The Multi-Dimensional Frobenius Problem 2

Jeffrey Amos, Charles Chen, Olga Lepigina,
Timur Nezhmetdinov, Darren Ong, Matthew Richer, Laura Zirbel
Under the Guidance of Professor Vadim Ponomarenko
Research Experiences for Undergraduates, Trinity University

July 27, 2006

Abstract

Consider the problem of determining maximal vectors g such that the Diophantine system $Mx = g$ has no solution. We provide a variety of results to this end: conditions for the existence of g, conditions for the uniqueness of g, bounds on g, determining g explicitly in several important special cases, constructions for g, and a reduction for M.

1 Introduction

We will begin where last year's combinatorics group stopped. We will be using the notation used in the paper that was recently submitted for publication. In fact, almost all of this introduction was copied straight from it with the proofs removed.

Let m, x be column vectors from $\mathbb{N}_0$. Georg Frobenius focused attention on determining maximal g such that the linear Diophantine equation $m^T x = g$ has no solutions. This problem has attracted substantial attention in the last 100+ years; for a survey, see a really cool book that Vadim checked out from the library, which contains almost 500 references as well as applications to algebraic geometry, coding theory, linear algebra, algorithm analysis, discrete distributed systems, and random vector generation. A natural generalization of this problem (and essential to some applications) is to determine maximal vector(s) g such that the system of linear Diophantine equations $Mx = g$ has no solutions. This has attracted relatively little attention, perhaps because maximality must be subject to a partial vector ordering. We attempt to redress this injustice by providing a variety of results in this multi-dimensional context.

We fix $\mathbb{R}^n$. For any real matrix X and any $S \subseteq \mathbb{R}$, we write X_S for $\{Xs : s \in S^k\}$, where k denotes the number of columns of X. Abusing this notation slightly, we write X_1 for the vector $X1^k$. We fix $M \subseteq \mathbb{Z}_{n\times(n+m)}$, and write $M = [A|B]$, where A is $n \times n$. We call $A_{\mathbb{R}^{\geq 0}}$ the *cone*, and $M_{\mathbb{N}_0}$ the *monoid*. $|A|$ denotes henceforth the absolute value of $\det A$. If $|A| \neq 0$, then we follow others and call the cone *volume*. If, in addition, each column of B lies in the cone, then we call M *simplicial*. Unless otherwise noted, we assume henceforth that M is simplicial. Note that if $n \leq 2$, then we may always rearrange columns to make M simplicial.

Let $u, v \in \mathbb{R}^n$. If $u - v \in A_{\mathbb{Z}}$, then we write $u \equiv v$ and say that u, v are *equivalent mod A*. If $u - v \in A_{\mathbb{R}^{\geq 0}}$, then we write $u \geq v$. If $u - v \in A_{\mathbb{R}^{>0}}$, then we write $u \succ v$. Note that $u \succ v$ implies $u \geq v$, and $u \succ v \geq w$ implies $u \succ w$; however, $u \gneq v$ does not necessarily imply that $u \succ v$. For $v \in \mathbb{R}^n$, we write $[\succ v] = \{u \in \mathbb{Z}^n : u \succ v\}$. We say that v is *complete* if $[\succ v] \subseteq M_{\mathbb{N}_0}$. We set G, more precisely $G(M)$, to be the set of all $\geq$-minimal complete vectors. We call elements of G *Frobenius vectors*; they are the vector analogue of g that we will investigate.

Set $Q = (1/|A|)\mathbb{Z}^n \subseteq \mathbb{Q}$. Although G is defined in $\mathbb{R}^n$, in fact it is a subset of Q^n, by the following result. Furthermore, the columns of B are

in $A_{Q^{\geq 0}}$; hence $M_{Q^{\geq 0}} = A_{Q^{\geq 0}}$ and without loss we henceforth work over Q rather than over $\mathbb{R}$.

Proposition 1.1. *Let $v \in \mathbb{R}^n$. There exists $v^\star \in Q^n$ with $[\succ v] = [\succ Av^\star]$ and $v \geq Av^\star$.*

In general, $M_{\mathbb{N}_0}$ does not form an $\leq$-lattice, because $A^{-1}B$ does not have integer entries and thus lub is not well-defined. However, because $\left(Q^{\geq 0}\right)^n$ is a chain product, our partial order $\leq$ is a lattice over Q. For $x = Ax', y = Ay'$, we see that $\mathrm{lub}(x, y) = Az'$, where z' is defined via $(z')_i = \max((x')_i, (y')_i)$.

For $u \in Q^n$, we set $V(u) = \left(u + A_{Q \cap (0,1]}\right) \cap \mathbb{Z}^n$. It was known to Dedekind that $|V(u)| = |A|$, and that $V(u)$ is a complete set of coset representatives mod A (as restricted to $\mathbb{Z}^n$).

The following equivalent conditions on M generalize the one-dimensional notion of relatively prime generators. We assume henceforth, unless otherwise noted, that M possesses these properties. We call such M *dense*.

Theorem 1.2. *The following are equivalent:*

1. *G is nonempty.*
2. *$M_{\mathbb{Z}} = \mathbb{Z}^n$.*
3. *For all unit vectors e_i $(1 \leq i \leq n)$, $e_i \in M_{\mathbb{Z}}$.*
4. *There is some $v \in M_{\mathbb{N}_0}$ with $v + e_i \in M_{\mathbb{N}_0}$ for all unit vectors e_i.*
5. *The GCD of all the $n \times n$ minors of M has absolute value 1.*
6. *The elementary divisors of M are all 1.*

Classically, there is a second type of Frobenius number f, maximal so that $m^T x = f$ has no solutions with x from $\mathbb{N}$ (rather than $\mathbb{N}_0$). This does not add much; it was shown that $f = g + m^T 1$. A similar situation holds in the vector context.

Proposition 1.3. *Call v* f-complete *if $[\succ v] \subseteq M_{\mathbb{N}}$. Set F to be all $\geq$-minimal f-complete vectors. Then $F = G + M_1$.*

For vector u and $i \in [1, n]$, let $C^i(u) = \{v : v \in \mathbb{Z}^n \setminus M_{\mathbb{N}_0}, v = u + Aw, (w)_i = 0, (w)_j \in (0, 1] \text{ for } j \neq i\}$ and let $C(u) = \bigcup_{i \in [1,n]} C^i(u)$, a disjoint union. Call elements of $C(u)$ *critical*. Note that if $v \in C^i(u)$, then $v + Ae_i \in V(u)$. Critical elements characterize G, as shown by the following.

Theorem 1.4. *Let x be complete. $x \in G$ if and only if $C^i(x) \neq \emptyset,\ \forall i \in [1, n]$.*

Theorem 1.5. *Fix A and vector $c \geq 0$. Set $C = c(1^n)^T$, a square matrix, and fix $k \in \mathbb{N}$. Set $M = [A|A + C|A + 2C| \cdots |A + kC]$. Suppose that M is dense. Then $G(M) = \{Ax + |A|c - A_1 - c : x \in \mathbb{N}_0^n, \|x\|_1 = \lceil (|A| - 1)/k \rceil\}$.*

Let MIN $= \{x : x \in M_{\mathbb{N}_0};$ for all $y \in M_{\mathbb{N}_0},$ if $y \equiv x$ then $y \geq x\}$. Provided M is dense, MIN will have at least one representative of each of the $|A|$ equivalence classes mod A. MIN is a generalization of a one-dimensional method; the following result shows that it characterizes G.

Theorem 1.6. *Let $g \in G$. Then $g = lub(N) - A_1$ for some complete set of coset representatives $N \subseteq MIN$. Further, if $n < |A|$ then there is some $N' \subseteq N$ with $|N'| = n$ and $lub(N) = lub(N')$.*

Theorem 1.7. *$MIN \subseteq \{Bx : x \in \mathbb{N}_0^m, ||x||_1 \leq |A| - 1\}$.*

Corollary 1.8. *If $m = 1$ then $G = \{|A|B - A_1 - B\}$.*

2 Adjacency

2.1 General

Definition 2.1. *Let $g_i \in G$ be distinct vectors. A vector $v \in M_{\mathbb{R}_{\geq 0}}$ is* inside *the g_i iff $glb(g_i) \leq v \leq lub(g_i)$.*

Definition 2.2. *Let $g_i \in G$ be distinct vectors. A vector $v \in M_{\mathbb{R}_{\geq 0}}$ is* strictly inside *the g_i iff $glb(g_i) \prec v \prec lub(g_i)$.*

Definition 2.3. *The distinct vectors $g_1 \ldots, g_k \in G$ are* adjacent *iff there is no $g \in G$ strictly inside the set $\{g_i\}$. We write $\{g_i\}$ adjacent as $\mathring{\wedge}[g_i]$. When we refer to only two vectors we may also write $g_1 \mathring{\wedge} g_2$ for simplicity.*

Definition 2.4. *Let $\mathscr{B}_i = \{B \subseteq G \mid |B| = i$ and $\mathring{\wedge}[B]\}$. If some $B \in \mathscr{B}_i$ is maximal under inclusion we say it is a* block. *Let $\mathscr{B}$ be the set of* blocks.

Definition 2.5. *Let $O(M) = \{lub(B) \mid B \in \mathscr{B}\}$. This is the O-*set.

The following Theorem characterizes, based on n, how large blocks in $\mathscr{B}$ can be.

