ON THE MARKOV BASIS

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

We will proceed by first going over some basic maps between elements of $\mathbb{N}^n$ and monomials. We will also touch on similar maps from $\mathbb{Z}^n$ and binomials.

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 will go into a little greater depth here than we would ordinarily need to, but we will use some of this logic to make some decisions later when we examine Gaussian integers.

We begin with a set of unique 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 $a_i \in \mathbb{N}$. If $A = \{0\}$ then our semigroup consists solely of the element 0, which is not interesting. Similarly if there exists some $n_i = 0 \in A$ then the semigroup formed by A is isomorphic to that formed by $A \setminus n_i$. In order to keep things simple we will define $n_i \neq 0$ for all $1 \leq i \leq k$.

Now if the elements of A have a greatest common denominator $c \neq 1$ then $c|s$ for every element $s \in S$. We can construct a semigroup $S' = \{a_1 n_1/c + \cdots + a_k n_k/c : a_i \in \mathbb{N}, n_i \in A\}$ where $S \simeq S'$. So we see that we can form a bijection between our S semigroup and a semigroup with a greatest common denominator of one by multiplying or dividing every element in the group by c. Therefore we will only consider semigroups with coprime bases.

Theorem 1. *The complement of a semigroup in $\mathbb{N}$ generated by a set of positive coprime integers is finite.*

Proof. Now consider $n_i, n_j \in A$. Then $\{an_i + bn_j > 0 | a, b \in \mathbb{Z}\} = E$. There is at least one element in this set (z_i) and so there is a smallest element. Let this smallest element be $c = az_i + bz_j$. Now if we divide z_i by c then we obtain $z_i = cq + r$ with $0 \leq r < c$. This leads to $r = z_i - cq = z_i - (az_i + bz_j)q = (1 - aq)z_i + bqz_j \in E$. Now because $0 \leq r < c$ and

c is a minimal element then $r = 0$. And so we have $z_i = cq$. That is to say $c|z_i$. Similarly $c|z_j$ and so $c = 1$.

Now if $1 \in E \subseteq S$ then $a, b \geq 0$ because the multiplication is just shorthand for the group addition. And so we have $1 = az_i + bz_j$. Now if $a, b \geq 0$ then either $z_i = 1$ or $z_j = 1$ or one of $z_i, z_j < 0$. In any of these cases we have $S = \mathbb{Z}$ which is not interesting, and so we restrict z_i to be in $\mathbb{N}$. □

Definition 1. [7] A numerical semigroup 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 numerical semigroup.*

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 numerical semigroup.*

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 numerical semigroup.*

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

2.2. Frobenius Numbers

The fact that numerical semigroups have a finite complement in $\mathbb{N}$ has a consequence. Namely that for some semigroup S there exists some minimal N such that for $n \in S$ for every $n > N$. This number is called the Frobenius number.

We have a semigroup S generated by the set of positive integers $A = \{n_1, \dots, n_k\}$. Let $n_{\max} = \max(\{n_1, \dots, n_k\})$ and $n_{\min} = \min\{n_1, \dots, n_k\}$. If we choose some $s_1 \in S$, then there exists at least one s_2 such that $s_1 < s_2 \leq s_2 + n_{\max}$. In fact, for any $n_i \in A, s_1 \in S$ we know that $s_1 < s_1 + n_i \leq n_{\max}$. This may seem obvious but let us continue.

This suggests a simple algorithm for finding a Frobenius number. Let us consider the numerical semigroup $\langle z_1, \dots, z_n \rangle$. We know that every numerical semigroup contains zero. Thus our first candidate for a Frobenius number is -1.

For this algorithm it will be convenient to work with the conductor, which is the Frobenius number plus one. And so we have our first conductor candidate $c_1 = 0$. At this point we have obviously accounted for every element in our semigroup smaller than our conductor candidate, and so we begin our algorithm by lettting $c_i = c_1$ and the set $F_i = \{c_i + z_1, \dots, c_i + z_n\}$. It is good to know that F_i has a maximum cardinality of $z_{\max}$, which is all the numbers we will need to keep track of for this algorithm.

Now we start our algorithm. Let us check the interval $[c_1 + 1, c_1 + z_{\min}]$. If every element of this interval is contained in our set, then we have found our conductor c_i and we are done.

Otherwise, we know that we have accounted for every member of our semigroup up to $\min F_i$. That means that we can make the smallest number of our set the new candidate for conductor, and then remove that number from our set. And so we take $c_{i+1} = \min F_i$.

Now if we add our new candidate to every element in our semigroup basis and put it in the set, then we know that we will have generated every number in our semigroup up to the smallest element in our set. So let us make $F_{i+1} = F_i \setminus \{c_{i+1}\} + \{c_{i+1} + z_1, \ldots c_{i+1} + z_n\}$. Now we set $i = i + 1$ and go back to the beginning of the algorithm.

