On the Vector Frobenius Problem

Team Awesome: Jeffrey Amos, Enrique Treviño, Iuliana Pascu, Yan Zhang
Under the Guidance of
Professor Vadim Ponomarenko
Research Experiences for Undergraduates, Trinity University

July 28, 2005

Abstract

Consider $a_1, a_2, \ldots, a_n \in \mathbb{N}$ with $\gcd(a_1, \ldots, a_n) = 1$. Let S be $\{\sum_i a_i x_i \mid x_i \in \mathbb{N}_0, i \in [1, n]\}$, the numerical monoid generated by the a_i. Then there exists a number g such that $g \notin S$ and $y > g \Rightarrow y \in S$.

Finding g is the classical Frobenius problem (sometimes called the Frobenius Coin-Change problem), a subject heavily studied in literature. In this paper, instead of numbers in $\mathbb{N}$, we consider vectors in $\mathbb{Z}^r$. Using this approach, we generalize many one-dimensional theorems proven in earlier papers, and prove new structural facts unique to higher-dimensional cases.

1 Definitions

Let $V = \{\mathbf{v_1}, \ldots, \mathbf{v_k}\} \subset \mathbb{Z}^r$. Define $S_{\mathbb{N}_0}(\mathbf{v_1}, \ldots, \mathbf{v_k})$ to be the set $\{c_1\mathbf{v_1} + \cdots + c_k\mathbf{v_k} | c_1, \ldots, c_k \in \mathbb{N}_0\}$. Similarly set $S_{\mathbb{N}}(\mathbf{v_1}, \ldots, \mathbf{v_k}) = \{c_1\mathbf{v_1} + \cdots + c_k\mathbf{v_k} | c_1, \ldots, c_k \in \mathbb{N}\}$, $S_{\mathbb{Z}}(\mathbf{v_1}, \ldots, \mathbf{v_k}) = \{c_1\mathbf{v_1} + \cdots + c_k\mathbf{v_k} | c_1, \ldots, c_k \in \mathbb{Z}\}$ and $S_{\mathbb{R}}(\mathbf{v_1}, \ldots, \mathbf{v_k}) = \{\alpha_1\mathbf{v_1} + \cdots + \alpha_k\mathbf{v_k} | \alpha_1, \ldots, \alpha_k \in \mathbb{R}\}$.

We say $T \subseteq \mathbb{Z}^r$ is *dense* if there is some $\mathbf{x} \in T$ such that $\mathbf{x} + \mathbf{e_i} \in T$ for all $i = 1, \ldots, r$, where $\mathbf{e_i}$ are the standard basis vectors. We say $T \subseteq \mathbb{Z}^r$ is *volume* if it is not contained in any $(r-1)$-dimensional subspace of $\mathbb{R}^r$.

Define a *simple cone* to be a set of the form $\{\alpha_1\mathbf{v_1} + \cdots + \alpha_r\mathbf{v_r} | \alpha_1, \ldots, \alpha_r \in \mathbb{R}_{\geq 0}\} \cap \mathbb{Z}_0^r$ where the vectors $\mathbf{v_1}, \ldots, \mathbf{v_r}$ are linearly independent over $\mathbb{R}^r$. We say $\mathbf{v_1}, \ldots, \mathbf{v_r}$ are the bounding vectors. Define $cone(\mathbf{a})$ for $\mathbf{a} \in \mathbb{R}^r$ as the set $\{\mathbf{a} + \alpha_1\mathbf{v_1} + \cdots + \alpha_k\mathbf{v_k} | \alpha_1, \ldots, \alpha_k \in \mathbb{R} \text{ and } \alpha_1, \ldots, \alpha_k \geq 0\} \cap \mathbb{Z}^r$. Define the $intcone(\mathbf{a})$ to be $\{\mathbf{a} + \alpha_1\mathbf{v_1} + \cdots + \alpha_k\mathbf{v_k} | \alpha_1, \ldots, \alpha_k \in \mathbb{R} \text{ and } \alpha_1, \ldots, \alpha_k > 0\} \cap \mathbb{Z}^r$. Similarly we define $simplecone(\mathbf{a})$ to be $\{\mathbf{a} + \alpha_1\mathbf{v_1} + \cdots + \alpha_r\mathbf{v_r} | \alpha_1, \ldots, \alpha_r \in \mathbb{R} \text{ and } \alpha_1, \ldots, \alpha_r > 0\}$

Let $RH \in \mathbb{R}^r$ be the set of all points such that for all $\mathbf{q} \in RH$ and for $i = 1, \ldots, r$ there exist $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ with $\alpha_i = 0$ and $\mathbf{q} + \sum_{i=1}^{r} \alpha_i\mathbf{v_i} \in \mathbb{Z}^r$.

We can define a vector relation where $\mathbf{a} < \mathbf{b}$ if $cone(\mathbf{a}) \supset cone(\mathbf{b})$. This relation is clearly reflexive and antisymmetric. Suppose that $\mathbf{a_1} \leq \mathbf{a_2}$ and $\mathbf{a_2} \leq \mathbf{a_3}$. Now there exist non-negative reals $\alpha_1, \ldots, \alpha_k, \alpha_1', \ldots, \alpha_k'$ such that $\mathbf{a_1} + \alpha_1\mathbf{v_1} + \ldots + \alpha_k\mathbf{v_k} = \mathbf{a_2}$ and $\mathbf{a_2} + \alpha_1'\mathbf{v_1} + \ldots + \alpha_k'\mathbf{v_k} = \mathbf{a_3}$. Adding these equations we see that $\mathbf{a_1} + (\alpha_1 + \alpha_1')\mathbf{v_1} + \ldots + (\alpha_k + \alpha_k')\mathbf{v_k} = \mathbf{a_3}$. Thus $\mathbf{a_1} \leq \mathbf{a_3}$ and the relation is a partial ordering.

We will use S to refer to either one of the sets $S_{\mathbb{N}_0}$ or $S_{\mathbb{N}}$. Define a vector $\mathbf{a} \in RH$ to be *complete* in S if every vector in $intcone(\mathbf{a})$ is in S. Define $\mathbf{v} \in RH$ to be an *f-vector* if $\mathbf{v}$ is complete in $S_{\mathbb{N}}$ and there is no $\mathbf{a} < \mathbf{v}$ such that $\mathbf{a}$ is also complete. Define $f(\mathbf{v_1}, \ldots, \mathbf{v_k})$, or the *f-set*, as the set of f-vectors. Define $\mathbf{v} \in RH$ to be a *g-vector* if $\mathbf{v}$ is complete in $S_{\mathbb{N}_0}$ and there is no $\mathbf{a} < \mathbf{v}$ such that $\mathbf{a}$ is also complete. Define $g(\mathbf{v_1}, \ldots, \mathbf{v_k})$, or the *g-set*, as the set of g-vectors. all $\mathbf{a} \in S_{\mathbb{N}}$ complete, $\mathbf{a} \in cone(\mathbf{v})$.

Let $\mathbf{v_1}, \ldots, \mathbf{v_k} \in \mathbb{Z}^r$ and $V = [\mathbf{v_1}, \ldots, \mathbf{v_k}]$. We can select r column vectors to form an $r \times r$ matrix in $\binom{k}{r}$ ways. Let m = $\binom{k}{r}$. We will label their determinates $d_1, \cdots, d_m$. Define $\gcd(\mathbf{v_1}, \ldots, \mathbf{v_k})$ as $\gcd(\mathbf{v_1}, \ldots, \mathbf{v_k}) = \gcd(d_1, \ldots, d_m)$. We define $\gcd(V)$ as $\gcd(V) = \gcd(\mathbf{v_1}, \ldots, \mathbf{v_k})$.

Let $V = \{\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_k}\}$. Assume $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_r} \in \mathbb{Z}^r$ are linearly independent. Let A be the matrix with columns $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_r}$. Let $m(V, \mathbf{a})$ be the set of minimal vectors for the equivalence class [$\mathbf{a}$], i.e $\omega \in m(V, \mathbf{a})$ iff $\omega \in S$, $\omega \equiv \mathbf{a} \mod (A)$ and for all $\mathbf{q} \equiv \mathbf{a} \mod (A)$ either $\omega \leq \mathbf{q}$ or ω is incomparable to $\mathbf{q}$ by cone partial ordering.

Let m(V) be all the minimal vectors. In other words $m(V) = \bigcup m(V, \mathbf{a})$ when $\mathbf{a}$ ranges through all the equivalence classes.

We define a fundamental domain of a vector $\mathbf{v}$:

$fund(\mathbf{v}) = \{\mathbf{v} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i} \mid \alpha_i \in \mathbb{R}\ ,\ 0 < \alpha_i \leq 1 \text{ for } i \in [1, r]\} \cap \mathbb{Z}^r$.

Given $\mathbf{v_1}, \ldots, \mathbf{v_r}$, let $P_i : \mathbb{R}^r \to \mathbb{R}$ be defined as $P_i(\alpha_1 \mathbf{v_1} + \ldots + \alpha_r \mathbf{v_r}) = \alpha_i$. $\{\mathbf{v_1}, \ldots, \mathbf{v_r}\}$ is an $\mathbb{R}$-basis for $\mathbb{R}^r$ so the function is well defined. This function is also a homomorphism. Clearly for any vector $\mathbf{v}$, we have $\mathbf{v} = \sum_{i=1}^{r} \big(P_i(\mathbf{v}) \mathbf{v_i}\big)$. Let $\mathbf{V_A} = \mathbf{v_1} + \ldots + \mathbf{v_r}$.

For D, a finite subset of RH, we define $lub(D)$ as a minimal vector in RH greater than or equal to all vectors in D.

1.1 Cone Ordering

Lemma 1. *Assume* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^r$ *in the simple cone, such that* $\mathbf{x} = \sum_{i=1}^{r} \alpha_i \mathbf{v_i}$ *and* $\mathbf{y} = \sum_{i=1}^{r} \beta_i \mathbf{v_i}$ *where* α_i,$\beta_i \in \mathbb{R}_0$. $\mathbf{x} \geq \mathbf{y}$ *if and only if for all i* $\alpha_i \geq \beta_i$

Proof. Assume $\mathbf{x} \geq \mathbf{y}$. Therefore $\mathbf{x} \in cone(\mathbf{y})$ hence $\mathbf{x} = \mathbf{y} + \sum_{i=1}^{r} \gamma_i \mathbf{v_i}$ where $\gamma_i \in \mathbb{R}_0$ Therefore

$$\mathbf{x} = \sum_{i=1}^{r} (\beta_i + \gamma_i) \mathbf{v_i}$$

and by uniqueness of representations $(\beta_i + \gamma_i) = \alpha_i$. Hence $\alpha_i = \beta_i + \gamma_i \geq \beta_i$.

Assume for all $i \in [1, r]$ we have $\alpha_i \geq \beta_i$. Therefore there exists $\gamma_i \geq 0$ such that $\alpha_i = \beta_i + \gamma_i$. Hence

$$\mathbf{x} = \sum_{i=1}^{r} \alpha_i \mathbf{v_i} = \sum_{i=1}^{r} (\beta_i + \gamma_i) \mathbf{v_i} = \sum_{i=1}^{r} \beta_i \mathbf{v_i} + \sum_{i=1}^{r} \gamma_i \mathbf{v_i} = \mathbf{y} + \sum_{i=1}^{r} \gamma_i \mathbf{v_i}$$

Hence $\mathbf{x} \in cone(\mathbf{y})$, therefore $\mathbf{x} \geq \mathbf{y}$. □

Lemma 1 can also be written in the following form:

Lemma 2. *Given a simple cone,* $\mathbf{x} \geq \mathbf{y}$ *if and only if* $P_i(\mathbf{x}) \geq P_i(\mathbf{y})$ *for* $i = 1, \ldots, r$.

1.2 The f-set and g-set

Lemma 3. *Let $\mathbf{v_1}, \ldots, \mathbf{v_k} \in \mathbb{Z}^r$. Then $\mathbf{v}$ is complete in $S_{\mathbb{N}_0}(\mathbf{v_1}, \ldots, \mathbf{v_k})$ if and only if $\mathbf{w} = \mathbf{v} + \mathbf{v_1} + \ldots + \mathbf{v_k}$ is complete in $S_{\mathbb{N}}(v_1, \ldots, \mathbf{v_k})$.*

Proof. "$\Longrightarrow$" Let $\mathbf{v}$ be a complete vector in $S_{\mathbb{N}_0}(\mathbf{v_1}, \ldots, \mathbf{v_k})$. This means that all the lattice points in $intcone(\mathbf{v})$ are in $S_{\mathbb{N}_0}$. Let $\mathbf{u} = \mathbf{w} + \sum_{i=1}^{k} \alpha_i \mathbf{v_i}$ with $\alpha_i \in \mathbb{R}_{>0}$ be a point in $intcone(\mathbf{w})$. We have $\mathbf{u} = \mathbf{v} + \sum_{i=1}^{k} (\alpha_i + 1)\mathbf{v_i}$. If $\mathbf{u}$ is a lattice point then $\mathbf{u} - (\mathbf{v_1} + \ldots + \mathbf{v_k})$ is also a lattice point. Since $\mathbf{v}$ is complete and $\mathbf{u} - (\mathbf{v_1} + \ldots + \mathbf{v_k}) = \mathbf{v} + \sum_{i=1}^{k} \alpha_i \mathbf{v_i} \in cone(\mathbf{v})$, it must also be in $S_{\mathbb{N}_0}$. So we can write $\mathbf{u} = \sum_{i=1}^{k} d_i \mathbf{v_i} + (\mathbf{v_1} + \ldots + \mathbf{v_k})$ for some $d_i \in \mathbb{N}_0$. Then $\mathbf{u} = \sum_{i=1}^{k} (d_i + 1)\mathbf{v_i}$. Since $d_i + 1 \in \mathbb{N}$ it follows that $\mathbf{u} \in S_{\mathbb{N}}$ so $\mathbf{w}$ is complete in $S_{\mathbb{N}}$.
"$\Longleftarrow$" The proof goes similarly in the other direction. Let $\mathbf{w}$ be a complete vector in $S_{\mathbb{N}}(\mathbf{v_1}, \ldots, \mathbf{v_k})$, so all the lattice points in $intcone(\mathbf{w})$ are in $S_{\mathbb{N}}$. Let $\mathbf{u} = \mathbf{v} + \sum_{i=1}^{k} \alpha_i \mathbf{v_i}$ with $\alpha_i \in \mathbb{R}_{>0}$ be a point in the interior of $cone(\mathbf{v})$. We have $\mathbf{u} = \mathbf{w} - \sum_{i=1}^{k} (\alpha_i + 1)\mathbf{v_i}$. If $\mathbf{u}$ is a lattice point then $\mathbf{u} + (\mathbf{v_1} + \ldots + \mathbf{v_k})$ is also a lattice point. Since $\mathbf{w}$ is complete and $\mathbf{u} + (\mathbf{v_1} + \ldots + \mathbf{v_k}) = \mathbf{w} + \sum_{i=1}^{k} \alpha_i \mathbf{v_i} \in cone(\mathbf{v})$, it must also be in $S_{\mathbb{N}_0}$. So we can write $\mathbf{u} = \sum_{i=1}^{k} d_i \mathbf{v_i} - (\mathbf{v_1} + \ldots + \mathbf{v_k})$ for some $d_i \in \mathbb{N}$. Then $\mathbf{u} = \sum_{i=1}^{k} (d_i - 1)\mathbf{v_i}$. Since $d_i - 1 \in \mathbb{N}_0$ it follows that $\mathbf{u} \in S_{\mathbb{N}_0}$ so $\mathbf{v}$ is complete in $S_{\mathbb{N}_0}$. □

Lemma 4. *Let $\mathbf{v_1}, \ldots, \mathbf{v_k} \in \mathbb{N}_0^r$. Then $\mathbf{g}$ is in the g-set of $\mathbf{v_1}, \ldots, \mathbf{v_k}$ if and only if $\mathbf{f} = \mathbf{g} + (\mathbf{v_1} + \ldots + \mathbf{v_k})$ is in the f-set of $\mathbf{v_1}, \ldots, \mathbf{v_k}$.*

Proof. "$\Longrightarrow$" By Lemma 3, since $\mathbf{g}$ is complete, $\mathbf{f}$ is also complete. We have to show that there exists no vector $\mathbf{a} \in \mathbb{Z}^r$, $\mathbf{a} < \mathbf{f}$ which is complete in $S_{\mathbb{N}}$. Suppose there is such an $\mathbf{a}$. Then $\mathbf{a} - (\mathbf{v_1} + \ldots + \mathbf{v_k}) < \mathbf{g}$ is also complete by the same lemma. Contradiction because $\mathbf{g}$ is in the g-set so it is minimal. Hence $\mathbf{f}$ is minimal so it is in the f-set of $\mathbf{v_1}, \ldots, \mathbf{v_k}$. The proof is similar in the other direction. □

1.3 Characterization of Density and Volume

Lemma 5. *S is dense $\Leftrightarrow \mathbf{e_i} \in S_{\mathbb{Z}}$ for all $i \in [1, r]$.*

Proof. "$\Longrightarrow$" If S is dense then there is some $\mathbf{v} \in S$ such that $\mathbf{v} + \mathbf{e_i} \in S$ for all $i \in [1, r]$. Then each $\mathbf{e_i}$ can be written as a linear combination of the vectors $\mathbf{v_i}$ with integer coefficients by taking $(\mathbf{v} + \mathbf{e_i}) - \mathbf{v} \in S_{\mathbb{Z}}$. Hence $\mathbf{e_i} \in S_{\mathbb{Z}}$ for all $i \in [1, r]$.
"$\Longleftarrow$" If $\mathbf{e_i} \in S_{\mathbb{Z}}$ then there exist $c_{ij} \in \mathbb{Z}$ such that $\mathbf{e_i} = \sum_{j=1}^{k} c_{ij} \mathbf{v_j}$, for all $i \in [1, r]$.
Choose $c_j > |c_{ij}|$, for all $j \in [1, k]$, $i \in [1, r]$. Let $\mathbf{a} = \sum_{j=1}^{k} c_j \mathbf{v_j}$, so $\mathbf{a} \in S$. Then $\mathbf{a} + \mathbf{e_i} = \sum_{j=1}^{k} (c_{ij} + c_j)\mathbf{v_j}$. Since $c_{ij} + c_j \geq 1$ it follows that $\mathbf{a} + \mathbf{e_i} \in S$ for all $i \in [1, r]$. Hence S is dense. □

Lemma 6. *Let $r > k$. Then S is not dense.*

Proof. It has been proven by Novikov [3] that if S is volume then $r \leq k$. Hence if $r > k$, S is not volume and cannot be dense. We give here another proof to this statement.

Assume S is dense. Let A be the matrix with column vectors $\mathbf{v_1}, \ldots, \mathbf{v_k}$. Then $A \in M_{r \times k}(\mathbb{Z})$. From Lemma 5, since S is dense, every basis vector can be written as a linear combination with integer coefficients of the vectors $\mathbf{v_1}, \ldots, \mathbf{v_k}$. Hence there exists $c_i \in M_{n \times 1}(\mathbb{Z})$, $i = 1, \ldots, r$ such that

$$
\begin{aligned}
A \cdot c_1 &= \mathbf{e_1} \\
A \cdot c_2 &= \mathbf{e_2} \\
&\vdots \\
A \cdot c_r &= \mathbf{e_r}
\end{aligned}
$$

We have $AC = I_r$, where $C \in M_r(\mathbb{Z})$ is the matrix with the vectors c_i as columns. Since rank$A \leq k < r$ $\det AC = 0$, hence we cannot have $AC = I_r$. Contradiction, so S is not dense. □

Lemma 7. *$S = S_{\mathbb{N}_0}(V)$ is volume if and only if $\gcd(V) \neq \infty$.*

Proof. First, suppose that S is volume. This means that there exist r vectors in V which are linearly independent. Thus, the matrix M containing these vectors as columns has nonzero determinant. We know that M (or a permutation of its columns) appears in the list of matrices used to calculate $\gcd(V)$. Therefore, $\gcd(V) \neq \infty$ since we know at least one of the matrices has nonzero determinant.

Now suppose that $\gcd(V) \neq \infty$. That means there exists at least one matrix M in the list of matrices used to calculate $\gcd(V)$ which has nonzero determinant. The column vectors of the corresponding matrix M must then be linearly independent over $\mathbb{R}^r$, so we have at least r linearly independent vectors. However, we have at most r linearly independent vectors in $\mathbb{R}^r$, so V has rank r. Thus, S is volume. □

1.4 Generalizing GCD to Vectors

Lemma 8. *Suppose $V = \{\mathbf{v_1}, ..., \mathbf{v_k}\}$ with $\gcd(V) = d$. Then $d\mathbf{e_i} \in S_{\mathbb{Z}}(V)$ for $i \in [1, r]$.*

Proof. Let $M_1, \ldots, M_m$ be the matrices that can be formed by choosing r distinct columns from $\mathbf{v_1}, ..., \mathbf{v_k}$, and let $d_n = |M_n|$ for $n \in [1, m]$. We will prove that for $i \in [1, r]$ and $n \in [1, m]$, we have $d_n\mathbf{e_i} \in S_{\mathbb{Z}}(V)$. For $d_n = 0$ the claim is trivial, so suppose $d_n \neq 0$. We have $M_n^{-1} = \frac{1}{|M_n|} adj(M_n)$. So $M_n \cdot adj(M_n) = |M_n| I_r = d_n I_r$. Because $adj(M_n) \in M_r(\mathbb{Z})$, the columns of $d_n I_r$ are integer linear combinations of the columns of M_n. The columns of M_n are in V and the columns of $d_n I_r$ are $d_n\mathbf{e_i}$ which proves $d_n\mathbf{e_i} \in S_{\mathbb{Z}}(V)$. Because d is an integer linear combination of $d_1, \ldots, d_m$, we know that $d\mathbf{e_i}$ is an integer linear combination of $d_1\mathbf{e_i}, \ldots, d_m\mathbf{e_i}$ for $i \in [1, r]$. Thus for $i \in [1, r]$, $d\mathbf{e_i} \in S_{\mathbb{Z}}(V)$. □

Theorem 1. *$S(V)$ is dense iff $\gcd(V) = 1$.*

Proof. Suppose that $V = \{\mathbf{v_1}, ..., \mathbf{v_k}\}$ with $\gcd(V) = 1$. By Lemmas 8, $\mathbf{e_i} \in S$ for $i \in [1, r]$. By Lemma 5, $S(V)$ is dense.