Theorem 2.6. *If $\mathscr{B}_i \neq \emptyset$, then $i \leq n$.*

Proof. Suppose that $i = n + 1$. For $B \in \mathscr{B}_i$ let $o = \text{lub}(B)$ such that $B = \{g_1, \ldots, g_{n+1}\} \subseteq G$. Since each $g_i \in B$ contributes one or more Ae_k components to o, by being maximal in that direction, we have by the pigeonhole principle that one of the g_i is strictly inside of B. Thus we have reached a contradiction and $\mathscr{B}_{n+1} = \emptyset$. This argument holds when $i > n + 1$ as well. □

Theorem 2.7. *For all $B_i \in \mathscr{B}_i$ there exists $B \in \mathscr{B}$ such that $B_i \subseteq B$.*

Proof. If $B_i \in \mathscr{B}$, then we are done. Suppose that $B_i \notin \mathscr{B}$. Clearly B_i is not maximal under inclusion; there must be some $B' \in \mathscr{B}_{i+1}$ such that $B_i \subseteq B'$. If again we have $B' \notin \mathscr{B}$, the process continues. By Theorem 2.6 this process is finite and so $\exists B'' \in \mathscr{B}$ such that $B_i \subseteq B''$.

□

The following Corollary shows that for all $g \in G$ there exists some $B \in \mathscr{B}$ such that $g \in B$.

Corollary 2.8. $\bigcup_{B \in \mathscr{B}} B = G$.

Proof. Clearly $\bigcup_{B \in \mathscr{B}} B \subseteq G$. By definition $\mathscr{B}_1 = G$ since $\forall g \in G$ it is true that $\mathring{\wedge}[g]$. By Theorem 2.7 we then have $G \subseteq \bigcup_{B \in \mathscr{B}} B$ so that $\bigcup_{B \in \mathscr{B}} B = G$. □

Theorem 2.9. *Let $B \subseteq G$. Then lub$(B) \notin M_{\mathbb{N}_0}$ if and only if $\mathring{\wedge}[B]$.*

Proof. Suppose $\mathring{\wedge}[B]$. Let $L = A^{-1}\text{lub}(B)$ and suppose that $\text{lub}(B) \in M_{\mathbb{N}_0}$. Since $AL \in M_{\mathbb{N}_0}$, we have that $L \in A^{-1}M_{\mathbb{N}_0}$. Now let $L' = L - \epsilon(I_n)_1$ where I_n is the identity matrix. Thus $[\geq L] \subseteq A^{-1}M_{\mathbb{N}_0}$ implies that L' is complete in $A^{-1}M_{\mathbb{N}_0}$ and therefore AL' is complete in $M_{\mathbb{N}_0}$. Since $L' < L$ we have $AL' < \text{lub}(B)$. Thus $\exists g \in G(M)$ such that g is strictly inside B, a contradiction.

Now suppose that $\text{lub}(B) \notin M_{\mathbb{N}_0}$. Then for all $v \in [\prec \text{lub}(B)]$ we have $v \notin G(M)$ and therefore there are no frobenius vectors strictly inside B so that $\mathring{\wedge}[B]$.

□

Corollary 2.10. $O(M) \cap M_{\mathbb{N}_0} = \emptyset$.

Proof. By construction, for all $o \in O(M)$ we have $o = \text{lub}(B)$ where $B \in \mathscr{B}$. Thus $\mathring{\wedge}[B]$ and the Corollary follows by Theorem 2.9.

□

2.2 Adjacency in two dimensions: the Ladder

The concept of adjacency can be used when looking at various properties of the sets of Frobenius vectors. For example, in two dimensions, it could be used to prove that since Frobenius vectors are incomparable to each other, they lie in a chain or a "ladder", where the least upper bound of each consecutive pair of vectors is the cut-off for each "step".

The following two propositions have already been proved earlier in the paper, and they are very useful in the two-dimensional case.

Proposition 2.11. *Let $g_1, g_2 \in G(M)$. Then $g_1 \mathring{\wedge} g_2$ iff $lub(g_1, g_2) \notin (M)_{\mathbb{N}_0}$.*

Proposition 2.12. $O(M) \cap (M)_{\mathbb{N}_0} = \emptyset$.

Below follows a description of various properties of adjacent Frobenius vectors in two dimensions and a proof that they all lie in a form of a "ladder" in two dimensions.

Definition 2.13. *Let $M = [a_1, a_2|B]$, for some vector g, and let* the angle of g *be the angle that g makes with a_2. We write the angle of a as Θ_a.*

Proposition 2.14. *Let $g_1, g_2 \in G(M)$. Then $\Theta_{g_1} = \Theta_{g_2}$ iff $g_1 = g_2$.*

Proof. If $g_1 = g_2$ then both g_1 and g_2 have the same coordinates, and therefore the angles that they make with the origin would be equal.

Let $\Theta_{g_1} = \Theta_{g_2} = \alpha$. Let $\Theta_{a_1} > \Theta_{a_2}$. Then, by the Definition 2.13, $\Theta_{a_1} \geq \Theta_{g_1}, ..., \Theta_{g_k} \geq \Theta_{a_2}$, where $k = |G(M)|$. Both g_1 and g_2 lie on the same line with the origin. Therefore let $g_2 = \beta g_1, \beta > 1$. Then let $g_1 = \Sigma \alpha_i a_i$, $\alpha_i \geq 0$ since $g_1 \geq 0$. Then $g_2 = \Sigma \beta_i \alpha_i a_i$. $g_2 - g_1 = \Sigma(\beta - 1)\alpha_i a_i$ so $g_2 > g_1$ which is a contradiction, because unless the g-vectors are equal to each other, they can not be comparable. □

Proposition 2.15. *Let $g_1, g_2 \in G(M), g_1 \neq g_2$. Let $\Theta_{g_1} > \Theta_{g_2}$, $a = lub(g_1, g_2)$ and $b = glb(g_1, g_2)$. Then $\Theta_{g_1} > \Theta_a > \Theta_{g_2}$ and $\Theta_{g_1} > \Theta_b > \Theta_{g_2}$.*

Proof. Suppose $A^{-1}g_1 = (x_1, y_1)$, $A^{-1}g_2 = (x_2, y_2)$. Then $\Theta_{g_1} > \Theta_{g_2} \Leftrightarrow y_1/x_1 > y_2/x_2$. Since $g_1||g_2$, $A^{-1}g_1||A^{-1}g_2$. Then $y_1 > y_2$ and $x_2 > x_1$. Since both a and b lie on the intersection of the cones of g_1 and g_2, both $A^{-1}a$ and $A^{-1}b$ lie on the intersection of the cones of $A^{-1}g_1$ and $A^{-1}g_2$. $A^{-1}A = [[1, 0], [0, 1]]$ therefore the cones are parallel to the first quadrant, and $A^{-1}a = (x_2, y_1), A^{-1}b = (x_1, y_2)$.
Since $y_1 > y_2 \Rightarrow y_1/x_2 > y_2/x_2 \Rightarrow \Theta_a > \Theta_{g_2}$.
$x_2 > x_1 \Rightarrow y_1/x_1 > y_1/x_2 \Rightarrow \Theta_{g_1} > \Theta_a \Rightarrow \Theta_{g_1} > \Theta_a > \Theta_{g_2}$.
$y_1 > y_2 \Rightarrow y_1/x_1 > y_2/x_1 \Rightarrow \Theta_{g_1} > \Theta_b$.
$x_2 > x_1 \Rightarrow y_2/x_1 > y_2/x_2 \Rightarrow \Theta_b > \Theta_{g_2} \Rightarrow \Theta_{g_1} > \Theta_b > \Theta_{g_2}$.

□

Proposition 2.16. *For any 3 vectors x, y, z, $x \neq y \neq z$, if $\Theta_x \geq \Theta_y \geq \Theta_z$ then at least one of the following has to be true:*
1. $y \leq x$
2. $y \leq z$
3. $y \geq x$
4. $y \geq z$
5. $glb(x, z) \prec y \prec lub(x, z)$

Proof. Suppose that $y||x$ and $y||z$, that is the first four conditions of the Proposition 2.16 do not apply. Then let $A^{-1}x = [x_1, y_1]$, $A^{-1}z = [x_2, y_2]$, and $A^{-1}y = [x_3, y_3]$. Since $y||x$ then either:
(1) $x_1 > x_3$ and $y_1 < y_3$ or
(2) $x_1 < x_3$ and $y_1 > y_3$.
Since $y||z$ then either:
(3) $x_2 > x_3$ and $y_2 < y_3$ or
(4) $x_2 < x_3$ and $y_2 > y_3$.
Note that since $x_1 < x_2$ and $y_1 < y_2$ only 3 out of the 4 combinations are possible: (1) and (3), (2) and (3), (2) and (4). However the (1),(3) combination results in $y_3/x_3 > y_1/x_1 \Rightarrow \Theta_y > \Theta_x$ which contradicts the assumption. The (2),(4) combination results in $y_3/x_3 < y_2/x_2 \Rightarrow \Theta_y < \Theta_z$ which also contradicts the initial assumption. Therefore, the only possible relationship is when $x_1 < x_3 < x_2$ and $y_1 > y_3 > y_2$. Therefore, since $\text{lub}(A^{-1}x, A^{-1}y) = [x_2, y_1]$ and $\text{glb}(A^{-1}x, A^{-1}y) = [x_1, y_2]$, $\text{glb}(x, z) \prec y \prec \text{lub}(x, z)$.

□

Corollary 2.17. *Let $g_1, g_2 \in G(M), g_1 \neq g_2$. Then $g_1 \mathring{\wedge} g_2$ iff there is no other $g \in G(M), g \neq g_1, g \neq g_2$ such that $\Theta_{g_1} > \Theta_g > \Theta_{g_2}$.*

Proof. Let $g_1 \mathring{\wedge} g_2$. Since g_1, g_2, $g \in G(M)$, $g_1||g_2||g$, and therefore by Proposition 2.16, $glb(g_1, g_2) \prec g \prec lub(g_1, g_2) \Rightarrow g$ is strictly inside g_1 and g_2 which contradicts the definition of adjacent vectors.

