ldots, x^{n_k} \rangle$. We choose $M \in I$ and $s \in S$ where $M = \prod_{i=1}^{k} (x_i^{n_i})^{a_i}$ while $s = \sum_{i=1}^{k} a_i n_i$. We observe that $\varphi(s) = \varphi(\sum_{i=1}^{k} a_i n_i) = \prod_{i=1}^{k} x_i^{a_i n_i} = \prod_{i=1}^{k} (x_i^{n_i})^{a_i} = M$. □

If we look at $\mathbb{Z}$ instead of $\mathbb{N}$ then we have an analogous map with binomials. In the binomial case we start with some $\mathbf{z} \in \mathbb{Z}^n$. We define $\mathbf{z} = (z_1, \ldots, z_n)$. We say that $\mathbf{z}^+ = \mathbf{z} \vee \mathbf{0}$ gives us a vector where $z_i^+ = \max(z_i, 0)$. Similarly $\mathbf{z}^- = \mathbf{z} \wedge \mathbf{0}$ is a vector where $z_i^- = \min(z_i, 0)$. We can map an element of $\mathbb{Z}^n$ to a binomials over field k by $\varphi : \mathbb{Z}^n \to k[x_1 \ldots x_n]$ where $\mathbf{z} \mapsto \mathbf{x}^{\mathbf{z}^+} - \mathbf{x}^{\mathbf{z}^-}$.

If we wish for the map to be bijective, then we need some addition restrictions. Let us assume that k has characteristic 2. We assume that $x - y = x + y$ for any $x, y \in k$. Then $\varphi(1, -1) = x - y = x + y = \varphi(1, 1)$ and $\varphi(1, 1) = x + y = y - x = \varphi(-1, 1)$. This map is obviously not one to one, and so we must restrict ourselves to fields who have characteristic other than 2.

Now consider the binomial $x + x^2$. This binomial is not in the image of φ. Bijection requires surjection, and so we restrict our codomain to be the set of pure binomials in $k[x_1, \ldots, x_n]$

4.1. Markov Bases

We wish to move from $\mathbb{N}$ to $k[x_1, \ldots, x_n]$. The tool we need for this is the Markov basis. These bases are troublesome to compute, but theorem 2 tells us that they provide a map from $\mathbb{N}$ to $\mathbb{Z}^n$. This combined with our above discussion on binomials will give us all that we need to complete this map.

Each element a of a numerical semigroup $S = \langle n_1, \ldots, n_k \rangle$ takes the form $a = a_1 n_1 + \cdots + a_k n_k$. Now we examine the vectors $(a_1, \ldots, a_k)$. Note that any given $a \in S$ may have more than one vector associated with it, and the set of these vectors make up the fiber over a.

Example 8. $S = \langle 3, 4, 5 \rangle$. *Notice that* $8 = 2 \cdot 4 = (3, 4, 5) \cdot (0, 2, 0)$ *and* $8 = 3 + 5 = (3, 4, 5) \cdot (1, 0, 1)$. *Thus the vectors* $(0, 2, 0)$ *and* $(1, 0, 1)$ *make up the fiber over* $8 \in S$.

The vectors $\mathbf{a} = (a_1, \ldots, a_k)$ and $\mathbf{b} = (b_1, \ldots, b_k)$ are connected if there exists some i such that $a_i > 0$ and $b_i > 0$. Furthermore, if $\mathbf{a}$ is connected to $\mathbf{b}$ and $\mathbf{b}$ is connected to $\mathbf{c}$ then $\mathbf{a}$ is connected to $\mathbf{c}$.

We are looking for elements of our NSG which have multiple associated but disconnected vectors. Once we have found two disconnected vectors associated with an element of our NSG, then we subtract them to find an element of our Markov basis. We continue until we have found the elements of our Markov basis guaranteed by Theorem 2.

Example 9. *We will find the Markov basis which corresponds to the NSG* $\langle 3,4,5\rangle$*. First we generate a list of vectors which correspond to the elements of our NSG.*

$$\left[\begin{array}{c|ccc} & 3 & 4 & 5 \\ \hline 3 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 \\ 5 & 0 & 0 & 1 \\ 6 & 2 & 0 & 0 \\ 7 & 1 & 1 & 0 \\ 8 & 1 & 0 & 1 \\ 8 & 0 & 2 & 0 \\ 9 & 3 & 0 & 0 \\ 9 & 0 & 1 & 1 \\ 10 & 2 & 1 & 0 \\ 10 & 0 & 0 & 2 \end{array}\right]$$

Now we see that $8, 9, 10$ *all have two associated but disconnected vectors. We subtract these vectors to obtain*

$$\begin{bmatrix} 3 & -1 & -1 \\ -1 & 2 & -1 \\ -2 & -1 & 2 \end{bmatrix}$$

Which is our Markov basis.