This algorithm will find the Frobenius number within 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 works quickly enough.[2]

3. Bijections

The things we need to understand is a common map that the literature takes for granted. There is a straightforward map between $\mathbb{N}^m$ and monomials over a field k. We choose some $\alpha \in \mathbb{N}^m$ such that $\alpha = (\alpha_1, \ldots, \alpha_m)$. Now we define a map for $\varphi : \mathbb{N}^n \to k[x_1, \ldots, x_m]$ such that $\alpha \mapsto \mathbf{x}^\alpha$.

Lemma 1. *Let S be a numerical semigroup. Then $\varphi(S)$ is the set of monic monomials of a monomial ideal of $k[x]$, where φ is as above.*

Proof. We take a numerical semigroup $S = \langle n_1, \ldots, n_m \rangle$. Under φ this set maps to $\{x^s : s \in S\}$. Of course $s = a_1 n_1 + \cdots + a_m n_m$ where $a_i \in \mathbb{N}$. Of course multiplying monomials is simply a matter of adding exponents, and so if $I = \langle x^{n_1}, \ldots, x^{n_m} \rangle$ then $\varphi : S \to I$ $\qquad \square$

We can do a similar 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 also define $\mathbf{z}^+$ and $\mathbf{z}^-$ as follows:

$$\mathbf{z}^+ = \mathbf{z} \vee \mathbf{0} \qquad\qquad \mathbf{z}^- = -(\mathbf{z} \wedge \mathbf{0})$$

Now we can map an element of $\mathbb{Z}^n$ to the binomials over field k if we define $\varphi : \mathbb{Z}^n \to k[x_1 \ldots x_n]$ as $\mathbf{z} \mapsto \mathbf{x}^{\mathbf{z}^+} - \mathbf{x}^{\mathbf{z}^-}$

3.1. Numerical Semigroups in Lattice Theory

Definition 2. [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 5. $\mathbb{N}^2$ *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 6. *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.*

3.2. Markov Bases

As we will see in Theorem 2 we can map a numerical semigroup to a Markov basis[5]. Each element a of a numerical semigroup $S = \langle n_1, \ldots, n_m \rangle$ takes the form $a = a_1 n_1 + \cdots + a_m n_m$. Now we examine the vectors $(a_1, \ldots, a_m)$. Note that any given $a \in S$ may have more than one vector associated with it.

Example 7. $S = \langle 3, 4, 5 \rangle$. *Notice that $8 = 2 \cdot 4 = 3 + 5$. Thus we have two vectors associated with $8 \in S$.*

We are looking for elements of our numerical semigroup which have multiple associated but disconnected vectors. The vectors $\mathbf{a} = (a_1, \ldots, a_m)$ and $\mathbf{b} = (b_1, \ldots, b_m)$ 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 $\mathbf{c}$. Once we have found two disconnected vectors associated with an element of our numerical semigroup, 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 8. *We will find the Markov basis which corresponds to the numerical semigroup $\langle 3, 4, 5 \rangle$. First we generate a list of vectors which correspond to the elements of our numerical semigroup.*

$$
\begin{bmatrix}
 & 3 & 4 & 5 \\
\hline
3 & 1 & 0 & 0 \\
4 & 0 & 1 & 0 \\
5 & 0 & 0 & 1 \\
6 & 2 & 0 & 0 \\
7 & 1 & 1 & 0 \\
8 & 1 & 0 & 1 \\
8 & 0 & 2 & 0 \\
9 & 3 & 0 & 0 \\
9 & 0 & 1 & 1 \\
10 & 2 & 1 & 0 \\
10 & 0 & 0 & 2
\end{bmatrix}
$$

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.

3.3. Smith Normal Form

We choose a Markov basis matrix M and it's associated numerical semigroup S. Every row v of M consists of two vectors a, b where $v = a - b$. Let $S = \langle n_1, \ldots, n_m \rangle$ and define the vector $s = (n_1, \ldots, n_m)$. Now $s \cdot a = s \cdot b$. 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 $Ms = 0$.

This suggests that we could use the Smith normal form of our Markov basis matrix to find our numerical semigroup.

Definition 3. If we are given some matrix M whose entries are in a principal ideal domain, then we can find some matrices U, V, B such that

$$
UAV = B = \begin{bmatrix}
a_1 & \cdots & 0 \\
\vdots & \ddots & \vdots \\
0 & \cdots & a_r
\end{bmatrix} \quad \text{with } a_i | a_{i+1}
$$

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

Example 9. *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 doing reflecting the row operations on U' and the column operations on V' to find our Smith normal form, along with the matrices which give us this form. Note that we are dealing with integers here, fractions are not allowed*

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

$$\Downarrow$$

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

$$\Downarrow$$

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

$$\Downarrow$$

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

$$\Downarrow$$

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

$$\Downarrow$$

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

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

We can use the software package Xcas[6] to easily compute these matrices.

4. Markov Bases

We have been speaking of Markov bases, but we have not explored what they are or where they come from. In this section we will explore their history and their relevance.