Let $g_1, g_2 \in G(M)$ and let there be no $g \in G(M)$ such that $\Theta_{g_1} > \Theta_g > \Theta_{g_2}$. Then since by Proposition 2.15, $\Theta_{g_1} > \Theta_{\text{lub}(g_1,g_2)} > \Theta_{g_2}$ and $\Theta_{g_1} > \Theta_{\text{glb}(g_1,g_2)} > \Theta_{g_2}$, there is no Frobenius vector that is strictly inside g_1 and g_2, therefore $g_1 \mathring{\wedge} g_2$. □

Theorem 2.18 (The Ladder)**.** *Let $k = |G(M)|$. Then all vectors $g_i \in G(M)$ can be relabeled in such a way that $\Theta_{g_1} > \Theta_{g_2} > \cdots > \Theta_{g_k}$ and for each g_i and g_{i+1} under the new labeling system, $g_i \mathring{\wedge} g_{i+1}$.*

Proof. By the Proposition 2.14 $g_i = g_k$ iff $\Theta_{g_i} = \Theta_{g_k} \Rightarrow$ if $g_i \neq g_k$ then $\Theta_{g_i} \neq \Theta g_k$. If $\Theta_{g_i} \neq \Theta g_k$ then either $\Theta_{g_i} > \Theta_{g_k}$ or $\Theta_{g_i} < \Theta_{g_k}$. Therefore, since there are k different Frobenius vectors, there are k unique angles, which can be listed by decreasing order of magnitude. Hence, $g_1, ..., g_k$ can be relabeled in such a way that $\Theta_{g_1} > \Theta_{g_2} > \cdots > \Theta_{g_k}$. Then, under this labeling system, each pair g_i and g_{i+1} has to be adjacent by the Proposition 2.17, since there are no other vectors $g \in G(M)$ for which $\Theta_{g_i} > \Theta_g > \Theta_{g_{i+1}}$. □

Proposition 2.19. *Let $k = |G(M)|$. Then $|O(M)| = k - 1$.*

Proof. By the Theorem 2.18 all of the vectors $g_i \in G(M)$ can be relabeled in such a way that $\Theta_{g_1} > \Theta_{g_2} > \cdots > \Theta_{g_k} \Rightarrow$ there are $k - 1$ pairs of vectors g_i, g_{i+1} that are adjacent and correspond to a unique element of O. Any other pair of vectors in $G(M)$ would have at least one other vector with an angle that lies between their angles $\Rightarrow$ by the Proposition 2.17 they would not be adjacent $\Rightarrow$ by the Proposition 2.12 their least upper bound would not be in $O(M)$. Therefore, $|O(M)| = k - 1$. □

Proposition 2.20 (The Big Chain)**.** *Let $n = |O(M)|$. Then all of the points in $O_i \in O(M)$ can be relabeled in such a way that $\Theta_{O_1} > \Theta_{O_2} > \cdots > \Theta_{O_n}$, and each pair of points O_i and O_{i+1} lies on the cone of a unique Frobenius vector.*

Proof. By the Proposition 2.19, $|G(M)| = n + 1$, and by the Theorem 2.18 all of the elements in $G(M)$ can be relabeled in such a way that $\Theta_{g_1} > \Theta_{g_2} > \cdots > \Theta_{g_{n+1}}$. Therefore, there are n pairs of adjacent vectors of the form g_i, g_{i+1}, each corresponding to a specific element O_i such that, by the Proposition 2.15, $\Theta_{g_i} > \Theta_{O_i} > \Theta_{g_{i+1}}$. Therefore, all elements of $O(M)$ can

be relabeled in such a way that $\Theta_{O_1} > \Theta_{O_2} > \cdots > \Theta_{O_n}$. In fact, the chain could be extended to $\Theta_{g_1} > \Theta_{O_1} > \Theta_{g_2} > \Theta_{O_2} > \cdots > \Theta_{O_i} > \Theta_{g_{i+1}}$. □

Proposition 2.21. *If $O_1, O_2 \in O(M), O_1 \neq O_2$ then $O_1 || O_2$*

Proof. Suppose that O_1 is comparable to O_2. WLOG let $O_1 > O_2$. But by the definition of the least upper bound, for any $\vec{v}, \vec{v} > O_2, \vec{v} \in M \Rightarrow O_1 = O_2$ which is a contradiction to the hypothesis. □

Applications of the Ladder and the Big Chain in the 4-2 case.

The fact that both the elements of $G(M)$ and $O(M)$ form a chain in two dimensions can be used to prove various properties of the g-set in two dimensions. For example, in the $4-2$ case, suppose that $M_1 = [a_1, a_2|b_1, b_2]$, and $M_2 = [a_1, a_2|b_1, b_2 + b_1]$, and $[a_1, a_2|b_1]$ is dense. Then the chain property of the Frobenius vectors in two dimensions could be used to prove that $|G(M_2)| \leq |G(M_1)|$.

Lemma 2.22. *Let $O_i \in O(M_2)$ and $O_i \in (M_1)_{\mathbb{N}_0}$. Then $O_i = d - b_1$ where $d \in [a_1, a_2|b_1 + b_2]\mathbb{N}_0$.*

Proof. Let $c^\star = \text{lub}(g_1, g_2)$, and let $g_1, g_2 \in G(M_2)$ such that $g_1 \mathring{\wedge} g_2$. By the Proposition 2.11, $c^\star \notin (M_2)_{\mathbb{N}_0}$. $c^\star \in (M_1)_{\mathbb{N}_0}$. Let $c^\star = c_1a_1 + c_2a_2 + c_3b_1 + c_4b_2$, where $c_1, c_2, c_3, c_4 \in \mathbb{N}_0$. There could be multiple ways to express $c^\star$ in terms of the vectors a_1, a_2, b_1, b_2 and let's consider the one with the minimal coefficient in front of b_2. Suppose $c_3 > c_4$. Then $c^\star = c_1a_1 + c_2a_2 + (c_3 - c_4)b_1 + c_4(b_2 + b_1) \Rightarrow c^\star \in (M_2)_{\mathbb{N}_0}$ which contradicts the assumption that $c^\star \notin (M_2)_{\mathbb{N}_0}$. Therefore, $c_3 < c_4$. Let $c_4 - c_3 > 1$. Let $d = c^\star + b_1$. $d = c_1a_1 + c_2a_2 + (c_3 + 1)b_1 + c_4b_2$. Since the coefficients in front of a_1, a_2 stay the same, c_4 is still the least possible coefficient in front of b_2. $c_3 + 1 < c_4$, therefore d can not be expressed as a multiple of $a_1, a_2, b_1, (b_2 + b_1)$ and therefore $d \notin (M_2)_{\mathbb{N}_0}$. But $d > c^\star$ which contradicts the hypothesis that $c^\star = \text{lub}(g_1, g_2)$ because $d \succ g$ for some $g \in G(M_2) \Rightarrow c_3 = c_4 - 1$ and $c^\star = c_1a_1 + c_2a_2 + (c_4 - 1)b_1 + c_4b_2 = c_1a_1 + c_2a_2 + c_4(b_1 + b_2) - b_1$. □

Lemma 2.23. *For each $O_i \in O(M_2)$ there exists $O_j \in O(M_1)$ such that $O_j = O_i - cb_1; c \in \mathbb{N}_0$.*

Proof. By the Lemma 2.22, $O_i = c_1a_1 + c_2a_2 + c_3(b_1 + b_2) - b_1$. Let $d^\star = O_i - c_3b_1 = c_1a_1 + c_2a_2 + c_3b_2 - b_1$. $O_i \notin (M_2)_{\mathbb{N}_0}$ by the Proposition 2.12,