It is convenient to write our Markov basis as a matrix, whose rows consist of the elements of the Markov basis.

4.2. Smith Normal Form

Now we have found a map from NSGs to pure binomial ideals of $k[x_1,\dots,x_n]$ where k is not characteristic 2. If we wish to consider the NSG and the binomial ideals the same objects, then given a Markov basis, we should be able to find an associated NSG. Let M be the matrix with rows corresponding to the vectors of a Markov basis. Every row v of M consists of two vectors a, b where $v = a - b$. Let $S = \langle n_1,\dots,n_k\rangle$ and define the vector $s = (n_1,\dots,n_k)$. Now if S is the semigroup associate with M then by construction $s \cdot a = s \cdot b$. And so $s \cdot v = 0$. This means that if we have M, we can find our numerical semigroup S by finding a nontrivial solution to $Ms = 0$.

The usual tools of linear algebra are not useful here. The major problem is that we are dealing with matrices in $\mathbb{Z}$ instead of $\mathbb{R}$ and so we don't have division available in general. The tool we need is the Smith normal form.

Definition 4. If we are given some matrix A whose entries are in a principal ideal domain, then we can find some matrices U, V, B such that

$$UAV = B = \begin{bmatrix} b_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & b_r \end{bmatrix} \text{ with } b_i | b_{i+1}$$

We call B the *Smith normal form* of A.[1]

If there exists some $s \neq \mathbf{0}, M \in \mathcal{M}_{q\times r}$ such that $Ms = \mathbf{0}$ then $\text{rank}(M) < r$. And so if we have $UMV = B$ where B is the Smith normal form of M then $B = \begin{bmatrix} b_1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & b_{r-1} & 0 \\ 0 & \cdots & 0 & 0 \end{bmatrix}$. Because the last column of B is $\mathbf{0}$ we know that if $\mathbf{v}$ is the last column of V then $M\mathbf{v} = \mathbf{0}$. The semigroup generated by the coordinates of $\mathbf{v}$ must be isomorphic to a unique numerical semigroup generated by the coordinates of some vector $\mathbf{s} = \alpha\mathbf{v}$ where $\alpha \in \mathbb{Q}$ and the greatest common divisor of the coordinates of s is 1.

Example 10. *Let us find the Smith normal form of* $A = \begin{bmatrix} 3 & -1 & -1 \\ -1 & 2 & -1 \\ -2 & -1 & 2 \end{bmatrix}$. *We start with* $U'AV' = I_A A I_A$. *We then use the standard row and column operations on* A *while recording the row operations on* U' *and the column operations on* V' *to find our Smith normal form, along with the* U *and* V. *Remember we are working over* $\mathbb{Z}$ *and so we will only be adding, subtracting, and multiplying, not dividing.*

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 3 & -1 & -1 \\ -1 & 2 & -1 \\ -2 & -1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$
$$\Downarrow$$
$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 3 & -1 & -1 \\ -1 & 2 & -1 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$
$$\Downarrow$$
$$\begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 3 & -3 \\ -1 & 2 & -1 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$
$$\Downarrow$$
$$\begin{bmatrix} 1 & 2 & 0 \\ 1 & 3 & 0 \\ 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 3 & -3 \\ 0 & 5 & -4 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$
$$\Downarrow$$
$$\begin{bmatrix} 1 & 2 & 0 \\ 1 & 3 & 0 \\ 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & -3 \\ 0 & 1 & -4 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$
$$\Downarrow$$
$$\begin{bmatrix} 1 & 2 & 0 \\ 1 & 3 & 0 \\ 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 1 & 5 \end{bmatrix}$$

And so $\begin{bmatrix} 1 & 2 & 0 \\ 1 & 3 & 0 \\ 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 3 & -1 & -1 \\ -1 & 2 & -1 \\ -2 & -1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 1 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

Observe that the Markov basis was the basis obtained in a previous example from the NSG $\langle 3,4,5\rangle$*. We see that the last column of* V *is* $(3,4,5)$ *which corresponds exactly to the NSG we began with.*

Calculating these matrices is tedious, time consuming and error prone. Fortunately computers well suited to these kinds of calculations. One software package that can easily compute these matrices is Xcas[6].