Next suppose $S(V)$ is dense. Let $M_1, \ldots, M_m$ be the matrices that can be formed by choosing r distinct columns from $\mathbf{v_1}, ..., \mathbf{v_k}$, and let $d_n = |M_n|$ for $n \in [1, m]$. Let W be the $r \times k$ matrix whose columns are $\mathbf{v_1}, \ldots, \mathbf{v_k}$. By Lemma 5, $\mathbf{e_i}$ can be written as an integer linear combination of $\mathbf{v_1}, \ldots, \mathbf{v_k}$ for $i = 1, \ldots, r$. Thus the exists a matrix $B \in M_{k \times r}(\mathbb{Z})$ such that $WB = I_r$.

If T is a subset of $\{1, \ldots, k\}$ with r elements, we write W_T for the $m \times m$ matrix whose columns are those columns of W that have indices from T. Similarly, we write B_T for the $m \times m$ matrix whose rows are those rows of B that have indices from T. The Cauchy-Binet formula then states

$$|WB| = \sum_T |W_T| \cdot |B_T|$$

where T goes over all r element subsets of $\{1, \ldots, k\}$.

Thus $|WB|$ is a linear combination of the determinants of the minors of W, there the coeffients are minors of B and thus integers. But $|WB| = 1$ and the minors of W are $d_1, \ldots, d_m$, thus $1 = \gcd(d_1, ..., d_m) = \gcd(\mathbf{v_1}, \ldots, \mathbf{v_k}) = \gcd(V)$. □

Note that this is a natural generalization of the 1-dimensional case, in which case we have two adjacent integers in S if and only if the generators have $\gcd = 1$ in the classical definition of $\gcd$.

Lemma 9. *Let* $V = \{\mathbf{v_1}, \ldots, \mathbf{v_l}\}$ *and* $W = \{\mathbf{w_1}, \ldots, \mathbf{w_m}\}$ *be two sets of vectors in* $\mathbb{Z}^r$*. Suppose that* $S_{\mathbb{Z}}(V) \subset S_{\mathbb{Z}}(W)$*. Then* $\gcd(W) | \gcd(V)$.

Proof. Let

$$\begin{bmatrix} \mathbf{v_{a_1}} & \mathbf{v_{a_2}} & \ldots & \mathbf{v_{a_r}} \end{bmatrix}$$

be a matrix contributing to $\gcd(V)$, where the $\mathbf{v_{a_i}}$'s are vectors in V. Because $\mathbf{v_{a_i}} \in S_{\mathbb{Z}}(W)$, we may write each $\mathbf{v_{a_i}}$ as a linear $\mathbb{Z}$-combination of vectors in W, giving the form

$$\begin{bmatrix} \sum a_{1i}\mathbf{w_i} & \sum a_{2i}\mathbf{w_i} & \ldots & \sum a_{ri}\mathbf{w_i} \end{bmatrix}$$

where each sum is over i with $1 \leq i \leq l$.

By this reasoning, we see that this determinant, used in the calculation of $\gcd(V)$, is a linear combination of determinants used in the calculation of $\gcd(W)$. Thus $\gcd(W)$ divides this determinant. We can then conclude that $\gcd(W)$ divides every matrix used in the calculation of $\gcd(V)$, which gives us that $\gcd(W) | \gcd(V)$.

□

Corollary 1. *If* $S_{\mathbb{Z}}(V) = S_{\mathbb{Z}}(W)$*, then* $\gcd(V) = \gcd(W)$.

1.5 Useful Lemmas

Following lemmas are for simple cones

Lemma 10. *In a simple cone.* $intcone(\mathbf{a}) = \{\mathbf{a} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i} | \alpha_i \in \mathbb{R}, i \in [1, r]$ *and* $\alpha_i > 0\} \bigcap \mathbb{Z}^r$

Proof.

$$intcone(\mathbf{a}) = \{\mathbf{a} + \sum_{i=1}^{k} \alpha_i \mathbf{v_i} | \alpha_i \in \mathbb{R}, i \in [1, k] \text{ and } \alpha_i > 0\} \bigcap \mathbb{Z}^r.$$

Let, $\mathbf{h} \in intcone(\mathbf{a})$ and $\mathbf{h} = \mathbf{a} + \sum_{i=1}^{k} \alpha_i \mathbf{v_i}$. Hence $\mathbf{h} = \mathbf{h'} + \mathbf{h''}$ where $\mathbf{h'} \in simplecone(\mathbf{a})$ and $\mathbf{h''} = \sum_{i>r} \alpha_i \mathbf{v_i}$ with $\alpha_i > 0$. But $\mathbf{v_i} \in simplecone(\mathbf{a})$ for $i > r$. Hence $\mathbf{h} \in simplecone(\mathbf{a})$.

□

Lemma 11. $fund(\mathbf{g}) \subset intcone(\mathbf{g})$.

Proof. Using Lemma 10:

$$fund(\mathbf{g}) = \{\mathbf{g} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i} | \alpha_i \in \mathbb{R}, \alpha_i \in (0, 1] \text{ for } i \in [1, r]\} \bigcap \mathbb{Z}^r \subset$$

$$\{\mathbf{g} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i} | \alpha_i \in \mathbb{R}_{>0}\} \bigcap \mathbb{Z}^r = intcone(\mathbf{g})$$

□

Lemma 12. $\mathbf{g} \in c(V)$ *if and only if* $fund(\mathbf{g}) \subset S$

Proof. Assume $\mathbf{g} \in c(V)$. And for the sake of contradiction, assume $fund(\mathbf{g}) \not\subset S$ then there exists $\mathbf{w} \in fund(\mathbf{g})$ such that $\mathbf{w} \notin S$. By Lemma 11 $\mathbf{w} \in fund(\mathbf{g})$ implies $\mathbf{w} \in intcone(\mathbf{g})$ therefore $\mathbf{w} \in S$. Contradiction.

Assume $fund(\mathbf{g}) \subset S$. Let $\mathbf{w} \in intcone(\mathbf{g})$. Then, by Lemma 10,

$$\mathbf{w} = \sum_{i=1}^{r} \alpha_i \mathbf{v_i} \text{ where } \alpha_i \in \mathbb{R} \text{ for } i \in [1, r].$$

Let c_i, γ_i be such that $\alpha_i = c_i + \gamma_i$ where $c_i \in \mathbb{N}_0$, $\gamma_i \in \mathbb{R}$ and $\gamma_i < 1$ for $i \in [1, r]$. And let

$$\mathbf{w'} = \sum_{i=1}^{r} \gamma_i \mathbf{v_i} \text{ where } \gamma_i \in \mathbb{R} \text{ for } i \in [1, r].$$

Note $\mathbf{w} = \mathbf{w'} + \sum_{i=1}^{r} c_i \mathbf{v_i} = \mathbf{w'} + \mathbf{w''}$, with $\mathbf{w''} \in S$.

$\mathbf{w'} \in fund(\mathbf{g})$ hence $\mathbf{w'} \in S$ hence $(\mathbf{w'} + \mathbf{w''}) \in S$, therefore $\mathbf{w} \in S$. □

Theorem 2. *If $\omega' \geq \omega \in S$ and $\omega' \equiv \omega \mod (A)$ then $\omega' \in S$.*

Proof. Let $\omega' = \sum_{i=1}^{r} \alpha_i \mathbf{v_i}$ for $\alpha_i \in \mathbb{R}$ and $\omega = \sum_{i=1}^{r} \beta_i \mathbf{v_i}$ for $\beta_i \in \mathbb{R}$. By Lemma 27 $c_i = \alpha_i - \beta_i \in \mathbb{Z}$. Since $\omega \in S$ then $\omega = \sum_{i=1}^{k} b_i \mathbf{v_i}$ where $b_i \in \mathbb{Z}$ for $i \in [1, k]$. Hence

$$\omega' = \omega + \sum_{i=1}^{r} c_i \mathbf{v_i} = \left(\sum_{i=1}^{r} (b_i + c_i) \mathbf{v_i} \right) + \left(\sum_{i=r+1}^{k} b_i \mathbf{v_i} \right).$$

Hence $\omega' \in S$. □

Corollary 2. *If $\omega' \geq \omega \in m(V)$ and $\omega' \equiv \omega \mod (A)$ then $\omega' \in S$.*

Lemma 13. *$\omega \in m(V)$ if and only if $\omega - \mathbf{v_i} \notin S$ for $i \in [1, r]$ and $\omega \in S$.*

Proof. Let $\omega \in m(V)$. Assume that for some i, $\omega - \mathbf{v_i} \in S$. Then $\omega' = \omega - \mathbf{v_i} \equiv \omega \mod (A)$ and $\omega' < \omega$. Contradiction by Theorem 2.

Let $\mathbf{w_i} = \omega - \mathbf{v_i} \notin S$ for $i \in [1, r]$ and $\omega \in S$. Assume $\mathbf{q} \equiv \omega \mod (A)$ and $\mathbf{q} < \omega$ and $\mathbf{q} \in S$ Hence $(\omega - \mathbf{q}) \in S(\mathbf{v_1}, \ldots, \mathbf{v_r})$. So $(\omega - \mathbf{x}) > \mathbf{v_i}$ for some i. So $\mathbf{w_i} = (\omega - \mathbf{v_i}) > \mathbf{x}$ and $\mathbf{w_i} \notin S$, contradiction to Theorem 2.

Therefore $\forall \mathbf{q} < \omega$, $\mathbf{q} \notin S$, together with the fact that $\omega \in S$ we conclude $\omega \in m(V)$. □

Lemma 14. *If $\mathbf{v} \in S$, there exists $\omega \in m(V)$ with $\omega \equiv \mathbf{v} \mod (A)$.*

Proof. Let $\mathbf{w_1} = \mathbf{v}$. $\mathbf{w_1}, \mathbf{w_2}, \ldots$ where $\mathbf{w_i} - \mathbf{w_{i+1}} = \mathbf{v_{f(i)}}$ for some $f(i) \in [1, r]$ and $\forall j$, $\mathbf{w_j} \in S$. If $\mathbf{v_{f(i)}}$ cannot be chosen, that is $\mathbf{w_i} - \mathbf{v_j} \notin S \; \forall j \in [1, r]$, then by Lemma 13 $\mathbf{w_i} \in m(V)$.

But $|\{\mathbf{x} \mid 0 \leq \mathbf{x} \leq \mathbf{v}\}| \leq \infty$ so this must stop.

□

Lemma 15. *If $\mathbf{g'} \in c(V)$, there exists $\mathbf{g} \leq \mathbf{g'}$ such that $\mathbf{g} \in g(V)$.*

Proof. Let $T = \{\mathbf{v} \in RH \bigcap c(V) \mid \mathbf{v} \leq \mathbf{g}'\}$. T is finite, since $|\{\mathbf{x} \mid -V_A \leq \mathbf{x} \leq \mathbf{g}'\}| \leq \infty$.

Let $\mathbf{g} \in T$ be minimal in T. Then there doesn't exist $\mathbf{h} < \mathbf{g}$ such that $\mathbf{h} \in T$, which means that if $\mathbf{h} < \mathbf{g}$ then either $\mathbf{h} \notin c(V)$ or $\mathbf{h} \notin RH$, this fact together with $\mathbf{g} \in c(V)$ and $\mathbf{g} \in RH$ implies $\mathbf{g} \in g(V)$. □

Lemma 16. *If* $\mathbf{a} \in cone(\mathbf{b})$, *then* $\mathbf{b} \leq \mathbf{a}$.

Proof. Since $\mathbf{a} \in cone(\mathbf{b})$ it means that $\mathbf{a} = \mathbf{b} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i}$ for some $\alpha_i \in \mathbb{R}_{\geq 0}$. Let $\mathbf{v} \in cone(\mathbf{a})$. Then $\mathbf{v} = \mathbf{a} + \sum_{i=1}^{r} \beta_i \mathbf{v_i}$ for some $\beta_i \in \mathbb{R}_{\geq 0}$. Hence $\mathbf{v} = \mathbf{b} + \sum_{i=1}^{r} (\beta_i + \alpha_i)\mathbf{v_i}$. So $\mathbf{v} \in cone(\mathbf{b})$. Therefore $cone(\mathbf{a}) \subseteq cone(\mathbf{b})$ and this implies that $\mathbf{b} \leq \mathbf{a}$.

□

Lemma 17. *If* $\mathbf{a} \in fund(\mathbf{b})$, *then* $\mathbf{b} \leq \mathbf{a}$.

Proof. By definition $\mathbf{a} \in fund(\mathbf{b})$ means that $\mathbf{a} = \mathbf{b} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i}$, for some $\alpha_i \in \mathbb{R}_{\geq 0}$. Hence $\mathbf{a} \in cone(\mathbf{b})$, so $\mathbf{b} \leq \mathbf{a}$ by Lemma 16. □

Lemma 18. *If* $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{R}^r$, *then* $\mathbf{a} \leq \mathbf{b} \iff \mathbf{a} + \mathbf{c} \leq \mathbf{b} + \mathbf{c}$.

Proof. It is sufficient to prove this in the forward direction. We have $\mathbf{a} \leq \mathbf{b} \Rightarrow cone(\mathbf{b}) \subseteq cone(\mathbf{a})$. Hence $\mathbf{b} \in cone(\mathbf{a})$ so $\mathbf{b} = \mathbf{a} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i}$, for some $\alpha_i \in \mathbb{R}_{\geq 0}$. Then $\mathbf{b} + \mathbf{c} = \mathbf{a} + \mathbf{c} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i}$, hence $\mathbf{b} + \mathbf{c} \in cone(\mathbf{a} + \mathbf{c})$. Then by Lemma 16 it follows that $\mathbf{a} + \mathbf{c} \leq \mathbf{b} + \mathbf{c}$. □

Lemma 19. *If* $\mathbf{a}, \mathbf{b} \in \mathbb{R}^r$ *and* $\mathbf{c} \in cone(\mathbf{0})$, *then* $\mathbf{a} \leq \mathbf{b} \Rightarrow \mathbf{a} \leq \mathbf{b} + \mathbf{c}$.

Proof. We have $\mathbf{a} \leq \mathbf{b} \Rightarrow cone(\mathbf{b}) \subseteq cone(\mathbf{a})$. Hence $\mathbf{b} \in cone(\mathbf{a})$ so $\mathbf{b} = \mathbf{a} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i}$, for some $\alpha_i \in \mathbb{R}_{\geq 0}$. Since $\mathbf{c} \in cone(\mathbf{0})$ we can write $\mathbf{c} = \sum_{i=1}^{r} \beta_i \mathbf{v_i}$, for some $\beta_i \in \mathbb{R}_{\geq 0}$. We have $\mathbf{b} + \mathbf{c} = \mathbf{a} + \sum_{i=1}^{r} (\alpha_i + \beta_i)\mathbf{v_i}$, hence $\mathbf{b} + \mathbf{c} \in cone(\mathbf{a})$ and it follows that $\mathbf{a} \leq \mathbf{b} + \mathbf{c}$. □

Lemma 20. *Let* $D = \{\mathbf{d_1}, ..., \mathbf{d_m}\}$ *where* $\mathbf{d_i} \in RH$. *Then* $lub(D)$ *is unique, and can be computed as follows:*

$$lub(D) = \sum_{i=1}^{r} \max_{j \in [1,m]} \big(P_i(\mathbf{d_j})\big)\mathbf{v_i}$$

Proof. Now for all $j = 1, \ldots, m$ we have $\sum_{i=1}^{r} \max_{y \in [1,m]} \big(P_i(\mathbf{d_y})\big)\mathbf{v_i} \geq \sum_{i=1}^{r} \big(P_i(\mathbf{d_j})\big)\mathbf{v_i} = \mathbf{d_j}$. Thus $\sum_{i=1}^{r} \max_{j \in [1,m]} \big(P_i(\mathbf{d_j})\big)\mathbf{v_i}$ is greater than or equal to all vectors in D.

Now suppose $\mathbf{w}$ is greater than or equal to all vectors in D. For all $i = 1, \ldots, r$ and for all $j = 1, \ldots, m$ we have $P_i(\mathbf{w}) \geq P_i(\mathbf{d_j})$. Thus $P_i(\mathbf{w}) \geq \max_{y \in [1,m]} \big(P_i(\mathbf{d_y})\big) = P_i\Big(\max_{y \in [1,m]} \big(P_i(\mathbf{d_y})\big)\mathbf{v_i}\Big) =$

$= P_i\Big(\sum_{x=1}^{r} \max_{y \in [1,m]} \big(P_x(\mathbf{d_y})\big)\mathbf{v_x}\Big)$. Finally, we can conclude that $\sum_{i=1}^{r} \max_{j \in [1,m]} \big(P_i(\mathbf{d_j})\big)\mathbf{v_i}$ is the unique minimum with the desired properties. □

1.6 Two Lemmas on Multiplying by D

We will assume that D is a nonsingular matrix with rational coefficients:

Lemma 21. *Suppose we have a cone generated by $v_1, \ldots, v_k$ with bounding vectors $v_1, \ldots, v_n$ in $\mathbb{Z}^r$. Then the cone generated by $Dv_1, \ldots, Dv_k$, where D is nonsingular, has bounding vectors $Dv_1, \ldots, Dv_n$.*

Proof. First, we show that $Dv_1, \ldots, Dv_n$ generate everything else. The points in the new cone have the form

$$\begin{aligned} \sum_{1 \leq i \leq n} a_i D v_i &= D(\sum_{1 \leq i \leq n} a_i v_i) \\ &= D(\sum_{1 \leq i \leq k} b_i v_i) \\ &= \sum_{1 \leq i \leq k} b_i D v_i, \end{aligned}$$

where a_i and b_i are nonnegative rationals, and in the second step we used the fact that $v_1, \ldots, v_k$ generate $v_1, \ldots, v_n$.

Now, it suffices to show that each of the Dv_i is actually a vertex on the convex hull of $S_{\mathbb{R}}(Dv_1, \ldots, Dv_r)$. If not, then without loss of generality Dv_1 can be written as a linear combination of the other Dv_i, and we have

$$\begin{aligned} Dv_1 &= \sum_{2 \leq i \leq k} a_i D v_i \\ v_1 &= \sum_{2 \leq i \leq k} a_i v_i, \end{aligned}$$

a contradiction since the v_i were vertices on the convex hull of $S_{\mathbb{R}}(v_1, \ldots, v_r)$.

□

The main use of this lemma is that we get a well-defined cone, so cone-ordering by inclusion still makes sense. Knowing this, we show that:

Lemma 22. *$a \leq b$ in $S_{\mathbb{R}}(v_1, \ldots, v_r)$ if and only if $Da \leq Db$ in $S_{\mathbb{R}}(Dv_1, \ldots, Dv_r)$.*

Proof. This is really a problem of semantics. Note that the left-hand side simply means:

$$b - a = \sum_i c_i v_i,$$

where the c_i are nonnegative. This obviously implies:

$$Db - Da = \sum_i c_i D v_i,$$

which is just the right-hand side. The converse is almost identical (note we can invert since D is assumed to be nonsingular). □

These results tell us that the points in the two cones have the same partial ordering and very similar structure.

1.7 G-vector test

Theorem 3. *If* $\mathbf{g}$ *is complete then* $\mathbf{g} \in g(V)$ *if and only if for all* $i = 1, \ldots, r$ *there exist* $\alpha_1, \ldots, \alpha_r \in \mathbb{R}_{\geq 0}$ *such that* $\alpha_i = 0$ *and* $\mathbf{g} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i} \in \mathbb{Z}^r - S$.

Proof. Suppose $\mathbf{g} \notin g(V)$. Then there exist a complete point $\mathbf{g}' \in RH$ with $\mathbf{g}' < \mathbf{g}$. There exists some $i \in [1, r]$, such that $P_i(\mathbf{g}') < P_i(\mathbf{g})$. Now for any vector in $\mathbb{Z}^r$ of the form $\mathbf{g} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i}$ with $\alpha_1, \ldots, \alpha_r \in \mathbb{R}_{\geq 0}$ and $\alpha_i = 0$ we have $\mathbf{g} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i} \geq \mathbf{g}' + \big(P_i(\mathbf{g}) - P_i(\mathbf{g}')\big) + \sum_{i=1}^{r} \alpha_i \mathbf{v_i} \in intcone(\mathbf{g}') \subset S$. Thus $\mathbf{g} + \sum_{i=1}^{r} \alpha_i \mathbf{v_i} \notin \mathbb{Z}^r - S$.