therefore -1 is the maximum possible coefficient in front of b_1 for $O_i \Rightarrow -1$ is the maximum coefficient in front of b_1 for $d^\star$, hence $d^\star \notin (M_1)_{\mathbb{N}_0}$, since one of the coefficients is negative. Now follows a proof by induction that every vector greater than $d^\star$ is in $(M_1)_{\mathbb{N}_0}$.
Let $c^\star = A^{-1}O_i$ and $c' = A^{-1}d^\star$. Let $\bar{a_1} = A^{-1}a_1 = [1,0], \bar{a_2} = A^{-1}a_2 = [0,1], \bar{b_1} = A^{-1}b_1, \bar{b_2} = A^{-1}b_2$.
Base case: $c' + [\epsilon, 0]$ and $c' + [0, \epsilon] \in A^{-1}(M_1)_{\mathbb{N}_0}$.
Since $[a_1, a_2|b_1]$ is dense, then $A^{-1}[a_1, a_2|b_1]$ is also dense $\Rightarrow [\epsilon, 0] = n_1\bar{a_1} + n_2\bar{a_2} + n_3\bar{b_1}; n_1, n_2, n_3 \in \mathbb{Z}$. $c^\star + [\epsilon, 0] \in A^{-1}(M_2)_{\mathbb{N}_0}$. $c^\star + [\epsilon, 0] = c_1\bar{a_1} + c_2\bar{a_2} + (c_4-1)\bar{b_1} + c_4\bar{b_2} + n_1\bar{a_1} + n_2\bar{a_2} + n_3\bar{b_1} \Leftrightarrow (c_1+n_1)\bar{a_1} + (c_2+n_2)\bar{a_2} + (c_4-1+n_3)\bar{b_1} + c_4\bar{b_2} \in A^{-1}(M_2)_{\mathbb{N}_0} \Rightarrow c_1+n_1 \geq 0; c_2+n_2 \geq 0$; and $c_4-1+n_3 \geq c_4 \Rightarrow n_3-1 \geq 0$. Now $c' + [\epsilon, 0]$ or $c' + [0, \epsilon]$ would equal to $(c_1 + n_1)\bar{a_1} + (c_2 + n_2)\bar{a_2} + (n_3 - 1)\bar{b_1} + c_4\bar{b_2}$, therefore, since all of the coefficients are non-negative, $c' + [0, \epsilon]$ and $c' + [\epsilon, 0] \in A^{-1}(M_1)_{\mathbb{N}_0}$.
Assume that $c' + [a, b] \in A^{-1}(M_1)_{\mathbb{N}_0}$, where $[a, b] > 0$. $c^\star + [a, b] \in A^{-1}(M_2)_{\mathbb{N}_0}$. Let $c' + [a, b] = d_1\bar{a_1} + d_2\bar{a_2} + d_3\bar{b_1} + d_4\bar{b_2}$, where $d_1, d_2, d_3, d_4 \in \mathbb{N}_0$. $c^\star + [a, b] = d_1\bar{a_1} + d_2\bar{a_2} + (d_3 + c_4)\bar{b_1} + d_4\bar{b_2}$. $c^\star + [a, b] + [0, \epsilon] \in A^{-1}(M_2)_{\mathbb{N}_0}$. Both $c^\star + [a, b]$ and $c^\star + [a, b] + [0, \epsilon] \in A^{-1}(M_1)_{\mathbb{Z}} \Rightarrow [0, \epsilon] \in A^{-1}(M_1)_{\mathbb{Z}} \Rightarrow [0, \epsilon] = s_1\bar{a_1} + s_2\bar{a_2} + s_3\bar{b_1} + s_4\bar{b_2} \Rightarrow s_1, s_2, s_3, s_4 \in \mathbb{Z}$. By the base case $c' + [0, \epsilon] \in A^{-1}(M_1)_{\mathbb{N}_0} \Rightarrow (c_1 + s_1)\bar{a_1} + (c_2 + s_2)\bar{a_2} + (s_3 - 1)\bar{b_1} + (s_4 + c_4)\bar{b_2} \in A^{-1}(M_1)_{\mathbb{N}_0} \Rightarrow s_3-1 \geq 0 \Rightarrow s_3 \geq 1$. $c^\star+[a, b]+[0, \epsilon] = (d_1+s_1)\bar{a_1}+(d_2+s_2)\bar{a_2}+(d_3+c_4+s_3)\bar{b_1}+(d_4+c_4)\bar{b_2} \in A^{-1}(M_2)_{\mathbb{N}_0} \Rightarrow d_1+s_1 > 0; d_2+s_2 > 0; d_4+c_4 > 0 \Rightarrow c' + [a, b] + [0, \epsilon] = (d_1 + s_1)a_1 + (d_2 + s_2)a_2 + (d_3 + s_3)b_1 + (d_4 + s_4)b_2$. Since $d_3 \geq 0$ and $s_3 \geq 1 \Rightarrow d_3 + s_3 \geq 1 \Rightarrow c' + [a, b] + [0, \epsilon] \in A^{-1}(M_1)_{\mathbb{N}_0}$. The argument for $c' + [a, b] + [\epsilon, 0]$ is exactly the same. Since $c' \notin A^{-1}(M_1)_{\mathbb{N}_0}$ and c' is complete, $c' \in O(A^{-1}M_1) \Rightarrow d^\star \in O(M_1)$.

□

Lemma 2.24. *Let $O_{j_1}, O_{j_2} \in O(M_1)$ such that $O_{j_1}+c_1b_1 = O_{i_1}, O_{i_1} \in O(M_2)$ and $O_{j_2} + c_2b_1 = O_{i_2}, O_{i_2} \in O(M_2)$, where $c_1, c_2 \in \mathbb{N}_0$. Then if $O_{j_1} = O_{j_2}$ then $O_{i_1} = O_{i_2}$.*

Proof. Let $O_{j_1} = O_{j_2} = p$. Then $O_{i_1} = p + c_1b_1$ $O_{i_2} = p + c_2b_1$. Suppose $O_{i_1} \neq O_{i_2}$ then $c_1 \neq c_2$. WLOG let $c_2 > c_1$. Then $O_{i_2} = O_{i_1} + (c_2 - c_1)b_1 \Rightarrow O_{i_2} > O_{i_1}$ but that contradicts Proposition 2.21, because O_{i_1} can not be comparable to O_{i_2}, therefore $O_{i_1} = O_{i_2}$. □

Proposition 2.25. $|G(M_2)| \leq |G(M_1)|$.

Proof. Let $|O(M_2)| = k$. Since, by Lemma 2.23 there is a function $f : O(M_2) \to O(M_1)$ And by Lemma 2.24, f is injective $\Rightarrow |O(M_1)| \geq |O(M_2)|$. Since by the Proposition 2.19, $|G(M_2)| = |O(M_2)| + 1$ and $|G(M_1)| = |O(M_1)| + 1$, $|G(M_2)| \leq |G(M_1)|$. □

Theorem 2.26. *Let $M_1 = [a_1, a_2|b_1, b_2]$ and $M_2 = [a_1, a_2|b_1, b_2 + c \cdot b_1]$, where $c \in \mathbb{N}_0$, and $[a_1, a_2|b_1]$ is dense. Then $|G(M_2)| \leq |G(M_1)|$.*

Proof. Let $N_0 = M_1, N_1 = [a_1, a_2|b_1, b_2 + b_1], ..., N_i = [a_1, a_2|b_1, b_2 + b_1 \cdot i], N_c = [a_1, a_2|b_1, b_2 + b_1 \cdot c] = M_2$. By the Proposition 2.25, $G(N_0) \geq G(N_1) \geq \cdots \geq G(N_c) \Rightarrow G(M_1) \geq G(M_2)$. □

The last theorem shows that the number of Frobenius vectors can only decrease as one of the b-vectors is added to another in the $4 - 2$ case by the means of establishing a relationship between the elements of the O-sets for the two sets of generating vectors. The concept of the chain could possibly be used for further research about the properties of the g-set in two dimensions, and the concept of adjacency can be used for the multi-dimensional proofs.

3 Order of b_i and the MIN set

Much of the time, information regarding frobenius vectors comes directly from a knowledge of the MIN set. The relationship between frobenius vectors and the least upper bounds of subsets of MIN is fundamentally important in this process. From some of the basic definitions of MIN we can prove theorems concerning the calculation of these vectors, specifically in cases where a unique frobenius vector is present. The following arguments are based on the relationship of the orders of the B vectors to the set MIN.

Consider the monoid $M_{\mathbb{N}_0}$ where $M = [A|B]$. Let b_i be the columns of B. We say $\operatorname{ord}_A(b_i)$ is the smallest $k \in \mathbb{N}$ such that $kb_i \equiv 0 \mod A$. We define the following function:

$$\Omega(M) = \prod_{i=1}^{m} \operatorname{ord}_A(b_i).$$

Let $S_M = \{\sum_{i=1}^{m} c_i b_i \mid 0 \leq c_i < \operatorname{ord}_A(b_i)\}$. We see that $|S_M| = \Omega(M)$. A known theorem states that the set MIN is totally dependent on B. In fact, we show that MIN is a subset of a specific finite subset of $B_{\mathbb{N}_0}$, namely S_M.

Proposition 3.1. $MIN \subseteq S_M$.

Proof. By Theorem 1.7 we have that $MIN \subseteq B_{\mathbb{N}_0}$ so now suppose that $v \in MIN$ but $v \notin S_M$. Since $v \in MIN \subseteq B_{\mathbb{N}_0}$ there exists some $v' \in \mathbb{N}_0^m$ such that $v = Bv'$. Now for some $j \in [1, n]$, it must be that $(v')_j \geq \text{ord}_A(b_j)$. Therefore $v \trianglerighteq v - b_j \text{ord}_A(b_j)$ and thus $v \notin MIN$, a contradiction. Hence $MIN \subseteq S_M$.

□

Theorem 3.2. *If* $\Omega(M) < |A|$, *then* $G(M) = \emptyset$. *Furthermore, if* $\gcd(M) = 1$ *and* $\Omega(M) = |A|$, *then* $G(M) = \{\sum_{i=1}^{m}(ord_A(b_i) - 1)b_i - A_1\}$.

Proof. Suppose that $\Omega(M) < |A|$. Thus no subset of S_M can be a complete set of minimal residues, and therefore there must exist some equivalence class ω that has no representatives in the monoid. Thus there can be no complete points and hence $G(M) = \emptyset$.

Now, let $\Omega(M) = |A|$. Due to $\gcd(M) = 1$ we know that $G(M)$ is nonempty and therefore there must be at least one minimal complete set of residues so that $|MIN| \geq |A|$. By Proposition 3.1, $MIN \subseteq S_M$, and $|S_M| = \Omega(M)$ we have that

$$|A| \leq |MIN| \leq |S_M| = \Omega(M) = |A|$$

So $|MIN| = |A|$ and particularly, $MIN = S_M$. Thus for every $g \in G(M)$, there is $L \subseteq MIN$ with $|L| = |A|$ such that $g + A_1 = \text{lub}(L)$, but then $L = MIN$ so that

$$g + A_1 = \text{lub}(MIN) \Rightarrow g = \sum_{i=1}^{m}(\text{ord}_A(b_i) - 1)b_i - A_1$$

Hence we have $G(M) = \{\sum_{i=1}^{m}(\text{ord}_A(b_i) - 1)b_i - A_1\}$.