Markov bases play a central role in the recent field of algebraic statistics. One of the earliest papers on this field[5] introduced the idea of a Markov basis for log linear statistical models[4] and related them to commutative algebra. This work has been applied in many

fields and has been particularly active in computational biology. 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 $S = \langle n_1, \ldots, n_m \rangle$ as a matrix $A = \begin{bmatrix} n_1 & \cdots & n_m \end{bmatrix}$. Then for every element $s \in S$ we can say $s = Au$ for some $u \in \mathbb{N}^m$.

Definition 4. [5] The set of tables

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

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 $\{v \in \mathbb{N}^m : Av = Au\}$

Example 10. *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 5. [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 11. *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 numerical semigroup.*

$$\begin{bmatrix} & 3 & 4 & 5 \\ \hline 3 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 \\ 5 & 0 & 0 & 1 \\ 6 & 2 & 0 & 0 \\ 7 & 1 & 1 & 0 \\ 8 & 1 & 0 & 1 \\ 8 & 0 & 2 & 0 \\ 9 & 3 & 0 & 0 \\ 9 & 0 & 1 & 1 \\ 10 & 2 & 1 & 0 \\ 10 & 0 & 0 & 2 \end{bmatrix}$$

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 $\{p^{\mathbf{z}^+} - p^{\mathbf{z}^-} \mid \mathbf{z} \in \mathcal{B}\}$ generates the toric ideal I_A.*

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 numerical semigroups, 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 numerical semigroups. 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.
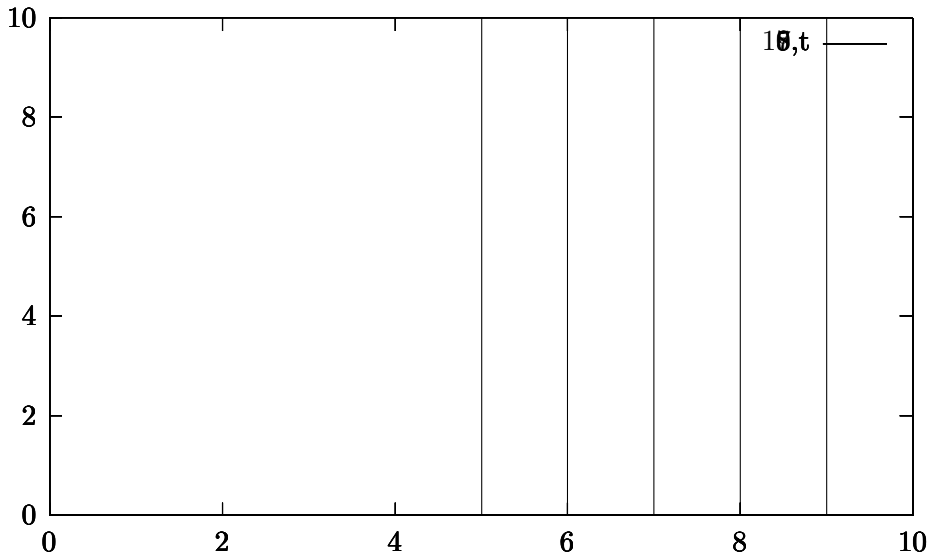
And if we add in **y** then we have
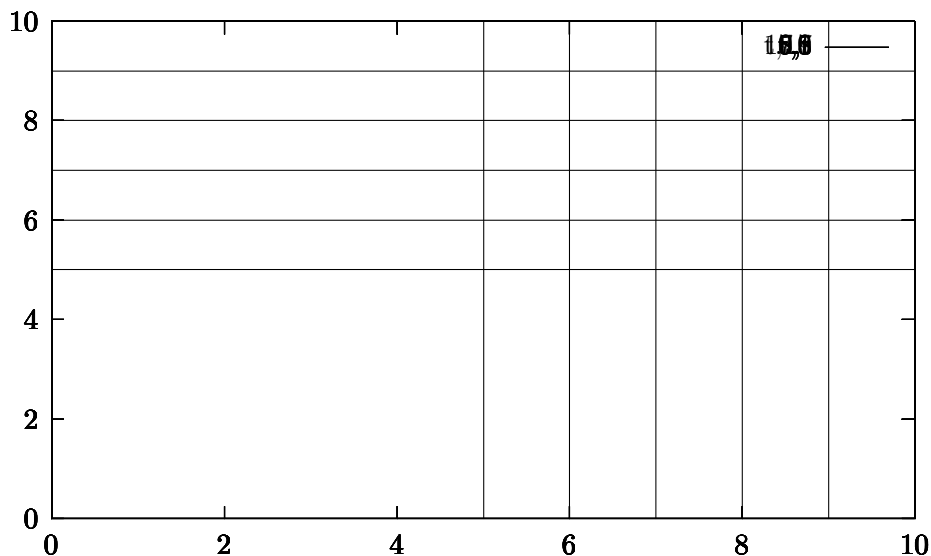
References

1. W. Adkins and S. Weintraub, *Algebra: An approach via module theory*, Graduate Texts in Mathematics, Springer New York, 2012.
2. Jon Allen, *Frobmask—a software program which uses bitmasked sets to find the frobenius numbers of numerical semigroups*, Available at 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.