4.3. Numerical Semigroups in Lattice Theory

We have already discussed NSGs, Markov basis, and binomials. Now we examine lattice ideals, which can be expressed as binomial ideals.

Definition 5. [8] A *lattice* is a partially ordered set in which every two elements have a unique least upper bound and a unique greatest lower bound.

Example 11. *The space* $\mathbb{N}^2$ *is a lattice with supremum and infinum for any two elements which belong to it. Notice that* $(1,2)$ *and* $(2,1)$ *have a lower bound of* $(1,1)$ *and an upper bound of* $(2,2)$*.*

Example 12. *We can form a lattice if we order* $\mathbb{N}$ *by division. The least common multiple forms a least upper bound and an greatest lower bound is formed by the greatest common denominator.*

The fundamental theorem of Markov bases (theorem 2) claims that there is a bijection between a lattice ideal and a Markov basis. As we have already seen, Markov bases are in bijection with NSGs.

Thus we see that every NSG corresponds to a lattice ideal.

Example 13. *We begin with a lattice ideal in* $k[x,y,x]$ *with* $char(k) \neq 2$

$$I_\Lambda = \langle x^3 - yz, y^2 - xz, z^2 - xy\rangle$$

We can map this generating set to $\mathbb{Z}^3$ *in the usual way.*

$$\begin{cases} x^3 - yz \\ y^2 - xz \\ z^2 - x^2y \end{cases} \Rightarrow \begin{bmatrix} 3 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}$$

The key here, is that we are guaranteed by Theorem 2, that these vectors are actually a Markov basis. And as we saw in the previous two sections, this basis corresponds to the numerical semigroup $\langle 3,4,5\rangle$*. And so we see*

$$\begin{cases} x^3 - yz \\ y^2 - xz \\ z^2 - xy \end{cases} \mapsto \langle 3,4,5\rangle$$

The reverse map is similarly straightforward.

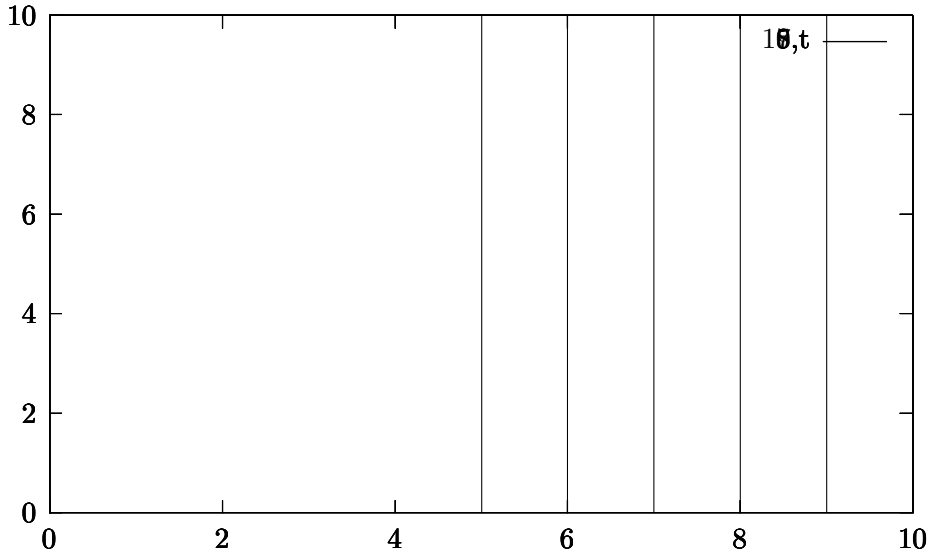
5. Gaussian Integers

Notice that the real and complex parts of Gaussian integers do not interact under addition. Now let us take the linear combination of some finite set of Gaussian integers.