Now suppose $\mathbf{g} \in g(V)$. By Lemma 33, there exist $q_1, \ldots, q_r \in \mathbf{Q}$ such that $RH = \{\sum_{i=1}^{r} q_i c_i \mathbf{v_i} | c_1, \ldots, c_r \in \mathbb{Z}\}$. For $i = 1, \ldots, r$ we know that $\mathbf{g}' = \mathbf{g} - q_i \mathbf{v_i}$ is not complete. Thus there exists a vector $\mathbf{x} \in \mathbb{Z}^r$, with $\mathbf{x} \notin S$ and $\mathbf{x} \in intcone(\mathbf{g}')$. There exist $\alpha_1, \ldots, \alpha_r \in \mathbb{R}_{>0}$ such that $\mathbf{x} = \mathbf{g}' + \sum_{i=1}^{r} \alpha_i \mathbf{v_i}$. Because $\alpha_i > 0$ and $\mathbf{x} \in RH$, $\alpha_i \geq q_i$. But $\mathbf{x} \notin intcone(\mathbf{g})$ so $\alpha_i \leq q_i$ and $\alpha_i = q_i$. Thus $\mathbf{x} = \mathbf{g} - q_i \mathbf{v_i} + \sum_{j=1}^{r} \alpha_j \mathbf{v_i} = \mathbf{g} + \sum_{j=1, i \neq j}^{r} \alpha_j \mathbf{v_j} \in \mathbb{Z}^r - S$. □

1.8 Reduction by GCD

Lemma 23. *Let* $D \in M_{r \times r}(\mathbb{Z})$. *Then* $\gcd(D\mathbf{v_1}, \ldots, D\mathbf{v_k}) = |D| \gcd(\mathbf{v_1}, \ldots, \mathbf{v_k})$.

Proof. Let $n = \binom{k}{r}$ and $M_1, \ldots, M_n$ be the matrices formed by taking r distinct column vectors from $\{\mathbf{v_1}, \ldots, \mathbf{v_k}\}$. Now $DM_1, \ldots, DM_n$ are the matrices formed by taking r distinct column vectors from $\{D\mathbf{v_1}, \ldots, D\mathbf{v_k}\}$. Now

$$\begin{aligned} \gcd(D\mathbf{v_1}, \ldots, D\mathbf{v_k}) &= \gcd(|DM_1|, \ldots, |DM_n|) \\ &= |D| \gcd(|M_1|, \ldots, |M_n|) \\ &= |D| \gcd(\mathbf{v_1}, \ldots, \mathbf{v_k}). \end{aligned}$$

□

Let p be a prime number. Let j be maximal in $[0, r]$ such that the first j rows contain some entry not divisible by p. For $i \in [1, j]$, let c_i be minimal so that $p \not| v_{ic_i}$. We say that matrix V is in ***p-form*** if the following conditions hold:

1) $c_1 < c_2 < \ldots < c_j$.

2) The last $r - j$ rows have only entries that are multiples of p.

Lemma 24. *For any* V, *there exists an* $r \times r$ *integer matrix* A *such that* AV *is in p-form and* $|A| = 1$.

Proof. Left multiplying V by an invertible matrix is equivalent to performing a series of elementary row operations on V, so all we must prove is that V can be put in p-form using elementary row operations. First will prove the lemma for a column matrix.

If p divides all entries, V is already in p-form. Suppose that not all entries are divisible by p. We can permute the rows so that some entry, a, not divisible by p is at the top. Because $p \not| a$, the sequence

$0, a, 2a, \ldots, (p-1)a$ is a complete set of residues (mod p). Now for any entry below the first, we can add it to a multiple of a so that the sum is divisible by p. Thus through elementary row operations we can make all entries, besides a, divisible by p. Thus V can be put in p-form which proves the base case.

We will induct on k. The base case $k = 1$ has already been proven. Suppose the lemma is true for $k-1$. First, we can perform elementary row operations so that the left $1 \times r$ sub-matrix is in p-form.
Case 1, All entries in the first column are divisible by p:
We can put the right $r \times (k-1)$ matrix in p-form through elementary row operations, by the inductive assumption. These row operations will leave all entries in the first column divisible by p. This puts V in p-form.
Case 2, In the first column, only the top entry is not divisible by p:
We can put the lower right $(r-1) \times (k-1)$ matrix in p-form through elementary row operations on the bottom $r-1$ rows. These row operations will leave the bottom $r-1$ entries in the first column divisible by p. This puts V in p-form, and proves the lemma. □

Lemma 25. *Let p be a prime with $p|d = \gcd(V)$. Then there exist $V^{'} \in M_{r\times k}[\mathbb{Z}]$ and $P \in M_{r\times r}[\mathbb{Z}]$ such that $V = PV^{'}$ and $|P| = p$.*

Proof. By lemma 24, there exists an $A \in M_{r\times r}[\mathbb{Z}]$ and such that $|A| = 1$ and AV is in p-form. Suppose for contradiction that $j = r$. Let M be the $r \times r$ matrix with columns $v_{c_1}, \ldots, v_{c_r}$. Evaluating (mod p), M is upper triangular so $|M| \equiv v_{1c_1} v_{2c_2} \ldots v_{rc_r} \not\equiv 0$, because none of $v_{1c_1}, \ldots, v_{rc_r}$ are divisible by p. Thus $|M|$ cannot be divisible by p. But $p|d = \gcd(\mathbf{v_1}, \ldots, \mathbf{v_k})$ and the columns of M come from $\mathbf{v_1}, \ldots, \mathbf{v_k}$, so p must divide $|M|$, which is a contradiction. Thus $j < r$, and all entries in the bottom row of AV are divisible by p. Let B be the diagonal $r \times r$ matrix with the first $r-1$ diagonal entries equal to 1 and the last diagonal entry equal to p. Let $P = A^{-1}B$ and $V^{'} = B^{-1}AV \in M_{r\times k}[\mathbf{Q}]$. Left multiplying by B^{-1} divides each entry on the bottom row by p, thus $V^{'} = B^{-1}AV \in M_{r\times k}[\mathbb{Z}]$. Also, $|P| = |A^{-1}B| = |A|^{-1}|B| = 1 \times p = p$. Finally, $V = (A^{-1}B)(B^{-1}AV) = PV'$ which proves the lemma. □

Theorem 4. *Let $d^{'}$ be an integer such that $d^{'}|d$. Then there exist $V^{'} \in M_{r\times k}[\mathbb{Z}]$ and $D \in M_{r\times r}[\mathbb{Z}]$ such that $V = DV^{'}$ and $|D| = d^{'}$ and $\gcd(V^{'}) = \frac{d}{d'}$.*

Proof. Let $p_1, \ldots, p_n$ be primes with $d^{'} = p_1 p_2 \ldots p_n$. We will induct on n. The base case $n = 1$ is lemma 25. Suppose the theorem is true for $n-1$. There exist matrices $D^{'} \in M_{r\times r}[\mathbb{Z}]$ and $V^{''} \in M_{r\times k}[\mathbb{Z}]$ such that $V = D^{'}V^{''}$ and $|D^{'}| = p_1 p_2 \ldots p_{n-1}$. But by lemma 23, $p_1 p_2 \ldots p_n = d^{'} \mid d = \gcd(V) = \gcd(D^{'}V'') = |D^{'}| \gcd(V^{''}) = p_1 p_2 \ldots p_{n-1} \gcd(V^{''})$. Thus $p_n | \gcd(V^{''})$. By lemma 25, there exist $V^{'} \in M_{r\times k}[\mathbb{Z}]$ and $P \in M_{r\times r}[\mathbb{Z}]$ such that $V^{''} = PV^{'}$ and $|P| = p_n$. Let $D = D^{'}P$. Now $|D| = |D^{'}||P| = (p_1 \ldots p_{n-1})(p_n) = d$. Thus $V = D^{'}V^{''} = D^{'}PV^{'} = DV^{'}$. By lemma 23, $\frac{d}{d'} = \frac{\gcd(V)}{d'} = \frac{\gcd(DV^{'})}{d'} = |D| \frac{\gcd(V^{'})}{d'} = \gcd(V^{'})$, which proves the theorem. □

2 Unique g-vector

Lemma 26. *Let $\mathbf{v} \in RH$ such that $cone(\mathbf{v}) \subset S$. Then there exists $\mathbf{v'} \in RH$ such that $\mathbf{v'} < \mathbf{v}$ and $\mathbf{v'}$ is complete.*

Proof. Let $< c_1, \ldots, c_r >$ be the RH-coordinates of $\mathbf{v}$. Take $\mathbf{v'}$ with the RH-coordinates $< c_1 - 1, \ldots, c_r - 1 >$. We then have $\mathbf{v'} < \mathbf{v}$. By the definition of RH-coordinates there are no lattice points strictly in between the boundaries of the cones of $\mathbf{v}$ and $\mathbf{v'}$. Hence $\mathbf{v'}$ is complete. □

Theorem 5. *Let* $\mathbf{g}$ *be a* g*-vector. Then* $\mathbf{g}$ *is the unique* g*-vector if and only if for all* $i \in [1, r]$ *there exists* $\mathbf{w_i} = \sum_{j=1}^{r} \alpha_j \mathbf{v_j} \in \mathbb{Z}^r$ *with* $\alpha_1, \ldots, \alpha_r \in (0, 1]$ *and* $\alpha_i = 0$ *such that for all* $k \in \mathbb{Z}_{\geq 0}$, $\mathbf{g} + k(\mathbf{V_A} - \mathbf{v_i}) + \mathbf{w_i} \notin S$.

Proof. We will prove first that if $\mathbf{g}$ is a g-vector satisfying the condition above, then $\mathbf{g}$ is unique.

Assume there exists another g-vector, call it $\mathbf{g}'$. Since $\mathbf{g}$ and $\mathbf{g}'$ are both minimal complete they are not comparable. So there exist l and m integers, $1 \leq l, m \leq r$ such that $P_l(\mathbf{g}) > P_l(\mathbf{g}')$ and $P_m(\mathbf{g}) < P_m(\mathbf{g}')$.

For l as above there exist vectors $\mathbf{a_k} = \mathbf{g} + k(\mathbf{V_A} - \mathbf{v_l}) + \mathbf{w_l}$ such that for all $k \geq 0$, $a_k \notin S$.

For $j \neq l$ we have $P_j(\mathbf{a_k}) = P_j(\mathbf{g}) + k + P_j(\mathbf{w_j})$. Choose $c \in \mathbb{Z}$ such that $c > \max_j(P_j(\mathbf{g}') - P_j(\mathbf{g}))$. Then $P_j(\mathbf{a_c}) = P_j(\mathbf{g}) + c + P_j(\mathbf{w_j}) > P_j(\mathbf{g}')$ for $j \neq l$, by the choice of c, and $P_l(\mathbf{a_c}) = P_l(\mathbf{g}) > P_l(\mathbf{g}')$. Hence $\mathbf{a_c} \in intcone(\mathbf{g}')$. But $\mathbf{a_c} \notin S$ so $\mathbf{g}'$ is not complete. It follows that $\mathbf{g}$ is the unique g-vector.

In the other direction we will prove the contrapositive. Let $\mathbf{g}$ be a g-vector. There exists some i, $i \in [1, r]$ such that for all $\mathbf{w}_\alpha = \sum_{j=1}^{r} \alpha_j \mathbf{v_j} \in \mathbb{Z}^r$ with $\alpha_i = 0$ and $\alpha_j \in (0, 1], j \neq i$ there exists $k_\alpha \in \mathbb{Z}_{\geq 0}$ such that $\mathbf{g} + k_\alpha(\mathbf{V_A} - \mathbf{v_i}) + \mathbf{w}_\alpha \in S$.

There are a finite number of points of the form $\sum_{j=1}^{r} \alpha_j \mathbf{v_j} \in \mathbb{Z}^r$ with $\alpha_i = 0$ and $\alpha_j \in (0, 1], j \neq i$, specifically at most $\det(A)$. Let k_{max} be the maximum k_α over all points of this form. Let $\mathbf{v} = \mathbf{g} + k_{max}(\mathbf{V_A} - \mathbf{v_i})$.

We will prove that $cone(v) \subset S$. We have $intcone(\mathbf{v}) \subset intcone(\mathbf{g}) \subset S$.

Let $\mathbf{w} \in \partial cone(\mathbf{v})$. We can consider two cases. If $\mathbf{w} = \mathbf{v} + \sum_{j=1}^{r} \beta_j \mathbf{v_j}$ with $\beta_i > 0$ and $\beta_j = 0$ for some $j \neq i$. We have $P_j(\mathbf{w}) = P_j(\mathbf{v}) + \beta_j = P_j(\mathbf{g}) + k_{max} + \beta_j > P_j(\mathbf{g})$ for all $j \neq i$. We also have $P_i(\mathbf{w}) = P_i(\mathbf{v}) + \beta_i > P_i(\mathbf{v}) = P_i(\mathbf{g})$. Therefore $\mathbf{w} > \mathbf{g}$, so $\mathbf{w} \in intcone(\mathbf{g}) \subset S$.

If $\mathbf{w} = \mathbf{v} + \sum_{j=1}^{r} \beta_j \mathbf{v_j}$ with $\beta_i = 0$ then $P_i(\mathbf{w}) = P_i(\mathbf{v}) = P_i(\mathbf{g})$. We have $\mathbf{w} = \mathbf{g} + k_{max}(\mathbf{V_A} - \mathbf{v_i}) + \sum_{j=1}^{r} \beta_j \mathbf{v_j}$. By our assumption there exists k_β such that $\mathbf{w}' = \mathbf{g} + k_\beta(\mathbf{V_A} - \mathbf{v_i}) + \sum_{j=1}^{r} \beta_j \mathbf{v_j} \in S$. We then have $\mathbf{w} - \mathbf{w}' = (k_{max} - k_\beta)(\mathbf{V_A} - \mathbf{v_i})$. Since $k_\beta \leq k_{max}$ and $\mathbf{w}' \in S$ it follows that $\mathbf{w} \in S$. So we have $cone(\mathbf{v}) \subset S$.

Hence by Lemma 26 we can find another vector $\mathbf{v}' < \mathbf{v}$ such that $\mathbf{v}'$ is complete. So $P_i(\mathbf{v}') < P_i(\mathbf{v}) = P_i(\mathbf{g})$ for all $i \in [1, r]$. By Lemma 15 there exists $\mathbf{g}' \leq \mathbf{v}'$ such that $\mathbf{g}'$ is a g-vector. Since $P_i(\mathbf{g}') \leq P_i(\mathbf{v}') < P_i(\mathbf{g})$ we cannot have $\mathbf{g}' = \mathbf{g}$. We cannot have $\mathbf{g}' < \mathbf{g}$ because $\mathbf{g}$ is minimal complete. So there exists another g-vector $\mathbf{g}'$. □

3 Minimal Elements in Sublattices of Congruence Classes

3.1 Mod A

Let $V = \{\mathbf{v_1}, \ldots, \mathbf{v_k}\}$ with S dense. Let A be the $r \times r$ matrix with columns $\mathbf{v_1}, \ldots, \mathbf{v_r}$.

Consider the set $A\mathbb{Z}^r$. Now for any $\mathbf{w_1}, \mathbf{w_2} \in \mathbb{Z}^r$ we have $A\mathbb{Z}^r \subset \mathbb{Z}^r$, $A\mathbf{w_1} + A\mathbf{w_2} = A(\mathbf{w_1} + \mathbf{w_2}) \in A\mathbb{Z}^r$, $A\mathbf{0} + A\mathbf{w_1} = A\mathbf{w_1}$ and $A\mathbf{w_1} + A(-\mathbf{w_1}) = A\mathbf{0} \in A\mathbb{Z}^r$. Addition is component-wise and thus is commutative and associative. Thus $A\mathbb{Z}^r$ is a normal subgroup of $\mathbb{Z}^r$. We define two vectors

$\mathbf{w_1}$ and $\mathbf{w_2}$ to be congruent $\mod (A)$ if $\mathbf{w_1}$ and $\mathbf{w_2}$ are in the same coset of $\mathbb{Z}^r/A\mathbb{Z}^r$. Notice that $\mathbf{v_i} \equiv \mathbf{0}$ for $i = 1, \ldots, r$.

Lemma 27. *Let* $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_0^r$ *such that* $\mathbf{x} = \sum_{i=1}^{r} \alpha_i \mathbf{v_i}$, $\mathbf{y} = \sum_{i=1}^{r} \beta_i \mathbf{v_i}$, *with* $\alpha_i, \beta_i \in \mathbb{R}_0$. *If* $\mathbf{x} \equiv \mathbf{y} \mod (A)$ *then for all* i, $\alpha_i - \beta_i \in \mathbb{Z}$.

Proof. If $\mathbf{x} \equiv \mathbf{y} \mod (A)$ then by definition $\mathbf{x} - \mathbf{y} = \sum_{i=1}^{r} a_i \mathbf{v_i}$ with $a_i \in \mathbb{Z}$. Since the representation of $\mathbf{x} - \mathbf{y}$ as a linear combination of $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_r}$ is unique, for all i $\alpha_i - \beta_i = a_i$. □

It can also be written as:

Lemma 28. *If* $\mathbf{w} \equiv \mathbf{w}'$ *then* $P_i(\mathbf{w}) - P_i(\mathbf{w}') \in \mathbb{Z}$ *for* $i = 1, \ldots, r$.

Theorem 6. *Suppose that* $V = \{\mathbf{v_1}, \ldots, \mathbf{v_{r+1}}\}$, *that* S *is dense, and that* $\{\mathbf{v_1}, \ldots, \mathbf{v_r}\}$ *are linearly independent. Let* A *be the* $r \times r$ *matrix with columns* $\mathbf{v_1}, \ldots, \mathbf{v_r}$. *Then* $\{\mathbf{0}, \mathbf{v_{r+1}}, 2\mathbf{v_{r+1}}, \ldots, (|A| - 1)\mathbf{v_{r+1}}\}$ *is a complete set of coset representatives for* $\mathbb{Z}^r/A\mathbb{Z}^r$. *Also* $|A|$ *is the smallest positive integer such that* $|A|\mathbf{v_{r+1}} \equiv \mathbf{0} \mod (A)$.

Proof. S is dense, so S contains a complete vector, say $\mathbf{g}$. Now for any residue, say $\mathbf{a}$, there exists a vector $\mathbf{v}$ in the interior of $cone(\mathbf{g})$ such that $\mathbf{v} \equiv \mathbf{a}$. Because $\mathbf{g}$ is complete, $\mathbf{v} \in S$ hence there exist $c_1, \ldots, c_{r+1} \in \mathbb{N}_0$ such that $\mathbf{v} = c_1\mathbf{v_1} + \ldots + c_{r+1}\mathbf{v_{r+1}}$. Evaluating this equation $\mod (A)$ have $\mathbf{a} \equiv c_{r+1}\mathbf{v_{r+1}}$. Thus each residue is congruent to some non-negative integer multiple of $\mathbf{v_{r+1}}$.

Now $\mathbb{Z}\mathbf{v_{r+1}}$ is homomorphic map of $\mathbb{Z}$, sending 1 to $\mathbf{v_{r+1}}$, thus $\mathbb{Z}\mathbf{v_{r+1}}$ is a cyclic group $\mod (A)$ generated by $\mathbf{v_{r+1}}$. Because $\mathbb{Z}\mathbf{v_{r+1}}$ contains all residues, the period of $\mathbb{Z}\mathbf{v_{r+1}}$ is the order of $\frac{\mathbb{Z}^r}{A\mathbb{Z}^r}$. We know that $|A| \neq 0$ because V spans $\mathbb{R}^r$ over $\mathbb{R}$, so $\{\mathbf{v_1}, \cdots, \mathbf{v_r}\}$ must be linearly independent over $\mathbb{R}$. Hence the order of $\mathbb{Z}^r/A\mathbb{Z}^r$ is $|A|$ by Theorem 3.3 in [2], and now there are $|A|$ residues. Therefore $\{\mathbf{0}, \mathbf{v_{r+1}}, 2\mathbf{v_{r+1}}, \ldots, (|A|-1)\mathbf{v_{r+1}}\}$ is a complete set of coset representatives for $\mathbb{Z}^r/A\mathbb{Z}^r$, and $|A|$ is the smallest positive integer such that $|A|\mathbf{v_{r+1}} \equiv \mathbf{0} \mod (A)$. □

Theorem 7. *Let* $\mathbf{v_1}, \ldots, \mathbf{v_r}, \mathbf{w}$ *be vectors in* $\mathbb{Z}^r$ *such that* $\{\mathbf{v_1}, \ldots, \mathbf{v_r}\}$ *are linearly independent. Let* A *be the* $r \times r$ *matrix with columns* $\mathbf{v_1}, \ldots, \mathbf{v_r}$. *Then* $\frac{|A|}{\gcd(\mathbf{v_1}, \ldots, \mathbf{v_r}, \mathbf{w})}$ *is the smallest positive integer such that* $\frac{|A|}{\gcd(\mathbf{v_1}, \ldots, \mathbf{v_r}, \mathbf{w})}\mathbf{v_{r+1}} \equiv \mathbf{0} \mod (A)$.