□

Several special cases involving a diagonal A matrix follow rather nicely from the above theorem.

Corollary 3.3. *Let A be a in Smith-Normal form with diagonal $[k_1, \ldots, k_n]$ where $k_i \in \mathbb{N}_0$. Let B be the $n \times n$ matrix (b_{ij}) with columns b_j. Also, let $\frac{k_p}{k_{n-q+1}} \mid b_{pq}$ for $n+1 < p+q \leq 2n$, and suppose $\gcd(M) = 1$; then there is a unique frobenius vector*

$$G(M) = \left\{ \left(\sum_{j=1}^{n} (k_j - 1) b_{n-j+1} \right) - A_1 \right\}.$$

Proof. Since $k_n b_{i1} \equiv 0 \mod k_n$ for all i, and all other diagonal entries divide k_n, we have that $\operatorname{ord}_A(b_1) \leq k_n$. For all j such that $1 \leq j < n$ we will show that $\operatorname{ord}_A(b_{n-j+1}) \leq k_j$.

For some j such that $1 \leq j < n$ we choose some column b_{n-j+1}; consider $k_j b_{n-j+1} \mod k_j$. Clearly for the entries $b_{i(n-j+1)}$ where $1 \leq i \leq j$ we have that $k_j b_{i(n-j+1)} \equiv 0 \mod k_i$ since all such $k_i \mid k_j$. Now when $j < i \leq n$ we have $n+1 < i + (n-j+1) \leq 2n$ so that the condition $\frac{k_p}{k_{n-q+1}} \mid b_{pq}$ applies. Thus there exists $y \in \mathbb{N}$ such that

$$\begin{aligned} k_j b_{i(n-j+1)} &= k_j \left(\tfrac{k_i}{k_{n-(n-j+1)+1}} \right) y \\ &= k_j \left(\tfrac{k_i}{k_j} \right) y \\ &= k_i y \equiv 0 \mod k_i \end{aligned}$$

Therefore, for all i we have $\operatorname{ord}_{k_i}\left(b_{i(n-j+1)}\right) \leq k_i \Rightarrow \operatorname{ord}_A(b_{n-j+1}) \leq k_j$ for all $1 \leq j \leq n$. Hence for all j we have $\operatorname{ord}_A(b_{n-j+1}) \leq k_j$. This shows that

$$\Omega(M) \leq \prod_{j=1}^{n} k_j = |A|$$

But since $\gcd(M) = 1$, we have $|A| \leq |MIN| \leq \Omega(M) \leq |A|$ so that $\Omega(M) = |A|$ and Theorem 3.2 shows that $G(M) = \left\{ \left(\sum_{j=1}^{n} (k_j - 1) b_{n-j+1} \right) - A_1 \right\}$. □

Corollary 3.4. *Let $A = dI$ where $d \in \mathbb{N}$ and I the identity matrix, B the same dimension as A, and suppose $\gcd(M) = 1$; then $G(M) = \{(d-1)B_1 - A_1\}$.*

Proof. Follows directly from Corollary 3.3.

□

Later sections will discuss the cases when there exists some $s \in \mathbb{N}$ such that $sb_1 \equiv b_2 \mod A$. Here we explore the case when no such s exists. In the next section, we see how any monoid can be reduced into a case where such an s exists, but under certain circumstances the following provides a simplified solution for cases in which there is a unique frobenius vector.

Theorem 3.5. *Without loss of generality, let* $1 < ord_A(b_j) \leq ord_A(b_i)$. *If there is an* $s_i \in \mathbb{N}$ *such that* $s_i b_i \equiv b_j \mod A$ *for* $i, j \in [1, m]$ *with* $i \neq j$ *then for every pair* b_i, b_j *we have* $\gcd(ord_A(b_i), ord_A(b_j)) = ord_A(b_j)$.

Proof. Now suppose that there exists an $s_i \in \mathbb{N}$ such that $s_i b_i \equiv b_j \mod A$. Then we have

$$\operatorname{ord}_A(b_j) = \operatorname{ord}_A(s_i b_i) = \frac{\operatorname{ord}_A(b_i)}{\gcd(s_i, \operatorname{ord}_A(b_i))}$$

Thus $\operatorname{ord}_A(b_j) \mid \operatorname{ord}_A(b_i)$ so that $\gcd(\operatorname{ord}_A(b_i), \operatorname{ord}_A(b_j)) = \operatorname{ord}_A(b_j)$.

□

Corollary 3.6. *Without loss of generality, let* $1 < ord_A(b_j) \leq ord_A(b_i)$. *If all* b_i, b_j *where* $i, j \in [1, m]$ *with* $i \neq j$ *are pairwise relatively prime, then there is no* $s_i \in \mathbb{N}$ *such that* $s_i b_i \equiv b_j \mod A$.

Proof. The proof follows immediately from Theorem 3.5.

□

We now demonstrate a partial solution for the case when there is no such $s_i \in \mathbb{N}$ so that $s_i b_i \equiv b_j \mod A$ for $i, j \in [1, m]$ with $i \neq j$, namely when the orders of the b_i are pairwise relatively prime.

Theorem 3.7. *A monoid* $M_{\mathbb{N}_0}$ *such that* $ord_A(b_i)$ *are pairwise relatively prime will have at most one frobenius vector,* $G(M) = \{lub(S_M) - A_1\}$.

Proof. Consider $\mathrm{ord}_A(b_i)$. We know that for all i, $\mathrm{ord}_A(b_i) \mid |A|$. Suppose $|A| = \prod_{i=1}^{r} p_i^{k_i}$ where the p_i are distinct primes. So all possible orders for the b_i must be some combination of elements from the multiset of prime divisors of $|A|$. Furthermore, when $\mathrm{ord}_A(b_i)$ are pairwise relatively prime, the orders of the b_i can have no terms in common. Thus $\Omega(M) \leq |A|$. When $\gcd(M) \neq 1$ some equivalence class has no representatives in $M_{\mathbb{N}_0}$ and so $G(M) = \emptyset$. If $\gcd(M) = 1$, by Theorem 3.2 we have $G(M) = \emptyset$ when $\Omega(M) < |A|$ and $G(M) = \{\mathrm{lub}(S_M) - A_1\}$ when $\Omega(M) = |A|$.

□

4 Useful Theorems

The following Theorems are general, basic results which appear in the proofs of later concepts.

Let $N \subset MIN$ be a complete set of residues. We've seen in Theorem 1.6 that for any $g \in G$, we can write $g + A_1 = \mathrm{lub}(N)$ for some complete set of residues. We will now prove two other properties of $\mathrm{lub}(N)$.

Theorem 4.1. *$lub(N) - A_1$ is complete.*

Proof. Let $v = \mathrm{lub}(N) - A_1$, and let $u \in [\succ v]$. Let w be the element in N congruent to u. We know that $u \succ v$, $v + A_1 \geq w$ and $u \equiv w$. Thus for each $i = 1, \ldots, n$ we have $(u)_i > (v)_i$, $(v)_i + 1 \geq (w)_i$, and $(u)_i - (w)_i \in \mathbb{Z}$. Now $(u)_i - (w)_i \geq (u)_i - ((v)_i + 1) > -1$, and $(u)_i - ((v)_i + 1) \geq 0$. Thus $w \leq v + A_1 \leq u$ and $u \in M_{\mathbb{N}_0}$. Finally, $[\succ v] \subset M_{\mathbb{N}_0}$ and v is complete.

□

Theorem 4.2. *Suppose $\omega = lub(N)$, where $\omega \in N$. Then $\omega - A_1 \in G$.*

Proof. By Theorem 4.1, $\omega - A_1$ is complete. Thus there exists a $g \in G$ such that $g \leq \omega - A_1$. By Theorem 1.6, there exists a complete set of residues $N' \subset MIN$ such that $g = \mathrm{lub}(N') - A_1$. Choose $\omega' \in N'$ such that $\omega \equiv \omega'$. But $\omega' \leq \mathrm{lub}(N') = g + A_1 \leq \omega$ so $\omega = \omega'$. Now $\mathrm{lub}(N') \geq \omega' = \omega$. Thus $\omega - A_1 = \mathrm{lub}(N') - A_1 \in G$.

□

5 Reduction formula

When solving the Frobenius number problem with three generators, Selmer found it useful to consider only the case where the three generators are relatively prime. We would like to take a similar approach to the Frobenius vector problem where $m = n = 2$.

In 1960, Johnson proved that $f(a_1, da_2, \ldots, da_k) = d \cdot f(a_1, \ldots, a_k)$, where a_1 need not be the smallest generator. Using this reduction formula, the Frobenius problem can be reduced to the case where any $k-1$ of the k generators have a gcd of 1. When $k = 3$, this reduces the problem down to the case were the three generators are pairwise relatively prime. This is the reduction formula Selmer used to solve the three generator case.

The next two theorems provide a perfect generalization of Johnson's formula into multiple dimensions. Loosely speaking, the first theorem considers the case where all vectors but a column of A are multiples of matrix D, and the second theorem considers the case where all vectors but a column of B are multiples of D. For notation simplicity we assume without loss of generality that the column receiving special treatment is either the first column of M in the first theorem, or the last column of M in the second theorem.