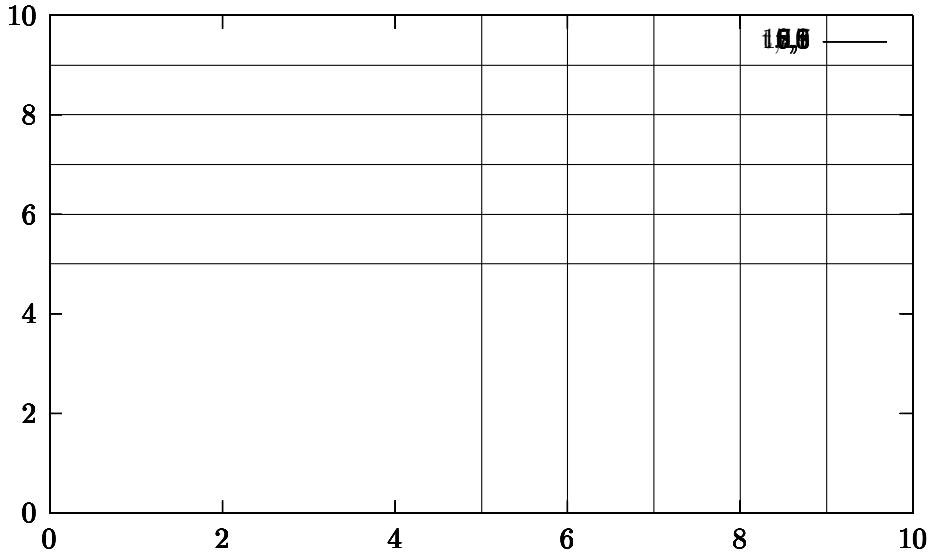
If we do not restrict ourselves to positive coefficients, then we wind up with semigroups that span the entire number line along multiples of a greatest common denominator. This is as uninteresting now as it was with NSGs, and so we will only look at positive values from here.

Now let us take some "Gaussian semigroup" $\mathbf{z} = \langle x_1 + y_1 i, \ldots, x_n + y_n i \rangle$ where $x_i, y_i \geq 0$. Notice that this semigroup is actually just the direct sum of two NSGs. Say $\mathbf{z} = \mathbf{x} \oplus \mathbf{y} = \langle x_1, \ldots, x_n \rangle \oplus \langle y_1, \ldots, y_n \rangle$.

Now as you may have guessed from our choice of notation, we are going to think of this direct sum as a Cartesian product. Now we know that the semigroup $\mathbf{x}$ has some Frobenius number after which every number is in the semigroup.



And if we add in $\mathbf{y}$ then we have



Now our intuition and our inspection of the graph leads us to believe that we can easily come up with an analog of a Frobenius number in $\mathbb{N}$ to a Gaussian Frobenius number in

$\mathbb{N}[i]$. We say that the Frobenius number for $\mathbf{x}$ is $F(\mathbf{x})$ and the Frobenius number for $\mathbf{y}$ is $F(\mathbf{x})$. Now let us choose some $F(\mathbf{x} < \mathbf{x} \in \mathbf{x}$. There are only a finite number of combinations that equal x. That means that for any x there are only a finitely many number of $y \in \mathbf{y}$ such that $x + yi \in \mathbf{z}$. But this means that for any point in our Gaussian semigroup, we can find an infinite number of Gaussian integers greater than that point which are not in our semigroup. The surprise here is that not only is there no analog to a Frobenius number but element is this semigroup remain sparse over the entire $\mathbb{N}^2$ lattice.

References

1. W. Adkins and S. Weintraub, *Algebra: An approach via module theory*, Graduate Texts in Mathematics, Springer New York, 2012.
2. Jon Allen, *Frobmask*, http://www.github.com/ylixir/frobmask.
3. S. Aoki, H. Hara, and A. Takemura, *Markov bases in algebraic statistics*, Springer Series in Statistics, Springer New York, 2012.
4. Persi Diaconis, Bernd Sturmfels, et al., *Algebraic algorithms for sampling from conditional distributions*, The Annals of statistics **26** (1998), no. 1, 363–397.
5. Mathias Drton, Bernd Sturmfels, and Seth Sullivant, *Lectures on algebraic statistics*, 2008.
6. Bernard Parisse and Renée De Graeve, *Giac/xcas*, http://www-fourier.ujf-grenoble.fr/~parisse/giac_fr.html, 2015.
7. J.C. Rosales and P.A. García-Sánchez, *Numerical semigroups*, Developments in Mathematics, Springer New York, 2009.
8. R.P. Stanley, *Enumerative combinatorics:*, Cambridge Studies in Advanced Mathematics, no. v. 1, Cambridge University Press, 2011.