Proof. Let $d = \gcd(\mathbf{v_1}, \ldots, \mathbf{v_r}, \mathbf{w})$. Now by Theorem 4, there exist a matrix D and $\mathbf{v_1}', \ldots, \mathbf{v_r}', \mathbf{w}'$ such that $|D| = d$, $D\mathbf{w}' = \mathbf{w}$, and $D\mathbf{v_i}' = \mathbf{v_i}$ for $i \in [1, r]$. Let A' be the $r \times r$ matrix with columns $\mathbf{v_1}', \ldots, \mathbf{v_r}'$. From the way D was chosen, we know that $\gcd(\mathbf{v_1}', \ldots, \mathbf{v_r}', \mathbf{w}') = 1$. Thus if S' is generated by $\mathbf{v_1}', \ldots, \mathbf{v_r}', \mathbf{w}'$, then S' is dense. By theorem 6, $n = |A'|$ is the smallest positive integer such that $n\mathbf{w}' \in A'\mathbb{Z}$. Now we have $n\mathbf{w}' \in A'\mathbb{Z} \iff Dn\mathbf{w}' \in DA'\mathbb{Z} \iff n\mathbf{w} \in A\mathbb{Z}$. Now the minimal positive integer such that $n\mathbf{w} \in A\mathbb{Z}$ is

$$n = |A'| = \frac{|A'|}{\gcd(\mathbf{v_1}', \ldots, \mathbf{v_r}', \mathbf{w}')} = \frac{|D||A'|}{|D| \gcd(\mathbf{v_1}', \ldots, \mathbf{v_r}', \mathbf{w}')} = \frac{|A|}{\gcd(\mathbf{v_1}, \ldots, \mathbf{v_r}, \mathbf{w})},$$

which proves the theorem. □

Suppose that $V = \{\mathbf{v_1}, \ldots, \mathbf{v_k}\}$, where $S_{\mathbb{R}}(V) \subset S_{\mathbb{R}}(\mathbf{v_1}, \ldots, \mathbf{v_r})$.

Split S into equivalence classes $\mod (A)$, the fundamental domain. In each equivalence class we have a sublattice on which the restriction of our partial ordering is still well-defined. For each of the $|A|$ equivalence classes, take an element of S minimal in the equivalence class. Label these elements $\omega_1, \ldots, \omega_{|\mathbf{A}|}$.

3.2 Results regarding equivalence classes

Theorem 8. *If* $\omega \in m(V)$ *then* $\exists\ a_i \in \mathbb{N}_0$, $i \in [r+1, k]$, $a_i \leq (|A| - 1)$ *such that*

$$\omega = \sum_{i=r+1}^{k} a_i \mathbf{v_i}$$

where $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_r}$ form a simple cone and $\mathbf{v_{r+1}}, \mathbf{v_{r+2}}, \ldots, \mathbf{v_k}$ are inside the cone generated by the first r vectors.

Proof. First, let's prove that $\omega = \sum_{i=r+1}^{k} a_i \mathbf{v_i}$ for $a_i \in \mathbb{N}_0$.

Let $\omega \in m(V)$. Since $\omega \in S$ then $\omega = \sum_{i=1}^{k} a_i \mathbf{v_i}$ with $a_i \in \mathbb{N}_0$ for $i \in [1, k]$.
Assume $\exists j$ such that $1 \leq j \leq r$ and $a_j > 0$
Consider

$$\omega^{'} = \sum_{i=r+1}^{k} a_i \mathbf{v_i}.$$

$a_i \in \mathbb{N}_0$ implies $\omega^{'} \in S$. Also

$$\omega - \omega^{'} = \sum_{i=1}^{r} a_i \mathbf{v_i}.$$

Which implies that $\omega \equiv \omega^{'} \mod (A)$. And, reordering the terms

$$\omega = \omega^{'} + \sum_{i=1}^{r} a_i \mathbf{v_i}$$

we conclude $\omega \in$ cone$(\omega^{'})$ hence $\omega^{'} \leq \omega$. Now since $a_j > 0$ then $\omega^{'} \neq \omega$ hence $\omega^{'} < \omega$ which is a contradiction to $\omega \in m(V)$.

Now if $\omega \in m(V)$, we can write $\omega = \sum_{i=r+1}^{k} a_i \mathbf{v_i}$ with $a_i \in \mathbb{N}_0$
Assume that $\exists j$ such that $a_j \geq |A|$. Let $\omega^{'}$ be

$$\omega^{'} = \omega - |A|\mathbf{v_j} = \left(\sum_{i=r+1}^{k} a_i \mathbf{v_i} \right) - |A|\mathbf{v_j} = \left(\sum_{i=r+1, i\neq j}^{k} a_i \mathbf{v_i} \right) + (a_j - |A|)\mathbf{v_j}$$

Since $a_j \geq |A|$ then the coeficients of $\omega^{'}$ are $\mathbb{N}_0$ so $\omega^{'} \in S$. And by reordering

$$\omega = \omega^{'} + |A|\mathbf{v_j}$$

hence $\omega \in$ cone$(\omega^{'})$ implying $\omega^{'} \leq \omega$. Since

$$\omega - \omega^{'} = |A|\mathbf{v_j} \neq 0,$$

we know that $\omega \neq \omega^{'}$, hence $\omega^{'} < \omega$ and by Theorem 6, we know that

$$\omega^{'} = \omega - |A|\mathbf{v_j} \equiv \omega \mod (A).$$

Therefore $\omega^{'} \equiv \omega \mod (A)$, $\omega^{'} \in S$ and $\omega^{'} < \omega$ which is a contradiction. Hence $\nexists j$ with $1 \leq j \leq r$ such that $a_j \geq |A|$ □

This theorem can also be written as: If $\omega \in m(V)$ then $\omega = \sum_{i=r+1}^{k} a_i \mathbf{v_i}$ for $a_i \in \mathbb{Z}_{|A|}$ for $i \in [r+1, k]$, because $a_i \leq |A| - 1$ and $a_i \in \mathbb{N}_0$.

Corollary 3. $|m(V)| = |\bigcup m(V,a)| = \sum |m(V,a)| \leq |A|^{k-r}$ *where* a *ranges through the* $|A|$ *equivalence classes.*

Proof. $|m(V)| = |\bigcup m(V,a)|$ by definition. And because $m(V,a) \bigcap m(V,b) = \emptyset$ for $a \not\equiv b \mod (A)$ we can conclude that $|\bigcup m(V,a)| = \sum |m(V,a)|$ where a ranges through the $|A|$ equivalence classes. By Theorem 8 Every $\omega \in m(V)$ can be written as $\omega = \sum_{i=r+1}^{k} a_i \mathbf{v_i}$ with $a_i \in \mathbb{Z}_{|A|}$. Let $f : m(V) \mapsto \mathbb{Z}_{|A|}^{k-r}$ where $f(\omega) = (a_{r+1}, a_{r+2}, \ldots, a_k)$ and $a_i \in \mathbb{Z}_{|A|}$ where $\omega \in m(V)$ and $\omega = \sum_{i=r+1}^{k} a_i \mathbf{v_i}$

If $\omega, \omega' \in m(V)$ and $f(\omega) = f(\omega')$ then $\omega = \sum_{i=r+1}^{k} a_i \mathbf{v_i} = \omega'$. So f is injective. Therefore $|m(V)| \leq |\mathbb{Z}_{|A|}^{k-r}| = |A|^{k-r}$.

□

Corollary 4. $|m(V,a)|$ *is finite.*

Proof. $m(V,a) \leq \sum |m(V,a)| \leq |A|^{k-r}$ where a ranges through all the equivalence classes. $|A|^{k-r}$ is a finite number. Therefore $m(V,a)$ is finite. □

Corollary 5. *If* $\omega \in m(V)$ *then* $\exists\ a_i \in \mathbb{N}_0$, $i \in [r+1, k]$, $a_i \leq (\frac{|A|}{\gcd(\mathbf{v_1}, \ldots, \mathbf{v_r}, \mathbf{v_j})} - 1)$ *such that*

$$\omega = \sum_{i=r+1}^{k} a_i \mathbf{v_i}$$

Proof. By Theorem 7 we can change $|A|$ to $\frac{|A|}{\gcd(\mathbf{v_1}, \ldots, \mathbf{v_r}, \mathbf{v_j})}$ and the proof works the same then Theorem 8. □

4 Constructing g(V) from m(V)

This is a direct generalization of a result in [1] which states:

For each i in $[0, a_1)$, let r_i be the smallest element of $S(a_2, \ldots, a_k)$ with $r_i \equiv \max_i(r_i)$. Then $g(S) = r_{max} - a_1$.

Theorem 9. *If* $\mathbf{g} \in g(V)$ *then there exist* $\omega_\mathbf{1}, \ldots, \omega_{|\mathbf{A}|} \in m(V)$*, a complete set of residue classes, such that* $\mathbf{g} + \mathbf{V_A} = lub(\omega_\mathbf{1}, \ldots, \omega_{|\mathbf{A}|})$.

Proof. Let $\mathbf{r_1}, \ldots, \mathbf{r}_{|\mathbf{A}|} \in \mathbb{R}^r$ such that $fund(\mathbf{g}) = \{\mathbf{g} + \mathbf{r_1}, \ldots, \mathbf{g} + \mathbf{r}_{|\mathbf{A}|}\}$. By the definition of $fund(\mathbf{g})$, we have $0 < P_i(\mathbf{r_j}) \leq 1$ for all $i \in [1, r]$ and all $j \in [1, |A|]$. By Lemma 11, we have $\mathbf{g} + \mathbf{r_i} \in S$, and thus there exists a minimal vector $\omega_\mathbf{i} \in m(V)$ such that $\omega_\mathbf{i} \equiv \mathbf{g} + \mathbf{r_i}$ and $\omega_\mathbf{i} \leq \mathbf{g} + \mathbf{r_i}$.

Since $\mathbf{g} \in g(V)$, $\mathbf{g} - q_i \mathbf{v_i}$ is not complete for $i = 1, \ldots r$. By Lemma 11 there exists some real numbers $\alpha_1, \ldots, \alpha_r \in (0, 1]$ such that

$$\mathbf{x} = \mathbf{g} - q_i \mathbf{v_i} + \sum_{y=1}^{r} \alpha_y \mathbf{v_y} \notin S.$$

Because $\mathbf{x} \notin fund(\mathbf{g})$, we have $0 < \alpha_i \leq q_i$ and $\alpha_i \in q_i\mathbb{Z}$ so $\alpha_i = q_i$ and $P_i(\mathbf{x}) = P_i(\mathbf{g})$. But $\mathbf{x}+\mathbf{v_i} \in fund(\mathbf{g})$, so there exist some $j \in [1, |A|]$ such that $\mathbf{x}+\mathbf{v_i} = \mathbf{g}+\mathbf{r_j}$. We have $\omega_\mathbf{j} \equiv \mathbf{g}+\mathbf{r_j} \equiv \mathbf{x}$, so there exist integers $c_1, \ldots, c_r$ such that $\omega_\mathbf{j} + c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} = \mathbf{x}$. But $\mathbf{x} \notin S$, so one of the c_i must be negative. Thus $\omega_\mathbf{j} \not\leq \mathbf{x}$ while $\omega_j \leq \mathbf{x} + \mathbf{v_i}$. By Lemma 2 we have $P_l(\omega_\mathbf{j}) \leq P_l(\mathbf{x} + \mathbf{v_i})$ for all $l = 1, \ldots, r$. We have $P_i(\omega_\mathbf{j}) > P_i(\mathbf{x})$. Combining these we have

$$P_i(\mathbf{x}) - P_i(\omega_\mathbf{j}) < 0 \leq P_i(\mathbf{x} + \mathbf{v_i}) - P_i(\omega_\mathbf{j})$$

where $P_i(\mathbf{x} + \mathbf{v_i}) - P_i(\omega_\mathbf{j}) \in \mathbb{Z}$ by Lemma 28. So $P_i(\omega_\mathbf{j}) = P_i(\mathbf{x} + \mathbf{v_i}) = P_i(\mathbf{g} + \mathbf{V_A})$.

For all $j = 1, \ldots, |A|$ we have

$$P_i(\mathbf{g} + \mathbf{V_A}) \geq P_i(\mathbf{g} + \mathbf{v_j}) \geq P_i(\omega_\mathbf{j}).$$

Thus

$$P_i(\mathbf{g} + \mathbf{V_A}) \geq \max_{y \in [1,|A|]}(P_i(\omega_\mathbf{y})) \geq P_i(\omega_\mathbf{j}) = P_i(\mathbf{g} + \mathbf{V_A})$$

and thus

$$\mathbf{g} + \mathbf{V_A} = \sum_{x=1}^{r} \max_{y \in [1,|A|]}(P_x(\omega_\mathbf{y}))\mathbf{v_x} = lub(\omega_\mathbf{1}, \ldots, \omega_{|\mathbf{A}|}),$$

proving the Theorem. □

Corollary 6. *For any* $\mathbf{g} \in g(V)$*, we have* $\mathbf{g} + \mathbf{V_A} \leq lub\big(m(V)\big)$.

Proof. There exists a subset $\{\omega_\mathbf{1}, \ldots, \omega_{|\mathbf{A}|}\}$ of $m(V)$ such that $\mathbf{g} + \mathbf{V_A} = lub(\omega_\mathbf{1}, \ldots, \omega_{|\mathbf{A}|})$. Now $lub(m(V)) \geq \omega_j$ for all $j \in [1, |A|]$ and so $\mathbf{g} + \mathbf{V_A} = lub(\omega_\mathbf{1}, \ldots, \omega_{|\mathbf{A}|}) \leq lub\big(m(V)\big)$. □

5 Bounding $g(V)$

Although we are now able to bound the size of vectors in $g(V)$, we need to know properties of $m(V)$ beforehand, which might be difficult to compute. The following theorem gives us a way to bound vectors in $g(V)$ by looking at V alone:

Theorem 10. *For any* $\mathbf{g} \in g(V)$*, we have* $\mathbf{g} \leq lub\big((|A|-1)\mathbf{v_{r+1}}, \ldots, (|A|-1)\mathbf{v_k}\big) - \mathbf{V_A}$.

Proof. Suppose $\omega \in m(V)$. By Lemma 8, we know that there exist non-negative integers $c_{r+1}, \ldots, c_k$ with $\omega = c_{r+1}\mathbf{v_{r+1}} + \ldots + c_k\mathbf{v_k}$. Suppose for the sake of contradiction that $c_{r+1} + \ldots + c_k \geq |A|$. Consider the sequence $U = \{\mathbf{0}, \mathbf{v_{r+1}}, \ldots, c_{r+1}\mathbf{v_{r+1}}, c_{r+1}\mathbf{v_{r+1}} + \mathbf{v_{r+2}}, \ldots, c_{r+1}\mathbf{v_{r+1}} + \ldots + c_k\mathbf{v_k}\}$. The sequence is strictly increasing, and thus it has a complete ordering. It has at least $|A| + 1$ terms, so some two are congruent mod(A). Let $\mathbf{a}, \mathbf{b} \in U$ such that $\mathbf{a} > \mathbf{b}$ and $\mathbf{a} \equiv \mathbf{b}$. Now $\omega - \mathbf{a}$ is clearly in S so $\omega - (\mathbf{a} - \mathbf{b}) \in S$. But $\omega > \omega - (\mathbf{a} - \mathbf{b})$ and $\omega \equiv \omega - (\mathbf{a} - \mathbf{b})$, which contradicts the minimality of ω in its residue class. Thus $c_{r+1} + \ldots + c_k \leq |A| - 1$.

Next, we will prove that $\omega \leq lub((|A|-1)\mathbf{v_{r+1}}, \ldots, (|A|-1)\mathbf{v_k})$. Now we have

$$\begin{aligned}
P_i(\omega) &= P_i(c_{r+1}\mathbf{v_{r+1}} + \ldots + c_k\mathbf{v_k}) \\
&= c_{r+1}P_i(\mathbf{v_{r+1}}) + \ldots + c_kP_i(\mathbf{v_k}) \\
&\leq (c_{r+1} + \ldots + c_k) \max_{j \in [r+1,k]}\big(P_i(\mathbf{v_j})\big) \\
&\leq (|A| - 1) \max_{j \in [r+1,k]}\big(P_i(\mathbf{v_j})\big) \\
&= \max_{j \in [r+1,k]}\big((|A| - 1)P_i(\mathbf{v_j})\big)
\end{aligned}$$

By Lemmas 2 and 20 we have $\omega \leq lub((|A|-1)\mathbf{v_{r+1}}, \ldots, (|A|-1)\mathbf{v_k})$ and thus $lub(m(V)) \leq lub((|A|-1)\mathbf{v_{r+1}}, \ldots, (|A|-1)\mathbf{v_k})$ by the definition of lub. Finally, by Corollary 6, we conclude that for any vector $\mathbf{g} \in g(V)$ we have $\mathbf{g} \leq lub\big(m(V)\big) - \mathbf{V_A} \leq lub\big((|A|-1)\mathbf{v_{r+1}}, \ldots, (|A|-1)\mathbf{v_k}\big) - \mathbf{V_A}$. □

The theorem is an r-dimensional generalization of a result of Schur [8] in 1935. When $r = 1$ it becomes Schur's bound exactly, and when $k = r + 1$ the bound is achieved by Theorem 18.

6 Saturation

6.1 v-directed Sets and v-directed Lattice Sets

First, we define the *ray along* $\mathbf{v}$ to be the ray $\mathbf{v} = \mathbb{R}^+\mathbf{v}$ in the same direction of $\mathbf{v}$, starting at the origin.

Now, we define the $\mathbf{v}$-*directed set* $[\mathbf{v}]$ of a set of vectors V as $\mathbf{v} \cap V$. Similarly, define the $\mathbf{v}$-*directed lattice set* $\{\mathbf{v}\}$ to be $\mathbf{v} \cap S(V)$.

Lemma 29. *For a nonzero* $\mathbf{v}$*, there exists an invertible linear transformation* $T : \mathbb{R}^r \to \mathbb{R}^r$ *which induces a monoid isomorphism* T' *between lattice points on* $\mathbf{v}$ *and* $\mathbb{N}_0$.

Proof. Since there are only a finite number of lattice points on $\mathbf{v}$, there exists a unique "first" nonzero lattice point $\mathbf{w}$ on $\mathbf{v}$ such that there are no lattice points of the form $\alpha\mathbf{w}$, $\alpha \in (0, 1)$. There is a unique invertible linear transformation $T : \mathbb{R}^r \to \mathbb{R}^r$ which sends $\mathbf{w}$ to $\mathbf{e_1} = (1, 0, \ldots, 0)$.

Suppose $\mathbf{w}' = (x + y)\mathbf{w}$, where x is integral and $\gamma \in (0, 1)$. This is equal to $x\mathbf{w} + \gamma\mathbf{w}$. $x\mathbf{w}$ has integral coordinates, and $\gamma\mathbf{w}$ does not by definition of $\mathbf{w}$. Thus, $\mathbf{w}'$ cannot be an integral point. Therefore, any lattice point on $\mathbf{v}$ is an integral multiple of $\mathbf{w}$, and will be subsequently sent by T to the lattice point $a\mathbf{e_1}$ for some $a \in \mathbb{N}$.

T^{-1} will send $a\mathbf{e_1}$ to aw, also a lattice point. So the lattice points on the two lines are in bijection. But there is also a natural isomorphism ϕ between points of form $a\mathbf{e_1}$ and $\mathbb{N}_0$, so we are done via the composition $T' = \phi \circ T$.

Both isomorphisms clearly preserve addition properties, so the result is not merely a bijection but a monoid isomorphism, as desired. □

Corollary 7. *Suppose* $\{\mathbf{v}\}$ *is generated by* $u_1 v, \ldots, u_k v$, $u_i \in \mathbb{N}$*, then there is a monoid isomorphism between* $\{\mathbf{v}\}$ *and the one-dimensional monoid in* $\mathbb{N}_0$ *generated by* $(u_1, \ldots, u_k)$.

This means that $\{\mathbf{v}\}$ has a semigroup structure identical to that of the one-dimensional Froebenius problem. So we can give a well-defined "Frobenius vector" for $\{\mathbf{v}\}$. Define $frob(\{\mathbf{v}\})$ as the preimage of g, where g is the generalized Frobenius number $G(\{\mathbf{v}\})$ of the image of $\{\mathbf{v}\}$ after applying T'.

Inspired by the above lemma, we define the first nonzero lattice point in the direction of $\mathbf{v}$ to be the *minimal unit* along $\mathbf{v}$. The set of minimal units along each bounding vector of the cone constitute the *minimal unit set*.

By Corollary 7 above, we also now have an intuitive notion of the lattice points along each ray $\mathbf{v}$, so it makes sense to say that a vector $av \in \mathbf{v}$ comes "before" a vector $bv \in \mathbf{v}$ if $a < b$, and "after" if $a > b$.

6.2 Saturation

Now, define a directed set $[\mathbf{v}]$ to be *full* if $\{\mathbf{v}\} \subset S([\mathbf{v}])$; in other words, for all vectors $\mathbf{w} \in \{\mathbf{v}\}$, $\mathbf{w}$ can be written as a nonnegative linear combination of the $\mathbf{v}$-directed set of V alone.

Finally, we define a set of vectors V to be *saturated* if for all vectors $\mathbf{v} \in V$, the $\mathbf{v}$-directed set $[\mathbf{v}]$ is full.