Theorem 5.1. *Let $M = [a_1|M']$ and $N = \left[\frac{Da_1}{|D|}\middle| DM'\right]$ be integer matrices where $D \in M_n[\mathbb{Z}]$ with $|D| \neq 0$ and $gcd(N) = 1$ with M or N simplicial. Then $D \cdot F(M) = F(N)$.*

To prove this theorem we will first prove that the transformations between $S(M)_{\mathbb{N}_0}$ and $S(N)_{\mathbb{N}_0}$ preserve inequality, congruence, least upper bounds, the MIN set, the G-set, and finally the F-set. Let A and A' be the left-most n by n submatrices of M and N respectively. Because in general M and N have different left n by n sub-matrices, the symbols $\geq$, $\equiv$, lub, and MIN are all ambiguous. For the duration of this proof we will always use a subscript to specify the context of each.

Lemma 5.2. *For any vectors v and w, we have $v \geq_M w \iff Dv \geq_N Dw$.*

Proof. Notice that for any vector u, we know that: $u \geq_M 0$
$\iff$ There exist non-negative reals $\alpha_1, \ldots, \alpha_n$ such that $\sum \alpha_i a_i = u$
$\iff$ There exist non-negative reals $\alpha_1, \ldots, \alpha_n$ such that $\sum \alpha_i D a_i = Du$
$\iff Du \geq_N 0$.
Now by letting $u = v - w$ we can see that $v - w \geq_M 0 \iff D(v-w) \geq_N 0$, which proves the lemma. □

All columns of M are $\geq_M 0 \iff$ all columns of N are $\geq_N 0$. Because one of M and N is simplicial, they must both be simplicial.

Lemma 5.3. *For any vectors v and w, we have $v \equiv_M w \iff Dv \equiv_N Dw$.*

Proof. Notice that for any vector u, we know that: $u \equiv_M 0$
$\implies$ There exist integers $c_1, \ldots, c_n$ such that $\sum c_i a_i = u$
$\implies$ There exist integers $c_1, \ldots, c_n$ such that $\sum c_i Da_i = Du$
$\implies Du \equiv_N 0$.
Now by letting $u = v - w$ we can see that $v - w \equiv_M 0 \implies D(v-w) \equiv_N 0$, which proves that multiplication by D preserves congruence. Because $S(N)_{\mathbb{N}_0}$ is dense, it contains all residue classes mod A', as does the set $D \cdot B_{\mathbb{N}_0}$. Thus multiplication by D is onto. Finally, $|A'| = \left|\frac{Da_1}{|D|}, Da_2, \ldots, Da_m\right| = \frac{1}{|D|}\left|Da_1, Da_2, \ldots, Da_m\right| = \frac{1}{|D|}|DA| = |A|$, so the number of residues mod A is equal to the number of residues mod A', and thus multiplication by D is a bijection of residue classes. □

Lemma 5.4. *For any vectors $v_1, \ldots, v_k$, we have $D \cdot lub_M(v_1, \ldots, v_k) = lub_N(Dv_1, \ldots, Dv_k)$.*

Proof. For $i = 1, \ldots, k$ we have $lub_M(v_1, \ldots, v_k) \geq_M v_i$, so by Lemma 5.2 $D \cdot lub_M(v_1, \ldots, v_k) \geq_N Dv_i$, thus $D \cdot lub_M(v_1, \ldots, v_k) \geq_N lub_N(Dv_1, \ldots, Dv_k)$. Similarly, for $i = 1, \ldots, k$ we have $lub_N(Dv_1, \ldots, Dv_k) \geq_N Dv_i$, so by Lemma 5.2 $D^{-1} \cdot lub_N(Dv_1, \ldots, Dv_k) \geq_M v_i$, and $D^{-1} \cdot lub_N(Dv_1, \ldots, Dv_k) \geq_M lub_M(v_1, \ldots, v_k)$, and thus $lub_N(Dv_1, \ldots, Dv_k) \geq_N D \cdot lub_M(v_1, \ldots, v_k)$. □

Lemma 5.5. $D \cdot MIN_M = MIN_N$.

Proof. It has been proven that both sets are contained in $D \cdot B_{\mathbb{N}_0}$. The sets are the elements that are minimal in their congruence class. From Lemmas 5.2 and 5.3 the two sets both use the same congruence condition and the same partial ordering, and thus the two sets are equal. □

We now have proven enough structural similarities to prove Theorem 5.1.

Proof. Let T be the set of points that can be written as the lub_M of a complete set of residues from MIN_M, and let $T^{'}$ be the set of points that can be written as the lub_N of a complete set of residues from MIN_N. It has been proven that $G(M)+A_1$ is contained in T. Also, all vectors in T are g-complete, thus $G(M)+A_1$ is equal to the set of minimal elements in T. By Lemma 5.2 this implies that $D\cdot G(M)+DA_1$ is equal to the set of minimal elements in $D\cdot T$. Similarly, $G(N)+A_1^{'}$ is equal to the set of minimal elements in $T^{'}$. From Lemmas 5.4 and 5.5, we can see that $D\cdot T=T^{'}$. Thus $D\cdot G(M)+DA_1=G(N)+A_1^{'}$. This result can be stated more succinctly in terms of the F-set. It becomes $D\cdot(F(M)-A_1-B_1)+DA_1=F(N)-A_1^{'}-DB_1+A_1^{'}$ or $D\cdot F(M)=F(N)$. □

Because the result of the second theorem mirrors the result of the first theorem, we will reuse much of the notation. We certainly are not assuming that Lemmas 5.2, 5.3, 5.4 and 5.5 remain valid in this new context.

Theorem 5.6. *Let* $M=[M',b_m]$ *and* $N=\left[DM'\middle|\frac{Db_m}{|D|}\right]$ *be integer matrices where* $D\in M_n[\mathbb{Z}]$ *with* $|D|\neq 0$ *and* $gcd(N)=1$ *with* M *or* N *simplicial. Then* $D\cdot F(M)=F(N)$.

First we will see that multiplication by D preserves both types of inequality.

Lemma 5.7. *For any vectors* v *and* w, *we have* $v\geq_M w \iff Dv\geq_N Dw$, *and* $v\succ_M w \iff Dv\succ_N Dw$.

Proof. Notice that for any vector u, we know that: $u\geq_M 0$
$\iff$ There exist non-negative reals $\alpha_1,\ldots,\alpha_n$ such that $\sum\alpha_i a_i=u$
$\iff$ There exist non-negative reals $\alpha_1,\ldots,\alpha_n$ such that $\sum\alpha_i Da_i=Du$
$\iff Du\geq_N 0$.
Now by letting $u=v-w$ we can see that $v-w\geq_M 0 \iff D(v-w)\geq_N 0$, which proves the first part of the lemma. The exact same argument with positive real for the α_i proves the second part. □

All columns of M are $\geq_M 0 \iff$ all columns of N are $\geq_N 0$. Because one of M and N is simplicial, they must both be simplicial. Now we will prove Theorem 5.6.

Proof. Throughout this proof we will consider congruence (mod D), where we define congruence as $a \equiv_D b$ iff $a - b \in D \cdot \mathbb{Z}^n$. We are considering the cosets of $\frac{\mathbb{Z}^n}{D \cdot \mathbb{Z}^n}$ under addition, so we have an equivalence relation and a group under addition. Suppose for contradiction that S_N does not contain some residues (mod D), say r. Now the sets S_N and $r + D_{\mathbb{Z}}$ are disjoint. Let v be any vector in $\mathbb{R}^n$. We know that both $DA_1 \equiv_D 0$ and $DA_1 = Da_1 + \cdots + Da_n \succ_N 0$. Thus for sufficiently large $k \in \mathbb{Z}$, we have $v - r \prec_N k \cdot DA_1$, or $v \prec_N k \cdot DA_1 + r \in \mathbb{Z}^n / S_N$. Thus v is not complete and $|G(N)| = 0$. This contradicts the fact that $gcd(N) = 1$. Thus S_N contains all residues (mod D). All but the last column of N is $\equiv_D 0$, thus $\frac{Db_m}{|D|}$ is a generator for all $|D|$ congruence classes.

We will define the vector function $f(x) = (|D| - 1)\frac{Db_m}{|D|} + D \cdot x$, which has inverse $f^{-1}(x) = D^{-1}\left(x - (|D| - 1)\frac{Db_m}{|D|}\right)$. By Lemma 5.7 this function preserves inequality and $\succ$ in both directions.

First we will see that if g is complete in $M_{\mathbb{N}}$, then $f(g)$ is complete in $N_{\mathbb{N}}$. Let v' be an integer vector such that $v' \succ_N f(g)$. For some $k = 0, \ldots, |D|-1$ we have $v' \equiv_D k\frac{Db_m}{|D|}$. We know that $v' - k\frac{Db_m}{|D|} \succ_N f(g) - k\frac{Db_m}{|D|} \geq f(g) - (|D| - 1)\frac{Db_m}{|D|} = D \cdot g$, and that $v' - k\frac{Db_m}{|D|} \equiv_D 0$. Thus we can write $v' - k\frac{Db_m}{|D|} = D \cdot v$ where v is an integer vector with $v \succ_M g$. Because g is complete in $M_{\mathbb{N}}$, $v \in M_{\mathbb{N}}$ and thus $D \cdot v \in D \cdot M_{\mathbb{N}} \subset N_{\mathbb{N}}$. Finally, by writing $v' = D \cdot v + k\frac{Db_m}{|D|}$ we see that $v' \in N_{\mathbb{N}}$ and $f(g)$ is complete.