For example, $V = \{(3,0),(4,4),(5,5),(0,3)\}$ is not saturated since $(3,3) \in S(V) \cap \{(4,4)\}$, but $(3,3) \notin S([4,4])$.

Lemma 30. *Given a set of vectors V, there exists $V' \supset V$ which is satuated. Furthermore, $|V' \backslash V| < \infty$, $S(V') = S(V)$, and $g(V') = g(V)$.*

Proof. We construct V'. Throughout this process, we will only add to V vectors already in $S(V)$. Thus $S(V) \supset S(V')$. Since $S(V) \subset S(V')$ trivially, $S(V) = S(V')$. Consequently, $g(V) = g(V')$.

Suppose $[\mathbf{v}]$ is full for $\mathbf{v} \in V'$. Then adding more vectors from $S(V') = S(V)$ into V' will make $[\mathbf{v}]$ still full, since any linear combination

$$a_1\mathbf{v_1} + \ldots + a_n v_n + b_1\mathbf{v'_1} + \ldots + b_m\mathbf{v'_m}$$

where $\mathbf{v_i} \in V$ and $\mathbf{v'_i} \in V \backslash V'$ can be written as an integral linear combination of just the $\mathbf{v_i}$'s by substituting $\mathbf{v'_i} = \sum c_j \mathbf{v_j}$, where $c_j \in \mathbb{N}_0$ exist since $\mathbf{v'_i} \in S(V)$.

Therefore, it suffices to show that we can make any directed set $[\mathbf{v}]$ full by adding vectors in $S(V)$ to V'. Since the number of directed sets is finite, repeating the process for all such sets creates a set V' which is saturated. New directed sets will also not be created, since we only add vectors in the same directions as vectors we already have.

By Lemma 29, we know that the points in $\{\mathbf{v}\}$ have a semigroup structure and are eventually periodic after some well-defined $frob(\{\mathbf{v}\})$.

Add to V all vectors in $\{\mathbf{v}\}$ between $\mathbf{0}$ and $frob(\{\mathbf{v}\})$. Now, take any vector in $\{\mathbf{v}\}$. If it is between $\mathbf{0}$ and $frob(\{\mathbf{v}\})$, we have already added it. If it is after $frob(\{\mathbf{v}\})$ along the ray $\mathbf{v}$, we can write this vector as some nonnegative linear combination of vectors before $frob(\{\mathbf{v}\})$. Thus, $[\mathbf{v}]$ is full. All of the vectors we added are in S, so S also remains constant, as desired.

Repeating the process for all $[\mathbf{v}]$ finishes our algorithm. Note again that this process is finite since there are only a finite number of directed sets in V, and no new ones are introduced in the process since any added vector is already in an existing directed set. □

Thus, in the above example, we note that $[(3,0)]$ and $[(0,3)]$ are full, but $[(4,4)]$ is not. The points in $[(4,4)] \cap S$ are exactly (a,a), where a is integral and at least 3. We can just insert $(3,3)$ to get $\{(3,0),(0,3),(4,4),(5,5),(3,3)\}$, which is saturated.

Lemma 31. *Suppose V is saturated. Then $frob(\{\mathbf{v}\})$ for any $\mathbf{v} \in V$ is not in $S(V)$.*

Proof. Suppose it were in $S(V)$. Then since V is saturated, it must be a nonegative linear combination of elements in $[\mathbf{v}]$ alone. However, $frob(\{\mathbf{v}\})$'s image g after the isomorphism in Lemma 29 is the Frobenius number of a set of numbers N. This Frobenius number is not in the image of $\{\mathbf{v}\}$. Since we have an isomorphism between $\{\mathbf{v}\}$ and N, g's preimage, aka $frob(\{\mathbf{v}\})$, is not in $\{\mathbf{v}\}$. Thus, this vector is not in S. □

We will show an application of the lemma through an intuitively true theorem:

Theorem 11. *Suppose that $V = [\mathbf{v_1}] \cup \ldots \cup [\mathbf{v_r}]$, the $\mathbf{v_i}$ linearly independent. Then*

$$g(V) = \{\sum_{1 \le i \le r} frob(\{\mathbf{v_i}\})\}.$$

Proof. Suppose $\mathbf{w} \in \{\mathbf{v_i}\}$ for some $\mathbf{v_i}$. Suppose $\mathbf{w} \in S(V)$. By the assumptions $\mathbf{w}$ is a bounding vector of V, so it must be a nonnegative linear combination of elements in $[\mathbf{v_i}]$ alone. So V is saturated.

Take the r bounding vectors for the cone which constitute the minimal spanning set, and denote them $\mathbf{w_1}, \ldots, \mathbf{w_r}$, respectively.

Since V is saturated, we know that $frob(\{\mathbf{v}\})$ for any $\mathbf{v} \in V$ is not in S by Lemma 31. Any vector has a unique representation as a linear combination of the w_i. Suppose $\mathbf{w}$ is complete, and equals

$$a_1\mathbf{w_1} + a_2\mathbf{w_2} + \ldots + a_r\mathbf{w_r},$$

where the a_i are nonnegative integers. We claim that $a_i \geq T'(frob(\{w_i\}))$. If not, then the cone at $\mathbf{w}$ fails to contain any of the lattice points with contribution $T'(frob(\{w_i\}))$ in the w_i direction.

So all complete points have each $a_i \geq T'(frob(\{w_i\}))$ for all i. However, any point satisfying these conditions are complete, since $a_i \geq T'(frob(\{w_i\}))$ means we can get any integer lattice point with an $a_i w_i$ contribution by our isomorphism. So, any complete vector is in the cone of

$$\sum T'(frob(\{w_i\})w_i = \sum frob(\{w_i\}),$$

which is itself a complete vector. So it is the unique element of the g-set. □

7 Hyperplanes Containing Lattice Points

In cones of dimension r, simple or not, the bounding hyperplanes are created by the origin and $r-1$ vectors that have at least one other lattice point on them. We wish to understand the structure of all hyperplanes parallel to one of these.

Inspired by these hyperplanes, we call a hyperplane *rational* (the intuitive meaning of this will become clear) if it passes through either[1]:

- r lattice vectors linearly independent over $\mathbb{R}$, or
- $r-1$ lattice vectors linearly independent over $\mathbb{R}$, plus the origin.

Lemma 32. *A hyperplane*

$$\{(x_1, \ldots, x_n) | x_1a_1 + x_2a_2 + \ldots + x_ra_r = d, a_i \neq 0, d \in \mathbb{Z}\},$$

is rational only if all a_i are rational.

Proof. The hyperplane goes through in either case r integral points $p_1, \ldots, p_r$. Suppose that $p_i = (p_{i1}, \ldots, p_{ir})$. Consider

$$\begin{bmatrix} p_{11} & \ldots & p_{1r} \\ \vdots & \ddots & \vdots \\ p_{r1} & \ldots & p_{rr} \end{bmatrix} \begin{bmatrix} a_1 \\ \vdots \\ a_r \end{bmatrix} = \begin{bmatrix} d \\ \vdots \\ d \end{bmatrix}.$$

Notice this exactly characterizes the conditions we have - the matrix takes the dot product between the points and the coefficients of our plane.

[1]The seemingly different definitions can be reconciled via the natural projection from the affine space $\mathbb{R}^r \cong \mathring{A}^r$ to the corresponding subset of the projective space $\mathbf{P}^r$ with the map $\phi : (a_1, \ldots, a_n) \to (1, a_1, \ldots, a_n)$. Then the two definitions become equivalent - the image of the hyperplane under ϕ contain r linearly independent lattice vectors.

Now, if the vectors are all linearly independent, then the leftmost matrix M they create is invertible. We may find the inverse M^{-1} of the left matrix M. This must have rational values since M contained integral values. Multiply M^{-1} on both sides to get

$$\begin{bmatrix} a_1 \\ \vdots \\ a_r \end{bmatrix} = [M] \begin{bmatrix} d \\ \vdots \\ d \end{bmatrix}.$$

Since d is rational, and M^{-1} contains rational numbers, the a_i are rational.

In the second case, we have $r-1$ linearly independent vectors and a row of 0's. Without loss of generality, this is the final row. By plugging in the origin to the hyperplane equation, we see that $d = 0$. This means we can scale any of the a_i to be rational.

Since the space spanned by the $r-1$ vectors does not have full rank, and $\{\mathbf{e_1}, \ldots, \mathbf{e_r}\}$ form a basis, at least one $\mathbf{e_i}$ is linearly independent with the $r-1$ vectors. Now, scale a_i to be rational. We know that

$$a_1 * 0 + \ldots + a_i * 1 + \ldots a_n * 0$$

takes the rational value a_i. Therefore, we may replace the 0 row in the matrix M by $\mathbf{e_i} = (0, \ldots, 1, 0)$ and the corresponding number in right-hand-side vector by a_i to get

$$\begin{bmatrix} p_{11} & \ldots & p_{1i} & \ldots & p_{1r} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 1 & \ldots & 0 \end{bmatrix} \begin{bmatrix} a_1 \\ \vdots \\ a_r \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ a_i \end{bmatrix}.$$

By the same reasoning as the first case, we can invert the left matrix and conclude that all the a_i's have to be in fact rational.

□

Corollary 8. *A hyperplane is a rational hyperplane if and only if it has the form*

$$\{(x_1, \ldots, x_n) | x_1 a_1 + x_2 a_2 + \ldots + x_r a_r = d, a_i \neq 0 \forall i\},$$

where d and the a_i are all integral, and $\gcd(a_1, \ldots, a_r) | d$.

Proof. Suppose H is rational. Then the a_i have to be all rational, and we may multiply both the a_i's and d by the lcm of the denominators and assume they are integral. Since we know that H goes through at least one integral point, we know an integral linear combination of the a_i gives d. But this means $\gcd(a_1, \ldots, a_r) | d$.

Now suppose H has a form where the d and the a_i are all integral, and $\gcd(a_1, \ldots, a_r) | d$. Then we know it goes through at least one lattice point. Suppose that

$$a_1 y_1 + \ldots + a_r y_r = d.$$

There are two cases: $d \neq 0$, or $d = 0$.

In the case where $d \neq 0$, note that

$$\begin{aligned} a_1(y_1 + a_i) + a_2 y_2 + \ldots + a_i(y_i - a_1) + \ldots + a_r y_r &= a_1 y_1 + a_2 y_2 + \ldots + a_r y_r + a_1 a_i - a_i a_1 \\ &= d, \end{aligned}$$

so $(y_1 + a_i, y_2, \ldots, y_i - a_1, \ldots, y_r)$ is also a lattice point on H for all $i \neq 1$. Consider the matrix formed by these $1 + (r-1) = r$ vectors:

$$\begin{bmatrix} y_1 & y_2 & y_3 & \ldots & y_r \\ y_1 + a_2 & y_2 - a_1 & y_3 & \ldots & y_r \\ y_1 + a_3 & y_2 & y_3 - a_1 & \ldots & y_r \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y_1 + a_r & y_2 & y_3 & \ldots & y_r - a_1 \end{bmatrix}.$$

Subtract the first row from the other rows to get

$$\begin{bmatrix} y_1 & y_2 & y_3 & \ldots & y_r \\ a_2 & -a_1 & 0 & \ldots & 0 \\ a_3 & 0 & -a_1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_r & 0 & 0 & \ldots & -a_1 \end{bmatrix}.$$

This matrix has determinant

$$y_1(-a_1)^{r-1} - y_2 a_2(-a_1)^{r-2} - y_3 a_3(-a_1)^{r-2} - \ldots y_r a_r(-a_1)^{r-2} \quad = \quad (-a_1)^{r-2}(-a_1 y_1 - a_2 y_2 - \ldots - a_r y_r).$$

If the original vectors were linearly dependent, this value would be zero. But we already know that $a_1 \neq 0$, so $a_1 y_1 + \ldots + a_r y_r = d$ would have to be 0, a contradiction. So we have r linearly independent vectors and hence a rational hyperplane.

In the case where $d = 0$, by the same reasoning if $(y_1, \ldots, y_r) \in H$, we also know that every row of

$$\begin{bmatrix} y_1 & y_2 & y_3 & \ldots & y_r \\ y_1 + a_2 & y_2 - a_1 & y_3 & \ldots & y_r \\ y_1 + a_3 & y_2 & y_3 - a_1 & \ldots & y_r \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y_1 + a_r & y_2 & y_3 & \ldots & y_r - a_1 \end{bmatrix}$$

is on H. But we know in particular that one choice of $(y_1, \ldots, y_r)$ is just $(0, \ldots, 0)$. Set the y_i's to 0's to get:

$$\begin{bmatrix} 0 & 0 & 0 & \ldots & 0 \\ a_2 & -a_1 & 0 & \ldots & 0 \\ a_3 & 0 & -a_1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_r & 0 & 0 & \ldots & -a_1 \end{bmatrix}.$$

Note that $a_1 \neq 0$, and for the rightmost $r-1$ coordinates, there is only one vector with a nonzero value in that coordinate, namely $-a_1$. So for some linear combination of the bottom $r-1$ vectors to be 0, every coefficient used must be 0. Thus, the bottom $r-1$ rows form linearly independent vectors, and again we have a rational hyperplane.

□

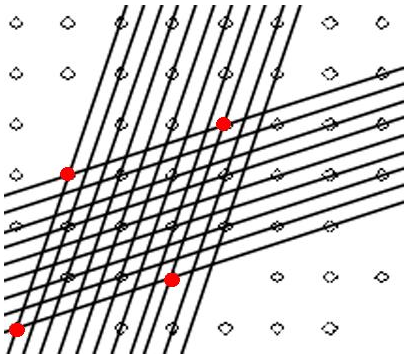

Figure 1: RH is represented by the intersections of the dark lines, which are evenly spaced.

Corollary 9. *The set of rational hyperplanes parallel to*

$$H = \{(x_1, \ldots, x_n) | x_1 a_1 + x_2 a_2 + \ldots + x_r a_r = d, a_i \neq 0 \forall i, \{d, a_1, \ldots, a_r\} \subset \mathbb{Z}\}$$

are exactly those with the form

$$\{(x_1, \ldots, x_n) | x_1 a_1 + x_2 a_2 + \ldots + x_r a_r = d', \gcd(a_1, \ldots, a_r) | d'\}.$$

This means that each family of parallel rational hyperplanes are equidistant from each other with a structure isomorphic to $\mathbb{Z}$.

In particular, we have a notion of the "closest" rational hyperplane parallel to a rational hyperplane H in one of two directions.

Lemma 33. *Given a simple cone generated by $v_1, \ldots, v_r$, there exist $a_1, \ldots, a_r \in \mathbf{Q}$ such that $RH = \{\sum_{1 \leq i \leq r} c_i a_i v_i | c_1, \ldots, c_r \in \mathbb{Z}\}$.*

Proof. Each point in RH is the intersection of r rational hyperplanes, each of the form $H_i = \{x | P_i(x) = d_i\}$. There is some integer f_i for which there exist exactly f_i rational hyperplanes parallel to H_i between H_i and the hyperplane $\{x | P_i(x) = 0\}$ (counting both hyperplanes). Then this point is exactly of the form $\{\sum_{1 \leq i \leq r} (f_i - 1) a_i v_i | f_1, \ldots, f_r \in \mathbb{Z}\}$, where $a_i v_i$ is the unique vector which is the distance between two adjacent rational hyperplanes parallel to H_i in the direction of v_i.

On the other hand, any point of the given form is the intersection of some r corresponding H_i, since we can just pick the H_i to be the rational hyperplane such that it has $c_i + 1$ rational hyperplanes between it and the hyperplane going through the origin. So RH is exactly characterized by the given form. □

Now, we can refer to each point in RH by a set of *RH-coordinates* $\langle c_1, \ldots, c_r \rangle$ defined as in Lemma 33. The corresponding point is simply

$$\sum_{1 \leq i \leq r} c_i \mathbf{v_i'},$$

where $\mathbf{v_i'} = a_i \mathbf{v_i}$. The transformation from the cartesian coordinates to the RH-coordinates is clearly an affine transformation in $\mathbb{R}^r$.

8 Integral g-vectors

Do we keep this section? It really depends on if you care about integral g-vectors at all. Ironically I use a couple of these for my theorems - but they are not that necessary.

8.1 Minimal Fundamental Domain

Recall that the first lattice vector in the direction of each of the bounding vectors $v_1, \ldots, v_r$ of a simple cone create the minimal spanning set $MS = \{v_1', \ldots, v_r'\}$. Now, we may define a domain using these vectors[2]. Call this the *minimal fundamental domain.* Notice that the fundamental domain can naturally be divided into minimal fundamental domains.

8.2 When $\gcd(MS) = 1$

When $\gcd MS = 1$, we have from Theorem 6 that the minimal fundamental domain contains a single lattice point. This case has many interesting properties.

Lemma 34. *Suppose* $\mathbf{a}$ *and* $\mathbf{b}$ *are simple cones,* a *and* b *integral vectors. Then* $cone(\mathbf{a}) \cap cone(\mathbf{b}) = cone(\mathbf{c})$*, where* $\mathbf{c}$ *is also an integral vector.*

Proof. (Yan is Lazy) □

Lemma 35. *A complete integral vector* g *is an integral* g*-vector if and only if there are no integral* g*-vectors in its reverse minimal fundamental domain.*

Proof. □

The main structural fact of V where $\gcd(MS) = 1$ is that $S(V)$ is isomorphic to $S(V')$, where V' has r bounding vectors along the axes, giving a cone in the shape of $\mathbb{R}_+^r$.

Note that in particular the classical 1-dimensional case always has $\gcd(MS) = 1$.

The most important facet of this case is:

Lemma 36. *When* $\gcd(MS) = 1$*,* $RH = \mathbb{Z}^r$.

Theorem 12. *When* $\gcd(MS) = 1$*, the set of integral* g*-vectors is the set of* g*-vectors.*

8.3 Correspondence

Theorem 13. *There is a many-to-one map* ϕ *which sends any integral* g*-vector to a* g*-vector, with fibres of cardinality at most* $\gcd(MS)$.

9 Constructing V to Tailor a Specific g-set

9.1 The General Case

Call a cone *legal* if each of its bounding hyperplanes are rational. Clearly all cones arising from a set of vectors with integral coordinates are legal, since each bounding hyperplane goes through the origin and $r - 1$ other integral points.

[2]This requires generalizing the notion of "mod A" to domains of our choice. This footnote will serve as a reminder.

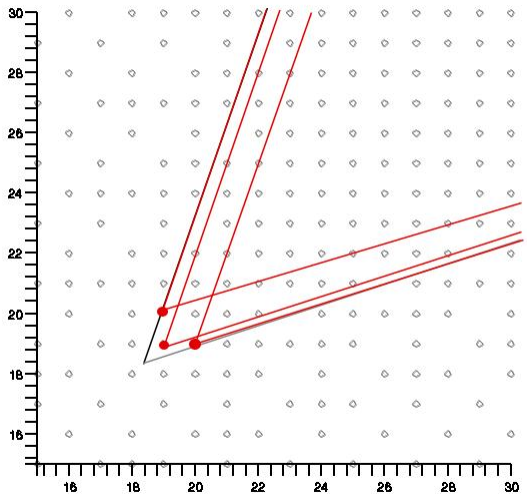

Figure 2: One g-vector includes more than one integral g-vectors in its cone.

Lemma 37. *Given a legal simple cone C and a set of h vectors $G = \{\mathbf{g_1}, \ldots, \mathbf{g_h}\} \subset RH$, there exists some set of vectors V with cone C such that $G \subset g(V)$ if and only if:*

1. *Supposing that $\mathbf{g_i}$ has RH-coordinates $\langle g_{i1}, \ldots, g_{ir}\rangle$, we have $g_{ij} \geq -1$ for all (i, j);*
2. *for all i and a bounding hyperplane H of $\mathbf{g_i}$,*

$$(0, \ldots, 0) \cup (\bigcup intcone(\mathbf{g_j})) \not\supset (\mathbb{Z}^r \cap H \cap cone(\mathbf{g_i}));$$

Proof. $\Rightarrow$:

We construct such a V. First, we want it to have C as its cone.

Now, for each bounding hyperplane H of each $\mathbf{g_i}$, by hypothesis there exists at least one lattice point $\mathbf{a_{H,g_i}}$ in $(\mathbb{Z}^r \cap H \cap cone(\mathbf{g_i})$ which is not the origin, and is also not contained in $\bigcup_{j \neq i} intcone(\mathbf{g_j})$.

Choose each $\mathbf{v_i}$ large enough so that for any of the finite choices of the ordered pair $(H, \mathbf{g_i})$, we have $\mathbf{a_{H,g_i}} = \sum_j a_{H,\mathbf{g_i},j}\mathbf{v_j}$, where $a_{H,\mathbf{g_i},j} < 1$. Hence, it is impossible to choose nonnegative integral coefficients $c_1, \ldots, c_r$ such that $a_{H,\mathbf{g_i},j} = \sum_k c_k \mathbf{v_k}$.