Conversely, we will see that if $f(g)$ is complete in $N_{\mathbb{N}}$, then g is complete in $M_{\mathbb{N}}$. Let v be an integer vector such that $v \succ g$. Now $f(v) \succ f(g)$. Because $f(g)$ is complete, there exist non-negative integers $c_1, \ldots, c_{n+m}$ such that $f(v) = \sum_{i=1}^{n} c_i Da_i + \sum_{i=1}^{m-1} c_{i+n} Db_i + c_{n+m}\frac{Db_m}{|D|}$. Because $f(v) \equiv_D (|D| - 1)\frac{Db_m}{|D|}$, we have $c_{n+m} \equiv (|D| - 1) \pmod{|D|}$. Letting $c'_{n+m} = \frac{c_{n+m} - |D| + 1}{|D|} \in \mathbb{N}$ we have $D \cdot v = f(v) - (|D| - 1)\frac{Db_m}{|D|} = \sum_{i=1}^{n} c_i Da_i + \sum_{i=1}^{m-1} c_{i+n} Db_i + c'_{n+m} Db_m$ and thus $v \in M_{\mathbb{N}}$ and g is complete.

We will show that $f(G(M)) = G(N)$ by showing that the sets are contained in one another.

Let $g \in G(M)$. Because $f(g)$ is complete in $N_{\mathbb{N}}$, there exists some g' such that $f(g') \leq_N f(g)$ and $f(g') \in G(N)$. Now g' is complete in $M_{\mathbb{N}}$, so there exists some $g'' \in G(M)$ such that $g'' \leq_M g' \leq_M g$. Now $g'', g \in G(M)$, so $g'' = g' = g$, and $f(g) = f(g') \in G(N)$.

Now let $f(g) \in G(N)$. Because g is complete in $M_{\mathbb{N}}$ there exists some

$g' \in G(M)$ such that $g' \leq g$. We've shown that $f(g') \in G(N)$ so $f(g') \leq f(g)$ implies that $f(g') = f(g)$ and $g = g' \in G(M)$. Thus $f(G(M)) = G(N)$.

Writing out function f we have $(|D| - 1)\frac{Db_m}{|D|} + D \cdot G(M) = G(N)$. Substituting in the formula for the F-set we get $(|D| - 1)\frac{Db_m}{|D|} + D \cdot (F(M) - M_1' - b_m) = F(N) - DM_1' - \frac{Db_m}{|D|}$ or $D \cdot F(M) = F(N)$. □

Theorems 5.1 and 5.6 are equivalent to the following unification:

Theorem 5.8. *Let M_1, M_2 be matrices with n rows and let c be a $n \times 1$ vector. Let $M = \left[M_1 \middle| c \middle| M_2\right]$ and $N = \left[DM_1 \middle| \frac{Dc}{|D|} \middle| DM_2\right]$ be $n \times (n + m)$ integer matrices where $D \in M_n[\mathbb{Z}]$ with $|D| \neq 0$ and $gcd(N) = 1$ with M or N simplicial. Then $D \cdot F(M) = F(N)$.*

Proof. When c is one of the first n columns of M the result follows from Theorem 5.1. When c is one of the last m columns of M the result follows from 5.6. □

Next, we will find what the transformation from N to M does to the gcd's of submatrices of M.

Theorem 5.9. *Define M, N, c, and D as in Theorem 5.8. Let M' and N' be sub-matrices of M and N respectively which are taken from corresponding columns of M and N. If column c is not contained in M', we have* $\gcd(M') = \frac{\gcd(N')}{|D|}$. *Otherwise,* $\gcd(M') \leq \gcd(N')$.

Proof. First, we will show that the determinants of all $n \times n$ submatrices which do not include c have been reduced by a factor of $|D|$, while the determinants of all other $n \times n$ submatrices have not been changed. Consider an $n \times n$ submatrix of M which does not contain c. It is D times its corresponding matrix in M, and thus the first determinate is $|D|$ times as large. Next, consider a $n \times n$ submatrix of N containing $\frac{Dc}{|D|}$, say $\left[\frac{Dc}{|D|} \middle| DS\right]$. Its determinate is the same as that of its corresponding submatrix in M: $\left|\left[\frac{Dc}{|D|} \middle| DS\right]\right| = |D|\left|\left[\frac{c}{|D|} \middle| S\right]\right| = \left|[c|S]\right|$.

Now suppose that M' does not contain c. Here, $DM' = N'$, so by Lemma 23 of last summer's paper, $|D| \gcd(M') = \gcd(DM') = \gcd(N')$. Finally, suppose M' contains c. Consider all pairs of corresponding $n \times n$ submatrices

of $M^{'}$ and $N^{'}$. Either the determinants are equal or the determinant of the submatrix of $N^{'}$ is $|D|$ times as large. In all cases, the first determinant divides the second, thus $\gcd(M^{'}) \leq \gcd(N^{'})$. $\square$

What remains is the show how Theorem 5.8 can be used to reduce the Frobenius vector problem into the case where any $n+m-1$ of the $n+m$ generating vectors have a gcd of 1.

Theorem 5.10. *Let $N \in M_{n\times(n+m)}[\mathbb{Z}]$ with $\gcd(M) = 1$. Then there exists $D \in M_n[\mathbb{Z}]$ and $M \in M_{n\times(n+m)}[\mathbb{Z}]$ where every $n \times (n+m-1)$ submatrix of M has a gcd of 1 and $F(N) = D \cdot F(M)$.*

Proof. Suppose that $N = \left[a_1^{'} \middle| N^{'}\right]$ with $gcd(N^{'}) = d$. Consider the matrix $\left[da_1^{'}, \middle| N^{'}\right]$. Every minor of this matrix which is also a minor of $N^{'}$ is divisible by d by assumption, as are all other minors of N because they contain the column $da_1^{'}$. Because $gcd(N^{'}) = d$, we must have $gcd\left(da_1^{'} \middle| N^{'}\right) = d$. By Theorem 4 from last summer's paper, there exist some $D \in M_n(\mathbb{Z})$ with $|D| = d$ and some $M = \left[a_1 \middle| M^{'}\right] \in M_{n,n+m}(\mathbb{Z})$ with a gcd of $\frac{d}{|D|} = 1$, such that $\left[da_1^{'} \middle| N^{'}\right] = D \cdot \left[a_1 \middle| M^{'}\right] = \left[Da_1 \middle| DM^{'}\right]$. The Frobenius vector problem is now reduced in the following manner: $F\left(a_1^{'} \middle| N^{'}\right) = F\left(\frac{Da_1}{|D|} \middle| DM^{'}\right) = D \cdot F\left(a_1 \middle| M^{'}\right)$, where the first equality is because the matrices have been chosen to be equal and the second equality is by Theorem 5.8.

By Theorem 5.9, $1 = \frac{\gcd(N^{'})}{|D|} = \gcd(M^{'})$. Also by Theorem 5.9, we have not increased any of the other gcd's. We perform the same process with every other set of $n+m-1$ vectors. We will be left with $F(N) = D_1 D_2 \cdots D_{n+m} \cdot F(M)$ where M is a matrix such that every $n \times (n+m-1)$ submatrix has a gcd of 1.

Notice that Theorem 5.8 performs a linear transformation on the vectors followed by multiplying one vector by a constant. When used repeatedly this process performs a linear transformation on the directions of the vectors, but not on the magnitudes of the vectors. $\square$

6 Small General Results

Theorem 6.1. *Let g_0 be the unique frobenius vector of $M_{\mathbb{N}}^0$ such that $g_0 + A_1 = lub\{w_i\}$. Let $M = [M^0 b_2]$. If for any k, $(b_2)_k > (w_i)_k$, then $g_0 \in G(M)$*

Proof: Let g_0 be such that $g_0 + A_1 = lub(w_i)$. If $b_2 \in M^0_{\mathbb{N}}$, be an earlier theorem, $M^0_{\mathbb{N}} = M_{\mathbb{N}}$, so $G(M^0) = G(M)$. Let $b_2 \neq M^0_{\mathbb{N}}$. For any coordinate k, without loss of generality, $(b_2)_k > (w_i)_k$.
Then for any $m \in MIN$, $m = (c_1b_1 + c_2b_2)_k > (w_i)_k$ for $c_2 > 0$ because $(c_1b_1 + c_2b_2)_k > (b_2)_k > (w_i)_k$. So $lub(w_i)$ is still minimal $\Rightarrow g_0 \in G$. $\square$.

Lemma 6.2. *Set $M' = [M|b_1]$. If $b_1 \in M_{\mathbb{N}}$ then $M_{\mathbb{N}} = M'_{\mathbb{N}}$ and $G(M) = G(M')$.*

Proof: Let the a_i's denote the $n + m$ columns of M. Suppose $b_1 \in M_{\mathbb{N}}$. Then we have that $b_1 = \sum_{j=1}^{n} c_j a_j$ for some non negative integers c_j. Consider the monoid generated by $M' = Mb_1$. Every element b_k in the monoid of M', S', can be expressed as $b_k = \sum_{i=1}^{n} d_i a_j + d_k b_1$ where d_k and the d_i's are also non negative integers. But then, for $b_k \in S'$,

$$\begin{aligned} b_k &= \sum_{i=1}^{n} d_i a_j + d_k b_1 \\ &= \sum_{i=1}^{n} d_i a_i + d_k \sum_{j=1}^{n} c_j a_j \\ &= \sum_{j'=1}^{n} c'_{j'} a_{j'}. \end{aligned}$$

But then for any $b_k \in S'$, $b_k \in S$. Every b_k in S is in S' because the columns of M are contained in the columns of M'. So, $S = S'$. Therefore, these two identical monoids have identical Frobenius numbers, so $G(M) = G(M')$. $\square$.