Now, for each vector in G, add to V all $|A|$ lattice points in its fundamental domain. Since we know that the g_{ij} are at least -1, lattice points in the $intcone(\mathbf{g_i})$ will have only nonnegative RH-coordinates, and therefore be in our cone. Call these vectors

$$\mathbf{v_{11}}, \ldots, \mathbf{v_{1|A|}}, \mathbf{v_{21}}, \ldots, \mathbf{v_{2|A|}}, \ldots, \mathbf{v_{h1}}, \ldots, \mathbf{v_{h|A|}},$$

where the $|A|$ points in the fundamental domain of $\mathbf{g_i}$ are $\mathbf{v_{i1}}$ through $\mathbf{v_{i|A|}}$. Note that some two $\mathbf{v_{ij}}$'s might be identical.

We assert that every element $\mathbf{g_i} \in G$ is in the g-set. Since $fund(\mathbf{g_i}) \subset S(V)$, $\mathbf{g_i}$ is complete by Lemma 11. It now suffices to show that $\mathbf{g_i}$ is minimal. We prove by contradiction.

Suppose for contradiction that there is some complete vector $\mathbf{g'} \in RH$ with $\mathbf{g_i}$ in its cone. We may assume that $\mathbf{g'}$ is on one of the bounding vectors of $cone(\mathbf{g_i})$, and $\mathbf{g'}$ is one fundamental distance away from $\mathbf{g_i}$. Without loss of generality, suppose this vector is parallel to $\mathbf{v_1}$, and $\mathbf{g'}$ has RH-coordinates $\langle g_{i1} - 1, g_{i2}, \ldots, g_{ir}\rangle$.

Set H to be the rational hyperplane $\{\langle x_1, \ldots, x_r\rangle | x_1 = g_{i1}\}$. By assumption, there exists some vector $\mathbf{p} = a_{H,g_i}$ in the interior of $H \cap cone(\mathbf{g_i})$ such that $\mathbf{p}$ is not in $intcone(\mathbf{g_j})$, $j \neq i$. $\mathbf{p} \in intcone(\mathbf{g'})$, so $\mathbf{p} \in S(V)$. Therefore,

$$\mathbf{p} = \sum_i b_i \mathbf{v_i} + \sum_{i,j} b_{ij} \mathbf{v_{ij}},$$

where the b_i and b_{ij} are nonnegative integers. □

If $b_{kl} \neq 0$ for some (k, l), we would have $\mathbf{p} \in cone(\mathbf{v_{kl}}) \subset intcone(\mathbf{g_k})$. However, this would mean $\mathbf{p} \in intcone(\mathbf{g_k})$. This is impossible for $k = i$ since $\mathbf{p}$ is on the boundary of $\mathbf{g_k}$. This is also impossible for $k \neq i$ by the choice of $\mathbf{p}$. So, $b_{kl} = 0$ for all (k, l), and we know that we may write

$$\mathbf{p} = \sum_i b_i \mathbf{v_i},$$

where the b_i would be nonnegative integers. Recall that our choice of $\mathbf{v_i}$ made it so that this would not be possible for any points of the form a_{H,g_i}, one of which being $\mathbf{p}$. So we have a contradiction.

$\Leftarrow$: Suppose the first condition is violated, and some $g_{ij} \leq -2$. Then $intcone(\mathbf{g_i}) \cap H$, where $H = \{\langle h_1, \ldots, h_r\rangle | h_j = g_{ij} + 1\}$, will contain (infinitely many) lattice points. But these lattice points are not in $cone(\mathbf{0})$, and so cannot be elements of S. This means $\mathbf{g_i}$ cannot be complete, a contradiction.

Suppose the second condition is violated. Then for some $(H, \mathbf{g_i})$ we have that

$$(0, \ldots, 0) \cup (\bigcup intcone(\mathbf{g_j})) \supset (\mathbb{Z}^r \cap H \cap cone(\mathbf{g_i}).$$

However, since the $\mathbf{g_j}$ are complete, the lattice points in $\bigcup intcone(\mathbf{g_j})$ all have to be in S. $(0, \ldots, 0)$ is also always in S. This means that there is some bounding hyperplane for $\mathbf{g_i}$ with all lattice points in S, meaning $\mathbf{g_i}$ cannot be a g-vector. So we have a contradiction yet again.

9.2 When $|V| = r + 1$

Theorem 14. *Let $\mathbf{a} = (a_1, \ldots, a_r) \in \mathbb{Z}^r$. There exists a vector set V of $r + 1$ vectors with a simple cone and $g(V) = \{\mathbf{a}\}$ if and only if $a_i \equiv 1 \pmod 2$ for some i.*

Proof. Suppose that $a_i \equiv 1 \pmod 2$ for some i. Without loss of generality, assume that $i = 1$.

Note that $\mathbb{Z}^r = \bigcup S(\{\pm e_1, \pm e_2, \ldots, \pm e_r\})$, one orthant for each choice of signs before the e_i. Take an orthant that $\mathbf{a}$ lies in (it could be one of several). Suppose the corresponding spanning set is

$$\{\mathbf{v_1} = b_1\mathbf{e_1}, \mathbf{v_2} = b_2\mathbf{e_2}, \ldots, \mathbf{v_r} = b_r\mathbf{e_r}\},$$

where each b_i is ± 1. We claim that the vectors

$$V = \{2\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_r}, \mathbf{v_{r+1}} = (\mathbf{a} + 2\mathbf{v_1} + \mathbf{v_2} + \ldots + \mathbf{v_r})\}$$

has gcd 1. Furthermore, $g(V) = \{\mathbf{a}\}$.

To see this, first observe that $\mathbf{v_{r+1}} \in cone(\mathbf{a})$. Also, $\mathbf{a} \in S_{\mathbb{R}^+}(\mathbf{v_1}, \ldots, \mathbf{v_r}$ by construction and subsequently is also in $S_{\mathbb{R}^+}(\mathbf{2v_1}, \ldots, \mathbf{v_r})$.

Note that

$$\begin{bmatrix}2\mathbf{v_1} & \dots & \mathbf{v_r}\end{bmatrix} = \begin{bmatrix}\pm 2 & 0 & \dots & 0 \\ 0 & \pm 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \pm 1\end{bmatrix}$$

is a matrix with determinant ± 2, and

$$\begin{bmatrix}\mathbf{v_{r+1}} & \mathbf{v_2} & \dots & \mathbf{v_r}\end{bmatrix} = \begin{bmatrix}a_1 \pm 2 & 0 & \dots & 0 \\ a_2 \pm 1 & \pm 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_r \pm 1 & 0 & \dots & \pm 1\end{bmatrix}$$

is a matrix with determinant $\pm(a_i \pm 2)$. These are relatively prime, so $\gcd(V) = 1$ and we may use Theorem 18 to get that the g-set contains the unique element

$$\begin{aligned}\mathbf{g} &= (|\det(\begin{bmatrix}2\mathbf{v_1} & \mathbf{v_2} & \dots \mathbf{v_r}\end{bmatrix})| - 1)\mathbf{v_{r+1}} - 2\mathbf{v_1} - \mathbf{v_2} - \dots - \mathbf{v_r} \\ &= (|2| - 1)(\mathbf{a} + 2\mathbf{v_1} + \mathbf{v_2} + \dots \mathbf{v_r}) - 2\mathbf{v_1} - \mathbf{v_2} - \dots - \mathbf{v_r} \\ &= \mathbf{a},\end{aligned}$$

as desired.

Now suppose $g(V) = \{\mathbf{v_1}, \dots, \mathbf{v_{r+1}}\} = \{\mathbf{a}\}$, $\mathbf{a}$ has integral coordinates, V is dense, and V has a simple cone generated by $\mathbf{v_1}, \dots, \mathbf{v_r}$. We claim that $\mathbf{a}$ has at least one coordinate which is $1 \pmod 2$. Suppose otherwise. Then,

$$\mathbf{a} = (|\det(\begin{bmatrix}\mathbf{v_1} & \mathbf{v_2} & \dots \mathbf{v_r}\end{bmatrix})| - 1)\mathbf{v_{r+1}} - \mathbf{v_1} - \mathbf{v_2} - \dots - \mathbf{v_r}$$

must have only even coordinates. There are two cases, depending on the parity of the determinant of $D = \begin{bmatrix}\mathbf{v_1} & \mathbf{v_2} & \dots & \mathbf{v_r}\end{bmatrix}$.

If $\det(D)$ is odd, then $(|\det(\begin{bmatrix}\mathbf{v_1} & \mathbf{v_2} & \dots \mathbf{v_r}\end{bmatrix})| - 1)\mathbf{v_{r+1}}$ has all even coordinates. Label the coordinates of $\mathbf{a}$ to be $a_1, \dots, a_r$ respectively. Similarly label the coordinates of each $\mathbf{v_i}$ to be $\mathbf{v_{i,1}}, \dots, \mathbf{v_{i,r}}$. We then have $a_i \equiv \sum_{1 \le j \le r} v_{i,j} \pmod 2$ for all i. This means that each row of D has an even number of odd integers.

Put D in 2-form via elementary row operations. By Lemma 23, with only row operations we may get a matrix A with $AD = D'$ having only even entries under the diagonal and $\det(D) = \det(D')$.

However, row operations do not change the fact that every row has an even number of odd integers, so the number of odd integers in the last row of D' must be even. Since that row has the first $r - 1$ numbers even, the last entry in the row must also be even, giving D' a row of even numbers and hence even determinant. Therefore, D also has even determinant, a contradiction.

On the other hand, suppose $\det(D)$ is even, then $(|\det(D)| - 1)\mathbf{v_{r+1}}$ has coordinates with the same parity as that of $\mathbf{v_{r+1}}$. Therefore, $v_{(r+1),j} \equiv \sum_{1 \le i \le r} v_{i,j} \pmod 2$.

Now consider the $gcd(V)$. There are $\binom{r+1}{r} = r + 1$ matrices involved. One of them is just D, which has even determinant.

The other r matrices take the form

$$\begin{bmatrix}\mathbf{v_1} & \dots & \hat{\mathbf{v}}_\mathbf{j} & \dots & \mathbf{v_{r+1}}\end{bmatrix},$$

where $\mathbf{v_j}$ is missing from the columns. Now, when taken $\pmod 2$, the determinant of this matrix is equal to the determinant of

$$\begin{bmatrix} v_{1,1} & \dots & \hat{v_{j,1}} & \dots & v_{r+1,1} \\ v_{1,2} & \dots & \hat{v_{j,2}} & \dots & v_{r+1,2} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ v_{1,r} & \dots & \hat{v_{j,r}} & \dots & v_{r+1,r} \end{bmatrix} = \begin{bmatrix} v_{1,1} & \dots & \hat{v_{j,1}} & \dots & \sum_{1\le i\le r} v_{i,1} \\ v_{1,2} & \dots & \hat{v_{j,2}} & \dots & \sum_{1\le i\le r} v_{i,2} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ v_{1,r} & \dots & \hat{v_{j,r}} & \dots & \sum_{1\le i\le r} v_{i,r} \end{bmatrix}$$
$$= \begin{bmatrix} \mathbf{v_1} & \dots & \hat{\mathbf{v_j}} & \dots & \mathbf{v_1} + \mathbf{v_2} + \dots + \mathbf{v_r} \end{bmatrix}.$$

Elementary row/column operations of the matrix viewed $\pmod 2$ do not change the determinant $\pmod 2$; that is to say, they do not change the parity of the determinant. We may subtract one copy of each of the first $r-1$ columns from the last to get

$$\begin{bmatrix} \mathbf{v_1} & \dots & \hat{\mathbf{v_j}} & \dots & \mathbf{v_r} & \mathbf{v_j} \end{bmatrix}.$$

The left $r-1$ columns of the matrix are the vectors $\mathbf{v_1}, \dots, \mathbf{v_r}$, missing $\mathbf{v_j}$. Since the rightmost column is $\mathbf{v_j}$, this matrix has exactly the columns of D up to a permutation, which has determinant $0 \pmod 2$ by assumption. Therefore, any of the r matrices found this way has 2 dividing the determinant. We then conclude $2 | \gcd(V)$, which contradicts that V must be dense for $g(V)$ to be defined. □

Corollary 10. *Any vector* $\mathbf{g}$ *which is not the origin in* $\mathbb{Z}^r$ *can be made to be the unique element of the generalized* G*-set for some set of vectors* V*.*

Proof. If there is an odd coordinate in $\mathbf{g}$, we just use the theorem. Otherwise, since $\mathbf{g} = (g_1, \dots, g_r)$ has at least one nonzero coordinate, we may write it as $k(g_1', \dots, g_r')$, where $\gcd(g_1', \dots, g_r') = 1$ and $k \in \mathbb{N}$. Therefore, at least one of g_i' is odd, and $\{g/k\} = g(V')$ for some V'. $V = kV'$ suffices by Theorem 22. □

9.3 When $r+1$ Vectors do not Suffice

First, we prove a general result in 1-dimension:

Lemma 38. *If* $k \not| g \in \mathbb{N}_0$*, then the set* $V = \{a_0, \dots, a_{k+1}\}$*, where*

$$\begin{aligned} a_0 &= k \\ a_1 &= g+1 \\ a_2 &= g+2 \\ &\dots \\ a_k &= g+k \end{aligned}$$

has the following properties:

1. $g(a_0, \dots, a_k) = g$*;*
2. *For any* $m > g$*, there exists* $n > m$ *such that if we write* $n = \sum_{0\le i\le k} b_i a_i$*,* b_i *nonnegative integers, then* $\sum_{1\le i\le k} b_i \ge 1$*;*

3. *take integral $n > g$. There exists a way to write $n = \sum_{0 \le i \le k} b_i a_i$, b_i nonnegative integers, and $\sum_{1 \le i \le k} b_i \ge 1$;*

Proof. 1. Take any $n > g$. n has some residue $n' \pmod k$. If $n' \neq 0$, then $n \ge g + n'$, which is in V. $n - (g + n') = bk$ for some $b \in \mathbb{N}_0$. Since $k \in V$, $n \in S(V)$. Now, if $g \in S(V)$, then $g = \sum_i c_i a_i$, $c_i \in \mathbb{N}_0$. Clearly $c_i = 0$ for $i \ge 1$, so $g = bk$ for some $b \in \mathbb{N}_0$, a contradiction since $k \not| g$.

2. Simply take some $n > m$ such that $n \not\equiv 0 \pmod k$. Then to write $n = \sum_i c_i a_i$, multiples of $a_1 = k$ alone cannot suffice, so we need at least one of the others. Thus, $c_i \ge 1$ for some i.

3. In the construction of our solution for the first part of this lemma, we used only one multiple of $g + n'$ and b multiples of k. Thus, we have $n = ba_1 + a_i$ for some i, which has $\sum_{1 \le i \le k} c_i$ equal to 1 for $k \not| n$, and 0 otherwise.

□

Theorem 15. *Let $\mathbf{g} = (g_1, \ldots, g_r)$, $g_i \in \mathbb{Z}$. If k does not divide some g_i, then there exists $r + k$ vectors forming V such that $g(V) = \{\mathbf{g}\}$.*

Proof. Without loss of generality, suppose that $k \not| g_1$. Similar to before, take an orthant that $\mathbf{g}$ lies in (it could be one of several). Suppose the corresponding spanning set is

$$\{\mathbf{v_1} = b_1\mathbf{e_1}, \mathbf{v_2} = b_2\mathbf{e_2}, \ldots, \mathbf{v_r} = b_r\mathbf{e_r}\},$$

where each b_i is ± 1. We claim that the set V of vectors

$$\begin{aligned} & k\mathbf{v_1}, \\ & \mathbf{v_2}, \\ & \ldots, \\ & \mathbf{v_r}, \\ \mathbf{v_{r+1}} &= (\mathbf{g} + \mathbf{v_1} + \mathbf{v_2} + \ldots + \mathbf{v_r}) \\ \mathbf{v_{r+2}} &= (\mathbf{g} + 2\mathbf{v_1} + \mathbf{v_2} + \ldots + \mathbf{v_r}) \\ & \ldots, \\ \mathbf{v_{r+k}} &= (\mathbf{g} + k\mathbf{v_1} + \mathbf{v_2} + \ldots + \mathbf{v_r}) \end{aligned}$$

has gcd 1. Furthermore, $g(V) = \{\mathbf{a}\}$.

To see this, first observe that $\mathbf{v_{r+1}} \in cone(\mathbf{a})$. Also, $\mathbf{a} \in S_{\mathbb{R}^+}(\mathbf{v_1}, \ldots, \mathbf{v_r}$ by construction and subsequently is also in $S_{\mathbb{R}^+}(\mathbf{2v_1}, \ldots, \mathbf{v_r})$.

Note that

$$\begin{bmatrix} k\mathbf{v_1} & \ldots & \mathbf{v_r} \end{bmatrix} = \begin{bmatrix} \pm k & 0 & \ldots & 0 \\ 0 & \pm 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \pm 1 \end{bmatrix}$$

is a matrix with determinant $\pm k$. Now, for some $1 \le i \le k - 1$, we have $\gcd(g \pm i, k) = 1$, where the sign for i is the same sign as $\mathbf{v_1} = \pm\mathbf{e_1}$. Thus,

$$\begin{bmatrix}\mathbf{v_{r+i}} & \mathbf{v_2} & \dots & \mathbf{v_r}\end{bmatrix} = \begin{bmatrix} g_1 \pm i & 0 & \dots & 0 \\ g_2 \pm 1 & \pm 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_r \pm 1 & 0 & \dots & \pm 1 \end{bmatrix}$$

is a matrix with determinant $\pm(g_i \pm i)$. These are relatively prime, so $\gcd(V) = 1$.

Now, we claim that this is the unique g-vector. Note that since $\gcd(MS) = 1$, we only have to consider integral vectors by Corollary 12. First, we claim that $\mathbf{g}$ is complete. Any integral point in its interior is of the form $(g_1 + a_1 b_1, g_2 + a_2 b_2, \dots, g_r + a_r b_r$, where $a_i \in \mathbb{N}$. By part (3) of Lemma 38, any vector of the form $g_1 + nb_1, g_2 + b_2, \dots, g_r + b_r$ is in S, where $n > 0$. Thus, by using $\mathbf{v_2}, \dots, \mathbf{v_r}$, any integral vector in $intcone(\mathbf{g})$ is also in S.

Suppose there is another complete vector $\mathbf{g'} = (g'_1, \dots, g'_r)$. By part (1) of Lemma 38, we need to have $g'_1 \geq g_1$. By part (2) of the same Lemma, $g'_i \geq g_i$ for any $i \neq 1$ since for arbitrarily big m, there is some n such that we need at least one $\mathbf{v_{r+j}}$, $j \geq 1$, to get all the points in $cone(\mathbf{g'})$ with the first coordinate $n > m$. Since $g'_i \geq g_i$ for all i, $\mathbf{g'} \in cone(\mathbf{g})$, so $\mathbf{g'}$ is not minimal. Therefore, $\mathbf{g}$ is the unique element of the g-set. □

As an example of this, consider $k = 5$. We then know that we can make any integral vector the unique g-vector using some orthant as the cone with $r + 5$ vectors. The only vectors which we cannot construct such a V for with this method must have $\gcd(1, 2, 3, 4, 5) = 60$ dividing every coordinate. Also, note that one direction of Theorem 14 is an immediate corollary of Theorem 15 in the case $k = 2$.

9.4 The $3r$ Bound

There is another way to bound the number of vectors needed in V. Rosales, et al. proves in [10] that:

Theorem 16. *Any integer m is equal to $g(V)$ for a set of numbers V of cardinality at most 3.*

With this, we can show:

Theorem 17. *Any integral vector can be made to be unique g-vector for some V with $3r$ vectors.*

Proof. Suppose we want $\mathbf{a} = (a_1, \dots, a_r)$ to be the unique g-vector. Again, take an orthant that $\mathbf{a}$ lies in, with the corresponding spanning set

$$\{b_1\mathbf{e_1}, b_2\mathbf{e_2}, \dots, b_r\mathbf{e_r}\},$$

where each b_i is ± 1.

By Theorem 16, for each i from 1 to r we may find a set V_i of at most 3 vectors such that the vectors are of the form $k_1 b_i \mathbf{e_i}, \dots, k_j b_i \mathbf{e_i}$, $j \leq 3$, with $g(k_1, \dots, k_j) = a_i$.

Take the set V to be the union of all V_i, which have at most $3r$ elements. The result is immediate by Theorem 11. □

Thus, we have two bounds on the number of vectors necessary to make a vector the unique g-vector. Neither is better than the other in every case.

10 Generalizations of 1-D Theorems

10.1 The k = r + 1 case

In the case $r = 1$ this next result reduces to a classical result about the Frobenius number of two relatively prime numbers: $g(a_1, a_2) = (a_1 - 1)(a_2 - 1) - 1$ which is due to Sylvester [6]. In 2003, Simpson [5] proved a result which is almost exactly the same as the following Theorem.

Suppose that $k = r + 1$ so that $V = \{\mathbf{v_1}, \ldots, \mathbf{v_{r+1}}\}$. Suppose further S is dense, and $S_{\mathbb{R}}$ is a simple cone generated by $\mathbf{v_1}, \ldots, \mathbf{v_r}$. Let A be the $r \times r$ matrix with columns $\mathbf{v_1}, \ldots, \mathbf{v_r}$.

Theorem 18. $g(\mathbf{v_1}, \ldots, \mathbf{v_{r+1}}) = \{(|A| - 1)\mathbf{v_{r+1}} - \mathbf{V_A}\}$

Proof. First we will prove that $\mathbf{g} = (|A| - 1)\mathbf{v_{r+1}} - \mathbf{V_A}$ is complete. Let $\mathbf{a}$ be a vector in the interior of $cone(\mathbf{g})$. By Theorem 6 there exists an integer $c_{r+1} \in [0, |A| - 1]$ such that $c_{r+1}\mathbf{v_{r+1}} \equiv \mathbf{a}$, hence there exist integers $c_1, \ldots, c_r$ such that

$$c_1\mathbf{v_1} + \ldots + c_{r+1}\mathbf{v_{r+1}} = \mathbf{a}.$$

Because $\mathbf{a} \in intcone(\mathbf{g})$ we know that there exist positive real numbers $\alpha_1, \ldots, \alpha_r$ such that

$$\mathbf{a} = \mathbf{g} + \alpha_1\mathbf{v_1} + \ldots + \alpha_r\mathbf{v_r}.$$

Combining these two representations for $\mathbf{a}$ we find that

$$\begin{aligned} c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} + (|A| - 1)\mathbf{v_{r+1}} &\geq c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} + c_{r+1}\mathbf{v_{r+1}} \\ &= \mathbf{a} \\ &= \mathbf{g} + \alpha_1\mathbf{v_1} + \ldots + \alpha_r\mathbf{v_r} \\ &= (\alpha_1 - 1)\mathbf{v_1} + \ldots + (\alpha_r - 1)\mathbf{v_r} + (|A| - 1)\mathbf{v_{r+1}}. \end{aligned}$$

Thus $c_i \geq \alpha_i - 1$ for $i = 1, \ldots, r$. But α_i is positive and c_i is an integer so we now have $c_i \geq 0$ for $i = 1, \ldots, r$. Finally, because $\mathbf{a} = c_1\mathbf{v_1} + \ldots + c_{r+1}\mathbf{v_{r+1}}$ we have $\mathbf{a} \in S$. Therefore $\mathbf{g}$ is complete.

Suppose for contradiction that for some $d_1, \ldots, d_r \in \mathbb{N}_0$ with at least one of $d_1, \ldots, d_r$ equal to zero, we have $\mathbf{g} + d_1\mathbf{v_1} + \ldots + d_r\mathbf{v_r} \in S$. So we have a solution $(c_1, \ldots, c_{r+1}) \in \mathbb{N}_0^{r+1}$ to the equation

$$c_1\mathbf{v_1} + \ldots + c_{r+1}\mathbf{v_{r+1}} = (|A| - 1)\mathbf{v_{r+1}} - \mathbf{V_A} + d_1\mathbf{v_1} + \ldots + d_r\mathbf{v_r},$$

and thus to

$$c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} + \mathbf{V_A} + (c_{r+1} + 1 - |A|)\mathbf{v_{r+1}} = d_1\mathbf{v_1} + \ldots + d_r\mathbf{v_r}.$$

Evaluating $\mod(A)$ we have $(c_{r+1} + 1 - |A|)\mathbf{v_{r+1}} \equiv \mathbf{0}$. Thus $|A|$ divides $c_{r+1} + 1$ and because $c_{r+1} \geq 0$ we have $c_{r+1} + 1 \geq |A|$. Because $c_{r+1} + 1 - |A| \geq 0$, $(c_{r+1} + 1 - |A|)\mathbf{v_{r+1}}$ can be written as a non-negative linear combination of $\mathbf{v_1}, \ldots, \mathbf{v_r}$. Now $\mathbf{v_1}, \ldots, \mathbf{v_r}$ is a basis for vector space $\mathbb{R}^n$. Thus

$$c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} + \mathbf{V_A} + (c_{r+1} + 1 - |A|)\mathbf{v_{r+1}}$$

can be uniquely written as a real linear combination of $\mathbf{v_1}, \ldots, \mathbf{v_r}$. This linear combination must have positive coefficients because c_i is non-negative for $i = 1, \ldots, r$ and $(c_{r+1} + 1 - |A|)\mathbf{v_{r+1}} \geq \mathbf{0}$. But we also have

$$c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} + \mathbf{V_A} + (c_{r+1} + 1 - |A|)\mathbf{v_{r+1}} = d_1\mathbf{v_1} + \ldots + d_r\mathbf{v_r},$$

which is a contradiction because one of $d_1, \ldots, d_r$ is zero. Therefore $\mathbf{g} + d_1\mathbf{v_1} + \ldots + d_r\mathbf{v_r} \notin S$.

Finally we will prove that if $\mathbf{a} \in RH$ is complete, then $\mathbf{a} \geq \mathbf{g}$. Suppose for contradition that $\mathbf{a}$ is a complete vector with $\mathbf{a} \not\geq \mathbf{g}$. Because $\mathbf{a}$ and $\mathbf{g}$ are in $cone(\mathbf{0})$, we know that there exist non-negative reals, $\alpha_1, \ldots, \alpha_r, \alpha_1^{'}, \ldots, \alpha_r^{'}$ such that $\alpha_1\mathbf{v_1} + \ldots + \alpha_r\mathbf{v_r} = \mathbf{a}$ and $\alpha_1^{'}\mathbf{v_1} + \ldots + \alpha_r^{'}\mathbf{v_r} = \mathbf{g}$. Because $\mathbf{a} \not\geq \mathbf{g}$ there is some $j \in [1, r]$ such that $\alpha_j < \alpha_j^{'}$. Let $d_1, \ldots, d_r \in \mathbb{N}_0$ such that $d_j = 0$ and $\alpha_i^{'} + d_i > \alpha_i$ for $i = 1, \ldots, r$ with $i \neq j$. Now we have

$$\mathbf{g}+d_1\mathbf{v_1}+...+d_r\mathbf{v_r}-\mathbf{a} = (\alpha_1^{'}+d_1)\mathbf{v_1}+...+(\alpha_r^{'}+d_r)\mathbf{v_r}-\mathbf{a} = (\alpha_1^{'}+d_1-\alpha_1)\mathbf{v_1}+\ldots+(\alpha_r^{'}+d_r-\alpha_r)\mathbf{v_r}$$

which has positive coeffients. Thus $\mathbf{g}+d_1\mathbf{v_1}+...+d_r\mathbf{v_r} \in intcone(\mathbf{a})$. But $\mathbf{g}+d_1\mathbf{v_1}+...+d_r\mathbf{v_r} \notin S$, which contradicts the completeness of $\mathbf{a}$. Thus if $\mathbf{a}$ is complete, then $\mathbf{a} \geq \mathbf{g}$. This shows that $\mathbf{g}$ is the unique minimal complete vector. Therefore $g(V) = \{\mathbf{g}\}$. □

10.2 The Linear Case

Let $\mathbf{v_1}, \ldots, \mathbf{v_r}, \mathbf{w} \in \mathbb{Z}_0^r$. Suppose $\mathbf{w} \in \text{cone}(\mathbf{0}, \{\mathbf{v_1}, \ldots, \mathbf{v_r}\})$. Let $k \in \mathbb{N}$. Let $V = \{\mathbf{v_i} + j\mathbf{w} \mid 0 \leq i \leq r, 0 \leq j \leq k\}$ and $V^{'} = \{\mathbf{v_1}, \ldots, \mathbf{v_r}, \mathbf{w}\}$.

Theorem 19. *Suppose that V is dense. Let $G = \{c_1\mathbf{v_1}+\ldots+c_r\mathbf{v_r}-\mathbf{V_A}+(|A|-1)\mathbf{w} \mid c_1, \ldots, c_r \in \mathbb{N}_0$ $c_1 + \ldots + c_r = \left\lfloor \frac{|A|-2}{k} \right\rfloor + 1\}$. Now $g(V) = G$.*

Proof. First we will prove that $S(V^{'})$ is dense. Let M be the set of matrices with columns from V. Let $M^{'}$ be the set of matrices with columns from $V^{'}$. Let $A \in M$. The columns of A are integer linear combinations of vectors in $V^{'}$. Because determinants are multi-linear, $|M|$ is an integer linear combination of the determinants of matrices in $M^{'}$. Because $S(V)$ is dense, 1 can be written as an integer linear combination of determinants of matrices in M. Thus 1 can be written as an integer linear combination of determinants of matrices in $M^{'}$. So $\gcd(V^{'}) = 1$ and $S(V^{'})$ is dense.

Next we will prove that all vectors in G are complete. Let $\mathbf{g} \in G$ and $c_1, \ldots, c_r \in \mathbb{N}_0$ with

$$\mathbf{g} = c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} - \mathbf{V_A} + (|A| - 1)\mathbf{w}$$

and

$$c_1 + \ldots + c_r = \left\lfloor \frac{|A| - 2}{k} \right\rfloor + 1.$$

Let $\mathbf{b} \in intcone(\mathbf{g})$. Because $V^{'}$ is dense, there exists an integer $m \in [0, |A| - 1]$ such that $b \equiv m\mathbf{w} \mod (A)$. Thus we can express

$$\mathbf{b} - m\mathbf{w} = c_1^{'}\mathbf{v_1} + \ldots + c_r^{'}\mathbf{v_r}$$

for some integers $c_1^{'}, \ldots, c_r^{'}$. Now we have

$$\begin{aligned} c_1^{'}\mathbf{v_1} + \ldots + c_r^{'}\mathbf{v_r} &= \mathbf{b} - m\mathbf{w} \\ &\geq \mathbf{b} - (|A| - 1)\mathbf{w} \\ &\in intcone(\mathbf{g} - (|A| - 1)\mathbf{w}) \\ &= intcone(c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} - \mathbf{V_A}). \end{aligned}$$

Thus for $i = 1, \ldots, r$ we have $c_i^{'} > c_i - 1$, and thus $c_i^{'} \geq c_i$. If we add these r inequalities we see that

$$c_1^{'} + \ldots + c_r^{'} \geq c_1 + \ldots + c_r = \left\lfloor \frac{|A| - 2}{k} \right\rfloor + 1.$$

Let $n = c_1^{'} + \ldots + c_r^{'}$. Consider all sums of n vectors in V. The sums form the set

$$S^{'} = \{d_1\mathbf{v_1} + \ldots + d_r\mathbf{v_r} + j\mathbf{w} | d_1, \ldots, d_r, j \in \mathbb{N}_0 d_1 + \ldots + d_r = n, 0 \leq j \leq nk\},$$

where $S^{'} \subset S_{\mathbb{N}_0}$ by definition. But we have

$$nk = (c_1^{'} + \ldots + c_r^{'})k \geq \left(\left\lfloor \frac{|A|-2}{k} \right\rfloor + 1\right)k > \left(\frac{|A|-2}{k}\right)k \geq |A| - 2,$$

so $nk \geq |A| - 1$. Thus $\mathbf{b} = c_1^{'}\mathbf{v_1} + \ldots + c_r^{'}\mathbf{v_r} + m\mathbf{w} \in S^{'}$ and $\mathbf{b} \in S$. Therefore $\mathbf{g}$ is complete which proves that all vectors in G are complete.

Lemma 39. *Let* $H = \{c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} + (|A| - 1)\mathbf{w} \mid c_1, \ldots, c_r \in \mathbb{Z}\ c_1 + \ldots + c_r \leq \lfloor \frac{|A|-2}{k} \rfloor\}$. *Now* $H \cap S_{\mathbb{N}_0} = \emptyset$.

Suppose for the sake of contradiction that $\mathbf{a} \in H$ can be written as the sum of n vectors in V.
Case 1, $n \leq \lfloor \frac{|A|-2}{k} \rfloor$:
All vectors in V are congruent to one of $0, \mathbf{w}, \ldots, k\mathbf{w} \mod (A)$, so $\mathbf{a}$ is congruent to one of $0, \mathbf{w}, \ldots, nk\mathbf{w}$. We have $nk \leq \lfloor \frac{|A|-2}{k} \rfloor k \leq \frac{|A|-2}{k}k = |A| - 2$. Thus $\mathbf{a} \not\equiv (|A| - 1)\mathbf{w}$. But this contradicts the fact that all elements of H are congrent to $(|A| - 1)\mathbf{w}$. Thus $\mathbf{a}$ cannot be written as the sum of n vectors in V.
Case 2, $n > \lfloor \frac{|A|-2}{k} \rfloor$:
Because $\mathbf{a} \in H$, there exist integers $c_1, \ldots, c_r$ with $c_1 + \ldots + c_r \leq \lfloor \frac{|A|-2}{k} \rfloor$ such that

$$\mathbf{a} = c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} + (|A| - 1)\mathbf{w}.$$

Because $\mathbf{a}$ is the sum of n vectors from V it can be written

$$\mathbf{a} = c_1^{'}\mathbf{v_1} + \ldots + c_r^{'}\mathbf{v_r} + m\mathbf{w}$$

with $c_1^{'}, \ldots, c_r^{'}, m \in \mathbb{N}_0$ and $c_1^{'} + \ldots + c_r^{'} = n$. Taking both representations of $\mathbf{a} \mod (A)$ we know that $m\mathbf{w} \equiv \mathbf{a} \equiv -\mathbf{w}$. Thus $|A|$ divides $m + 1$. Because m is non-negative, we conclude that $m \geq |A| - 1$. Now we have

$$\begin{aligned} c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} &\geq c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} + (|A| - 1)\mathbf{w} - m\mathbf{w} \\ &= \mathbf{a} - m\mathbf{w} \\ &= c_1^{'}\mathbf{v_1} + \ldots + c_r^{'}\mathbf{v_r}. \end{aligned}$$

Thus $c_i \geq c_i^{'}$ for $i \in [1, r]$. Adding these r inequalities we have

$$\lfloor \frac{|A|-2}{k} \rfloor \geq c_1 + \ldots + c_r \geq c_1^{'} + \ldots + c_r^{'} = n > \lfloor \frac{|A|-2}{k} \rfloor,$$

which is a contradiction. Therefore $\mathbf{a}$ cannot be written as the sum of n vectors in V. Hence for any $\mathbf{a} \in H$ we have $\mathbf{a} \notin S_{\mathbb{N}_0}$.

Next we will prove that for any $\mathbf{g} \in G$ we have $\mathbf{g} \in g(V)$. Because of the analogous definitions of G and H we have $\mathbf{g} + \mathbf{V_A} - \mathbf{v_i} \in H$ and thus $\mathbf{g} + \mathbf{V_A} - \mathbf{v_i} \notin S_{\mathbb{N}_0}$ for $i \in [i, r]$. We have proved that $\mathbf{g}$ is complete and now by Theorem 3, we have $\mathbf{g} \in g(V)$. Thus $G \subset g(V)$.

Lemma 40. *Let* $c_1, \ldots, c_r, m \in \mathbb{Z}$ *with* $m < |A|$ *and at least one of* $c_1, \ldots, c_r$ *negative. Then* $\mathbf{a} = c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} + m\mathbf{w} \notin S_{\mathbb{N}_0}$.

Proof. Suppose for the sake of contradiction that $\mathbf{a} \in S_{\mathbb{N}_0}$. Thus there exist $c_1^{'}, \ldots, c_r^{'}, m^{'} \in \mathbb{N}_0$ such that

$$a = c_1^{'}\mathbf{v_1} + \ldots + c_r^{'}\mathbf{v_r} + m^{'}\mathbf{w}.$$

But

$$\mathbf{0} \equiv \mathbf{a} - \mathbf{a} \equiv m^{'}\mathbf{w} - m\mathbf{w} \equiv (m^{'} - m)\mathbf{w},$$

and thus $|A|$ divides $m^{'} - m$. Thus for some integer k we have $m^{'} - m = k|A|$. But $m < |A|$ and $m^{'}$ is positive, so $k \geq 0$. By Theorem 6 $|A|\mathbf{w} \equiv \mathbf{0}$. Thus for some $d_1, \ldots, d_r \in \mathbb{N}_0$, we have

$$d_1\mathbf{v_1} + \ldots + d_r\mathbf{v_r} = |A|\mathbf{w}.$$

Now

$$\begin{aligned} c_1^{'}\mathbf{v_1} + \ldots + c_r^{'}\mathbf{v_r} + m^{'}\mathbf{w} - m^{'}\mathbf{w} &= \mathbf{a} - (m + k|A|)\mathbf{w} \\ &= c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} + m\mathbf{w} - m\mathbf{w} - k(d_1\mathbf{v_1} + \ldots + d_r\mathbf{v_r}) \\ &= (c_1 - kd_1)\mathbf{v_1} + \ldots + (c_r - kd_r)\mathbf{v_r}. \end{aligned}$$

Thus $c_i^{'} = c_i - kd_i$ for $i \in [1, r]$. But for some $j \in [1, r]$, we have $c_j < 0$. Since k and d_j are non-negative, $c_j^{'}$ is negative, which is a contradiction. Thus $\mathbf{a} \notin S_{\mathbb{N}_0}$. □

Finally, we will prove that $g(V) \subset G$. We will do this by showing that $\mathbf{g} \notin G$ implies $\mathbf{g} \notin g(V)$. For some real $\alpha_1, \ldots, \alpha_r$ we have

$$\mathbf{g} = \alpha_1\mathbf{v_1} + \ldots + \alpha_r\mathbf{v_r} + (|A| - 1)\mathbf{w}.$$

Let

$$\mathbf{a} = (\lfloor\alpha_1\rfloor + 1)\mathbf{v_1} + \ldots + (\lfloor\alpha_r\rfloor + 1)\mathbf{v_r} + (|A| - 1)\mathbf{w}$$

and

$$\mathbf{b} = \lfloor\alpha_1\rfloor\mathbf{v_1} + \ldots + \lfloor\alpha_r\rfloor\mathbf{v_r} + (|A| - 1)\mathbf{w}.$$

Now $\mathbf{g} \in cone(\mathbf{b})$ and $\mathbf{a} \in intcone(\mathbf{g})$.

Case 1, $\lfloor\alpha_1\rfloor + \ldots + \lfloor\alpha_r\rfloor + r \leq \lfloor\frac{|A|-2}{k}\rfloor$:
Now $\mathbf{a} \in H$ by the definition of H so $\mathbf{a} \notin S$, and $\mathbf{g}$ is not complete, thus $\mathbf{g} \notin g(V)$.

Case 2, $\alpha_j < -1$ for some $j \in [1, r]$:
Now $\lfloor\alpha_j\rfloor + 1$ is negative and $m < |A|$, so by Lemma 40, $\mathbf{a} \notin S$. Thus $\mathbf{g}$ is not complete and $\mathbf{g} \notin g(V)$.

Case 3, $\lfloor\alpha_1\rfloor + \ldots + \lfloor\alpha_r\rfloor + r > \lfloor\frac{|A|-2}{k}\rfloor$ and $\alpha_1, \ldots, \alpha_r \geq -1$:
There exist integers $c_1, \ldots, c_r$ such that $-1 \leq c_i \leq \lfloor\alpha_i\rfloor$ for $i \in [1, r]$ and

$$c_1 + \ldots + c_r + r = \left\lfloor \frac{|A| - 2}{k} \right\rfloor.$$

Let

$$\mathbf{g}^{'} = c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r}.$$

Now $\mathbf{g}^{'} \in G$ and thus $\mathbf{g}^{'}$ is complete. Also $\mathbf{g}^{'} \leq \mathbf{b} \leq \mathbf{g}$ so $\mathbf{g} \notin g(V)$.
Therefore $\mathbf{g} \notin G$ implies $\mathbf{g} \notin g(V)$. Thus $g(V) \subset G$ and finally $g(V) = G$.

□

This result directly generalizes the 1-D result in [4] which computes the Frobenius number for the case when the numbers form an arithmetic progression. The result states that $g(m, m + w, m + 2w, \ldots, m + (k - 1)w) = m\lfloor\frac{m-2}{k-1}\rfloor + (m - 1)w$.

10.3 Another Linear Case

If we let $n = 1$, the following Theorem reduces to Theorem 18.

Theorem 20. *Let $\mathbf{v_1}, \ldots, \mathbf{v_r}, \mathbf{w} \in \mathbb{Z}^r$ such that $\mathbf{v_1}, \ldots, \mathbf{v_r}$ form a simple cone. Let*

$$V = \{\mathbf{v_1}, \ldots, \mathbf{v_r}, c_1\mathbf{w}, \ldots, c_n\mathbf{w}\}$$

where $c_1, \ldots, c_n \in \mathbb{N}$ with $c_1, \ldots, c_n, |A|$ relatively prime. Suppose further that $S(V)$ is dense. Now we have $g(V) = \{g(c_1, \ldots, c_n, |A|)\mathbf{w} + |A|\mathbf{w} - \mathbf{V_A}\}$ where g is the Frobenius function.

Proof. Let $V' = \{\mathbf{v_1}, \ldots, \mathbf{v_r}, \mathbf{w}\}$. Because $c_1\mathbf{w}, \ldots, c_n\mathbf{w}$ are multiples of $\mathbf{w}$, we have $S_{\mathbb{Z}}(V) \subset S_{\mathbb{Z}}(V')$. By Theorem 7, $|A|\mathbf{w} \equiv \mathbf{0}$ so $|A|\mathbf{w}$ is an integer linear combination of $\mathbf{v_1}, \ldots, \mathbf{v_r}$ and thus $|A|\mathbf{w} \in S_{\mathbb{Z}}(V)$. But $c_1, \ldots, c_r, |A|$ are relatively prime, thus $\mathbf{w}$ can be written as an integer linear combination of $c_1\mathbf{w}, \ldots, c_n\mathbf{w}, |A|\mathbf{w}$ and thus $\mathbf{w} \in S_{\mathbb{Z}}(V)$. Thus $S_{\mathbb{Z}}(V') \subset S_{\mathbb{Z}}(V)$ and $S_{\mathbb{Z}}(V') = S_{\mathbb{Z}}(V)$, so we can conclude that $S(V')$ is dense. By Theorem 6, $|A|\mathbf{w}$ is the smallest multiple of $\mathbf{w}$ congruent to $\mathbf{0}$.

Let $\mathbf{m} \in m(V)$. By Lemma 8, there exist $a_1, \ldots, a_n \in \mathbb{N}_0$ such that $\mathbf{m} = \sum_{i=1}^{n} a_i c_i \mathbf{w} \in \mathbb{Z}\mathbf{w}$. Thus $m(V) \subset \mathbb{Z}\mathbf{w}$ and $m(V)$ is completely ordered. Thus each congruence class has a unique element in $m(V)$.

Suppose for contradiction that $g(c_1, \ldots, c_n, |A|)\mathbf{w} \in S_{\mathbb{N}}(V)$. Then there exist $a_1, \ldots, a_r, b_1, \ldots, b_n \in \mathbb{N}_0$ such that

$$g(c_1, \ldots, c_n, |A|)\mathbf{w} = \sum_{i=1}^{r} a_i \mathbf{v_i} + \sum_{i=1}^{n} a_i c_i \mathbf{w}.$$

Now we can see that $\sum_{i=1}^{r} a_i \mathbf{v_i}$ is a multiple of $\mathbf{w}$, so there exists some $d \in \mathbb{N}$ with $d\mathbf{w} = \sum_{i=1}^{r} a_i \mathbf{v_i}$. But $d\mathbf{w} \equiv \mathbf{0}$ so by Theorem 6, $|A|$ divides d. But now $g(c_1, \ldots, c_n, |A|)\mathbf{w}$ is a positive non-negative integer linear combination of $c_1\mathbf{w}, \ldots, c_n\mathbf{w}, |A|\mathbf{w}$, which contradicts the definition of the Frobenius function. Thus $g(c_1, \ldots, c_n, |A|)\mathbf{w} \notin S_{\mathbb{N}}(V)$.

Let $d \in \mathbb{N}$ be greater than $g(c_1, \ldots, c_n, |A|)$. By Theorem 6, $|A|\mathbf{w}$ is congruent to $\mathbf{0}$ and thus $|A|\mathbf{w} \in S_{\mathbb{N}}(V)$. But now by the definition of the Frobenius function, we see that $d\mathbf{w}$ can be written as a non-negative integer linear combination of $c_1\mathbf{w}, \ldots, c_n\mathbf{w}, |A|\mathbf{w}$. Thus $d\mathbf{w} \in S_{\mathbb{N}}(V)$.

In particular

$$g(c_1, \ldots, c_n, |A|)\mathbf{w} + |A|\mathbf{w} \in S_{\mathbb{N}}(V),$$

and thus

$$g(c_1, \ldots, c_n, |A|)\mathbf{w} + |A|\mathbf{w} \in m(V).$$

Because

$$g(c_1, \ldots, c_n, |A|)\mathbf{w} + \mathbf{w}, \ldots, g(c_1, \ldots, c_n, |A|)\mathbf{w} + (|A| - 1)\mathbf{w}$$

are all in $S_{\mathbb{N}}(V)$, we see that $g(c_1, \ldots, c_n, |A|)\mathbf{w} + |A|\mathbf{w}$ is the maximal element in $m(V)$.

Suppose $\mathbf{g} \in g(V)$. By Theorem 9, there exists a complete set of residues $\omega_{\mathbf{1}}, \ldots, \omega_{|\mathbf{A}|}$ such that $\mathbf{g} = lub(\omega_{\mathbf{1}}, \ldots, \omega_{|\mathbf{A}|}) - \mathbf{V_A}$. But each congruence class has a unique element in $m(V)$ so one of $\omega_{\mathbf{1}}, \ldots, \omega_{|\mathbf{A}|}$ is equal to $g(c_1, \ldots, c_n, |A|)\mathbf{w} + |A|\mathbf{w}$. Thus

$$\mathbf{g} = lub(\omega_{\mathbf{1}}, \ldots, \omega_{|\mathbf{A}|}) - \mathbf{V_A} = g(c_1, \ldots, c_n, |A|)\mathbf{w} + |A|\mathbf{w} - \mathbf{V_A}.$$

Therefore $g(V) = \{g(c_1, \ldots, c_n, |A|)\mathbf{w} + |A|\mathbf{w} - \mathbf{V_A}\}$.

□

11 Multiplying by d

Theorem 21 is a generalization of a Theorem published by Johnson [9] in 1960.

Theorem 21. *Let $V = \{\mathbf{v_1}, \ldots, \mathbf{v_k}\}$ and $V' = \{\mathbf{v_1}, \ldots, \mathbf{v_r}, d\mathbf{v_{r+1}}, \ldots, d\mathbf{v_k}\}$ where $d \in \mathbb{N}$. Suppose that $S(V)$ and $S(V')$ are dense. Now $g(V) - \mathbf{V_A} = dg(V') - \mathbf{V_A}$.*

Before proving this Theorem, we will first prove several Lemmas.

Lemma 41. *Let G be a finite additive group and let $d \in \mathbb{N}$. Now let $\phi : G \to G$ be defined by $\phi(g) = dg$ for all $g \in G$. Then ϕ is an automorphism if and only if $(o(G), d) = 1$.*

Proof. Suppose ϕ is an automorphism. Now $\ker(\phi) = \{0\}$. Suppose for the sake of contradiction that there exist a prime p with $p|o(G)$ and $p|d$. By Cauchy's Theorem, there exists a $g \in G$ with $o(g) = p$. Now $\phi(g) = dg = 0$. But now $g \in ker(\phi)$ thus $o(g) = 1$, which is a contradiction. Thus $(o(G), d) = 1$.

Now suppose that $(o(G), d) = 1$. Let $g \in G$ with $g \neq 0$. We have $o(g)|o(G)$ so $(o(g), d) = 1$. Also $o(g) \neq 1$ so $o(g) \nmid d$. Thus $dg \neq 0$ and $g \notin ker(\phi)$. Thus $ker(\phi) = \{0\}$ and ϕ is an automorhism. □

We are assuming $S(V')$ to be dense, so we need multiplication by d to be an automorphism of $\mathbb{Z}^r/A$. By Lemma 41, this is exactly when $|A|$ and d are relatively prime.

Lemma 42. *If $\omega_\mathbf{1}, \ldots, \omega_{|\mathbf{A}|} \in m(V)$ is a complete set of residues, then $\mathbf{g} = lub(\omega_\mathbf{1}, \ldots, \omega_{|\mathbf{A}|}) - \mathbf{V_A}$ is a complete vector.*

Proof. Let $\mathbf{v}$ be some vector in $fund(\mathbf{g})$. There exists a $j \in [1, |A|]$ such that $\omega_\mathbf{j} \equiv \mathbf{v}$. Now $P_i(\mathbf{v}) > P_i(\mathbf{g})$, and

$$\begin{aligned} P_i(\omega_\mathbf{j}) &\leq \max(P_i(\omega_\mathbf{1}), \ldots, P_i(\omega_{|\mathbf{A}|})) \\ &= P_i(lub(\omega_\mathbf{1}), \ldots, P_i(\omega_{|\mathbf{A}|})) \\ &= P_i(\mathbf{g} + \mathbf{V_A}) \\ &= P_i(\mathbf{g}) + 1. \end{aligned}$$

Now for all $i \in [1, r]$ we have

$$P_i(\mathbf{v}) - P_i(\omega_\mathbf{j}) > P_i(\mathbf{g}) - (P_i(\mathbf{g}) + 1) = -1.$$

But by Lemma 28, $P_i(\mathbf{v}) - P_i(\omega_\mathbf{j}) \in \mathbb{Z}$, so $P_i(\mathbf{v}) \geq P_i(\omega_\mathbf{j})$. Thus $\mathbf{v} \geq \omega_\mathbf{j}$ and $\mathbf{v} \in S$. Thus $fund(\mathbf{g}) \subset S$, and by Lemma 11, $\mathbf{g}$ is a complete vector. □

We have

$$gcd(V') = gcd(\mathbf{v_1}, \ldots, \mathbf{v_r}, d\mathbf{v_{r+1}}, \ldots, d\mathbf{v_k}) | gcd(d\mathbf{v_1}, \ldots, d\mathbf{v_k}) = d \cdot gcd(\mathbf{v_1}, \ldots, \mathbf{v_k}) = d,$$

and $gcd(V')$ divides $|A|$, so $gcd(V') = 1$ and $S(V')$ is dense.

Lemma 43. $dm(V) = m(V')$.

Proof. Suppose $\omega \in m(V)$. By Lemma 8, there exist $c_{r+1}, \ldots, c_k \in \mathbb{N}_0$ such that $\sum_{i=r+1}^{k} c_i \mathbf{v_i} = \omega$. Now $d\omega = \sum_{i=r+1}^{k} c_i d\mathbf{v_i} \in S(V')$. There exist some $\omega' \in \mathbf{Q}^r$ such that $d\omega' \in m(V')$, $d\omega' \equiv d\omega$,

and $d\omega^{'} \leq d\omega$. By Lemma 8, there exist $c_{r+1}^{'}, \ldots, c_k^{'} \in \mathbb{N}_0$ such that $\sum_{i=r+1}^{k} c_i^{'} d\mathbf{v_i} = \omega^{'}$. Now $\omega^{'} = \sum_{i=r+1}^{k} c_i^{'}\mathbf{v_i}$, $\omega^{'} \leq \omega$, and $\omega^{'} \equiv \omega$. Because $\omega \in m(V)$, we must have $d\omega = d\omega^{'} \in m(V^{'})$.

Now suppose $\omega \notin m(V)$.

Case 1: $\omega \notin S(V)$. For all $c_{r+1}, \ldots, c_k \in \mathbb{N}_0$ we have $\sum_{i=r+1}^{k} c_i\mathbf{v_i} \neq \omega$, thus $\sum_{i=r+1}^{k} c_i d\mathbf{v_i} \neq d\omega$ and by the converse of Lemma 8 we have $d\omega \notin m(V^{'})$.

Case 2: $\omega \in S(V)$ with ω not minimal in its residue class. Let $\omega^{'}$ be a vector in $m(V)$ with $\omega^{'} < \omega$ and $\omega^{'} \equiv \omega$. Now there exist $c_{r+1}, \ldots, c_k \in \mathbb{N}_0$ such that $\sum_{i=r+1}^{k} c_i d\mathbf{v_i} = \omega^{'}$. Now $d\omega^{'} \in S(V^{'})$, $d\omega^{'} \equiv d\omega$, and $d\omega^{'} < d\omega$. Thus $d\omega \notin m(V^{'})$, which proves the lemma. □

Lemma 44. *If $\mathbf{g} - \mathbf{V_A}$ is complete in $S(V)$, then $d\mathbf{g} - \mathbf{V_A}$ is complete in $S(V^{'})$.*

Proof. Suppose $\mathbf{g} - \mathbf{V_A}$ is complete. Let $\mathbf{g}^{'} - \mathbf{V_A}$ be a vector in $g(V)$ with $\mathbf{g}^{'} \leq \mathbf{g}$. By Theorem 9 there exist a complete set of residues, $\omega_\mathbf{1}, \ldots, \omega_{|\mathbf{A}|} \in m(V)$, such that $\mathbf{g}^{'} = lub(\omega_\mathbf{1}, \ldots, \omega_{|\mathbf{A}|})$. Thus $\mathbf{g}^{'} \geq \omega_j$ for $j \in [1, |A|]$. Also $d\mathbf{g} \geq d\mathbf{g}^{'} \geq d\omega_j$, thus $d\mathbf{g} \geq lub(d\omega_\mathbf{1}, \ldots, d\omega_{|\mathbf{A}|})$. By Lemma 43 we have $d\omega_j \in m(V^{'})$ for $j \in [1, |A|]$, and thus by Lemma 42 we have $d\mathbf{g} - \mathbf{V_A} \geq lub(d\omega_\mathbf{1}, \ldots, d\omega_{|\mathbf{A}|}) - \mathbf{V_A}$ is complete in $S(V^{'})$. □

Lemma 45. *Let $\mathbf{g} \in \mathbb{Z}^r$. If $d\mathbf{g} - \mathbf{V_A} \in S(V^{'})$, then $\mathbf{g} - \mathbf{V_A} \in S(V)$.*

Proof. There exist $c_1, \ldots, c_k \in \mathbb{N}_0$ with $c_1, \ldots, c_r \geq 1$, such that

$$d\mathbf{g} = c_1\mathbf{v_1} + \ldots + c_r\mathbf{v_r} + c_{r+1}d\mathbf{v_{r+1}} + \ldots + c_k\mathbf{v_k}.$$

Now

$$\mathbf{g} = \frac{c_1}{d}\mathbf{v_1} + \ldots + \frac{c_r}{d}\mathbf{v_r} + c_{r+1}\mathbf{v_{r+1}} + \ldots + c_k\mathbf{v_k},$$

so

$$\mathbf{g} \in intcone(c_{r+1}\mathbf{v_{r+1}} + \ldots + c_k\mathbf{v_k}).$$

Also $d\mathbf{g} \equiv c_{r+1}d\mathbf{v_{r+1}} + \ldots + c_kd\mathbf{v_k}$, and because multiplication by d is an automorphism of residue classes, we have $\mathbf{g} \equiv c_{r+1}\mathbf{v_{r+1}} + \ldots + c_k\mathbf{v_k}$. Thus by Lemma 28 $\frac{c_i}{d} \in \mathbb{N}$ for all $i \in [1, r]$, and thus $\mathbf{g} - \mathbf{V_A} \in S(V)$. □

And now we are ready to prove Theorem 21.

Proof. Suppose $\mathbf{g} - \mathbf{V_A} \in g(V)$. By Lemma 44, $d\mathbf{g} - \mathbf{V_A}$ is complete in $S(V^{'})$. By Theorem 3, for all $i \in [1, r]$ there exist $\alpha_1, \ldots, \alpha_r \in \mathbb{R}_{\geq 0}$ such that $\alpha_i = 0$ and $\mathbf{g} - \mathbf{V_A} + \sum_{i=1}^{r} \alpha_i\mathbf{v_i}$ is in $\mathbb{Z}^r$ but not in $S(V)$. By Lemma 45, $d\mathbf{g} - \mathbf{V_A} + \sum_{i=1}^{r} \alpha_i d\mathbf{v_i} \notin S(V^{'})$. Now by Theorem 3, we have $d\mathbf{g} - \mathbf{V_A} \in g(V^{'})$, which proves the first direction.

Now suppose $d\mathbf{g}-\mathbf{V_A} \in g(V^{'})$. By Theorem 9 there exist a complete set of residues $d\omega_{\mathbf{1}}, \ldots, d\omega_{|\mathbf{A}|} \in m(V^{'})$ such that $d\mathbf{g} = lub(d\omega_{\mathbf{1}}, \ldots, d\omega_{|\mathbf{A}|})$. Now

$$\begin{aligned} lub(\omega_{\mathbf{1}}, \ldots, \omega_{|\mathbf{A}|}) &= \sum_{i=1}^{r} max(P_i(\omega_{\mathbf{1}}), \ldots, P_i(\omega_{|\mathbf{A}|}))\mathbf{v_i} \\ &= \frac{1}{d}\sum_{i=1}^{r} max(P_i(d\omega_{\mathbf{1}}), \ldots, P_i(d\omega_{|\mathbf{A}|}))\mathbf{v_i} \\ &= \frac{1}{d} lub(d\omega_{\mathbf{1}}, \ldots, d\omega_{|\mathbf{A}|}) \\ &= \mathbf{g}. \end{aligned}$$

Thus by Lemma 42, $\mathbf{g} - \mathbf{V_A}$ is complete. There exist $\mathbf{g}^{'}$ with $\mathbf{g}^{'} - \mathbf{V_A} \in g(V)$ and $\mathbf{g}^{'} \leq \mathbf{g}$. By the first direction, we know that $d\mathbf{g}^{'} - \mathbf{V_A} \in g(V^{'})$. But $d\mathbf{g}^{'} - \mathbf{V_A} \leq d\mathbf{g} - \mathbf{V_A} \in g(V^{'})$, so $\mathbf{g}^{'} = \mathbf{g}$. Thus $\mathbf{g} - \mathbf{V_A} \in g(V)$, which proves the second direction. □

12 Generalized Problem for Non-dense Situations

As a natural generalization of our problem, it makes sense to consider the cases when $\gcd(V) \neq 1$.

Call points of the form $\{a|(intcone(a) \cap S_{\mathbb{Z}}(V)) \subset S(V)\}$ *generalized-complete*, and the set of all such points $C(V)$. We define $G(V)$, the *generalized g-set* as

$$\{\min(a \in \gcd(V)RH|a \in C(V))\},$$

the set of minimums determined with respect to cone inclusion. Note that this is analogous to definition of $g(V)$ as

$$\{\min(a \in RH|a \in c(V))\},$$

where $c(V)$ is the set of complete points. Furthermore, it is clear that when $gcd(V) = 1$, $g(V) = G(V)$.

Bridging the gap between $G(V)$ and $g(V)$ is not difficult since we have already done enough work to show the preservation of cone inclusion under multiplication of a matrix.

Theorem 22. *Suppose that $V = DV'$, where $|D| = gcd(V)$. Then $G(V) = Dg(V')$.*

Proof. Consider $G \in G(V)$. It is an element in $gcd(V)RH$, so multiplying by D^{-1} gives an element $g \in RH$. Note that $S_{\mathbb{Z}}(V) = D\mathbb{Z}^r$ by Lemma **??**. We claim that $g \in g(V')$. If not, there is some g' which is complete and has $g > g'$. However, by Lemma 22, $G = Dg > Dg'$. Since g' is complete, $(intcone(g') \cap \mathbb{Z}^r) \subset S(V')$. Thus,

$$\begin{aligned} (intcone(Dg') \cap D\mathbb{Z}^r) &\subset S(DV') \\ &= S(V). \end{aligned}$$

Since $Dg' \in gcd(V)RH$, Dg' is a generalized-complete vector, contradicting the fact that G was minimal.

The other direction is almost identical. If $g \in g(V')$, then $Dg = G \in gcd(V)RH$. If $G \notin G(V)$, then there is some G' which is generalized-complete and has $G > G'$. So $g = D^{-1}G > D^{-1}G'$. Since G' is generalized-complete,

$$\begin{aligned}(intcone(D^{-1}G') \cap D^{-1}S_{\mathbb{Z}}(V)) &\subset S(D^{-1}V)\\ (intcone(D^{-1}G') \cap D^{-1}D\mathbb{Z}^r) &\subset S(D^{-1}V)\\ (intcone(D^{-1}G') \cap \mathbb{Z}^r) &\subset S(V').\end{aligned}$$

Since $D^{-1}G' \in RH$, $D^{-1}G'$ is complete, and g cannot have been minimal. □

We recall that the classical problem, where finding the g-set of $V = \{a_1, \ldots, a_n\}$ is finding their Frobenius number. We have only defined the problem when $\gcd(V) = 1$. Suppose we relax this condition and allow $\gcd(V) = k$, $k < \infty$. Then:

Corollary 11. *Suppose $r = 1$, $V = \{a_1, \ldots, a_n\}$, and $\gcd(V) = k$. Then $G(V) = \{k \times frob(V')\}$, where $V' = \{a_1/k, \ldots, a_n/k\}$.*

So, in the 1-d case, we can still get a *generalized Frobenius number* as the sole member of our g-set. We denote this number by $frob(V)$.

For example, when $V = \{10, 14\}$, $S_{\mathbb{Z}}(V) = \{2a, a \in \mathbb{Z}\}$. $frob(V) = 26$, since any even number greater than 26 can be generated by V, but 26 cannot.

References

[1] Brauer, Alfred; Shockley, James E. *On a problem of Frobenius*. J. Reine Angew. Math. 211, 215-220, 1962.

[2] Dedekind, Richard. *Theory of algebraic integers*. Cambridge University Press, Cambridge, 1996.

[3] Novikov, B.V. *On the structure of subsets of a vector lattice that are closed with respect to addition*. J. Math. Sci. 72, 3223-3225, 1994.

[4] Roberts, J.B. *Note on linear forms*.Proc. Amer. Math. Soc. 7 (1956), 465–469.

[5] Simpson, R.J.; Tijdeman, R. *Multi-dimensional versions of a theorem of Fine and Wilf and a formula of Sylvester*. Proc. Amer. Math. Soc. 131(6), 1661–1671 (electronic), 2003

[6] Sylvester, J.J. *Question 7832*. Mathematical Questions from the Educational Times. 41, 21, 1884

[7] Brauer, Alfred: *On a Problem of Frobenius*. Journal f?ur die reine und angewandte M, vol. 211, pp. 215-220, 1962.

[8] Schur. 1935.

[9] S. M. Johnson. *A Linear Diophantine Problem*. Canadian Journal of Mathematics, vol. 12, pp. 390-398, 1960.

[10] Rosales, J.C. et al. *Every positive integer is the frobenius number of a numerical semigroup with three generators*. Math. Scand. 94. pp. 5-12, 2004.

[11] Wikipidea.org. *Cauchy-Binet formula*. http://en.wikipedia.org/wiki/Cauchy-Binet_formula, 2005.