Lemma 6.3. *Suppose that $M = [AB]$ and $M' = [ABb_i]$ with $b_i \notin MIN'$. Then $M_{\mathbb{N}} = M'_{\mathbb{N}}$.*

Proof: Suppose $b_i \notin MIN'$. Then there exists some v with $v \equiv b_i$ and $v < b_i$. $v < b_i$ and $v \in MIN' \Rightarrow v = \sum c_j b_j$ with $j \neq i$. $b_i = v + d_1a_1 + d_2b_2 = \sum c_j b_j + d_1a_1 + d_2a_2 \in M_{\mathbb{N}}$. Therefor $b_i \in M_{\mathbb{N}}$. By lemma 6.2, $M_{\mathbb{N}} = M'_{\mathbb{N}}$. $\square$

Lemma 6.4. *If $x \in MIN$, with $\omega \in M_{\mathbb{N}}$, then for some $u = (x - \omega) \cap M_{\mathbb{N}}$, $u \in MIN$.*

Proof: It is equivalent to show that if $u \notin MIN$, then $x \notin MIN$. Suppose $u \notin MIN$, then there is some $w \in M_{\mathbb{N}}$ with $w \equiv u \mod A$ and $w < u$. But then $w+\omega \equiv u+\omega \mod A$ and $w+\omega < u+\omega$. So $x = u+\omega \notin MIN$. $\square$

Lemma 6.5. *Let $M = [Ab_1b_2]$ and $M' = [Ab_1(b_1+b_2)]$. If $w \in MIN$ and $w \in M'_{\mathbb{N}}$, then $w \in MIN'$.*

Proof: Suppose towards contradiction that $w \in MIN$ and $w \in M'_{\mathbb{N}}$, but $w \notin MIN'$. So there is some $u \in M'_{\mathbb{N}}$, with $u \equiv w$ and $u < w$. $u = c_1a_1 + c_2a_2 + d_1b_1 + d_2(b_1+b_2) = c_1a_1 + c_2a_2 + (d_1+d_2)b_1 + d_2b_2 \in M_{\mathbb{N}}$. But then $u \in M_{\mathbb{N}}$ with $u \equiv w$ and $u < w \Rightarrow w \notin MIN$. But this is a contradiction of $w \in MIN$. $\square$

Lemma 6.6. *Let $M = [Ab_1b_2]$. Let g_0 be the unique frobenius vector generated by the submonoid $M^0 = [Ab_1]$. Suppose $b_2 \notin M^0_{\mathbb{N}}$, with $(b_2)_x > (b_1)_x$ and $b_2 \leq lub(\{jb_i | 1 \leq j \leq |A|\})$. Then there exists some $g_1 \in G(M)$ with $(g_1)_y < (g_0)_y$.*

Proof: If $b_2 \notin M^0_{\mathbb{N}} \Rightarrow b_2 \equiv kb_1$ with $1 \leq k \leq |A|$. If $b_2 \notin MIN$, then $b_2 = c_1a_1 + c_2a_2 + d_1b_1 \Rightarrow b_2 \in M^0_{\mathbb{N}}$, which contradicts our hypothesis. So $b_2 \in MIN$.

So $b_2 \equiv kb_1$ and b_2 incomparable to kb_1. Likewise, $b_2 \equiv kb_1 \Rightarrow b_2 + b_1 \equiv (k+1)b_1$. Likewise, b_2 is incomparable to $kb_1 \Rightarrow b_2 + b_1$ is incomparable to $(k+1)b_1$. Therefor, $b_2 + b_1 \in MIN$ for $k < a_{1,1}a_{2,2}$.

Likewise, for all $b_2 + d_1b_1$ such that $0 \leq d_1 \leq (a_{1,1}a_{2,2} - k)$, $b_2 + d_1b_1 \equiv (k+d_1)b_1$ and $b_2 + d_1b_1$ incomparable to $(k+d_1)b_1$, so $b_2 + d_1b_1 \in MIN$.

So there is subset of MIN, say W such that $W = \{b_1, 2b_1, \ldots, (k-1)b_1, b_2, b_2+b_1, b+2+2b_1, \ldots, b_2+(|A|-k)b_1\}$. By Theorem 4.1, $lub(W) - A_1 = h$ is g-complete.

However $(lub(W))_y < (lub(\{jb_1\}))_y$ because $(lub(W))_y = ((k-1)b_1)_y$ or $(lub(W))_y = ((b_2+(|A|-k)b_1)_y$. In either case, $(lub(W))_y < (lub(\{jb_1\}))_y = (|A|b_1)_y$.

So there is some $h = lub(W) - A_1$, with h g complete by Theorem 4.1. Either h is a g vector or there is some $g_k < h$ with $g_k < h$. Either way there exists some $g_1 \in G(M)$ with $(g_1)_y < (g_0)_y$. $\square$

Lemma 6.7. *Let $M = [Ab_1b_2]$ with diagonal A. Let g_0 be the unique frobenius vector generated by the submonoid $M^0 = [Ab_1]$. Suppose $b_2 \notin M^0_{\mathbb{N}}$, with $(b_2)_y > (b_1)_y$ and $b_2 \leq lub(\{jb_i | 1 \leq j \leq |A|\})$. Then there exists some $g_1 \in G(M)$ with $(g_1)_x < (g_0)_x$.*

Proof: This follows from the argument above, exchanging x and y. $\square$

Lemma 6.8. *Let $M = [Ab_1b_2]$ with diagonal A. Let g_0 be the unique frobenius vector generated by the submonoid $M^0 = [Ab_1]$. If $b_2 \notin M^0_{\mathbb{N}}$ and $|G(M)| = 1$, then $g_0 \notin G(M)$.*

Proof: By lemmas 6.6 and 6.7, there is some $g_1 \in G(M)$, and wlog, with $(g_1)_x < (g_0)_x$. If $(g_1)_y > (g_0)_y$, then g_0 and g_1 are incomparable, so $|G(M)| \neq 1$. So $(g_1)_y \leq (g_0)_y$. But then $g_1 < g_0$, so $g_0 \notin G(M)$. $\square$

Theorem 6.9. *Let $g_0 \in G(M)$ with $M = [AB]$ and let $M' = [ABb_1]$. If $b_1 \not\leq g_0 + A_1$, then $g_0 \in G(M')$.*

Proof: If $b_1 > g_0 + A_1$, then $b_1 \in M_{\mathbb{N}}$. By lemma 6.2, $M_{\mathbb{N}} = M'_{\mathbb{N}}$, so $G(M) = G(M')$; hence, $g_0 \in G(M')$.

If $b_1 > g_0 + A_1$ and $b_1 \not\leq g_0 + A_1$, then b_1 is incomparable to g_0. Without loss of generality, assume $(g_0)_x < (b_1)_x$ and $(g_0)_y > (b_1)_y$. By theorem 6.1, $g_0 \in G(M')$. $\square$

7 A further reduction in the case where b_2 lies along an a vector

Theorem 7.1. *Suppose $m = n = 2$ and $b_1 = ka_2$ for some $k \in \mathbb{R}^+$. Then there exist $D \in M_2[\mathbb{Z}]$ and $a, b, d \in \mathbb{N}_0$ such that $F(M) = D \cdot \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & a & b & d \end{bmatrix}$*

By Theorem 5.10, there exist $D_1 \in M_n[\mathbb{Z}]$ and $M' \in M_{n\times(n+m)}[\mathbb{Z}]$ where every 2×3 submatrix of M has a gcd of 1 and $F(M) = D_1 \cdot F(M')$. Let $M' = \left[a'_1, a'_2, b'_1, b'_2\right]$. We still have $b'_1 = k'a'_1$ for some $k' \in \mathbb{R}$ because Theorem 5.10 performs a linear transformation on the directions of the generators.

Because $a_1^{'}$ and $b_1^{'}$ are integer vectors, $k^{'} = \frac{b}{a}$ for some relatively prime $a, b \in \mathbb{N}$. Using the Euclidean Algorithm, we can write $x = \frac{1}{a}a_2^{'}$ as a linear combination of $a_2^{'}$ and $b_1^{'}$, thus $\frac{1}{a}a_2^{'}$ is an integer vector. Next, we see that $a_2^{'} = a \cdot x$ and $b_1^{'} = b \cdot x$. Let $D_2 = \left[a_1^{'}, x\right]$. We have $\gcd\left[a_1^{'}, a_2^{'}, b_1^{'}\right] = 1$ and $\left[a_1^{'}, a_2^{'}, b_1^{'}\right]_{\mathbb{N}_0} \subset D_{2,\mathbb{N}_0}$, thus $D_{2,\mathbb{N}_0}$ is dense, $|D_2| = 1$, and D_2 is invertible over $\mathbb{Z}$. Let $D_2^{-1}b_2^{'} = \begin{bmatrix} c \\ d \end{bmatrix}$. By Theorem 5.8, we have $F(M^{'}) = F\left[D_2 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & a & b \end{bmatrix} \Big| \frac{b_2^{'}}{|D_2|}\right] = D_2 \cdot F \begin{bmatrix} 1 & 0 & 0 & c \\ 0 & a & b & d \end{bmatrix}$.

However, $\gcd(a_2^{'}, b_1^{'}, b_2^{'}) = 1$, and the previous application of Theorem 5.8 does not increase this gcd by Theorem 5.9. Thus $\gcd \begin{bmatrix} 0 & 0 & c \\ a & b & d \end{bmatrix} = 1$, we must have $c = 1$. From our simplicial assumption, a, b, and d do not have different signs, so we can choose them to be non-negative.

8 A Needlessly Long Proof Reducing the $1-0-0-0$ Case to the 1-0-0-0 and $c = 1$ Case

Let $M^c = \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & a & b & d \end{pmatrix}$.

Definition 8.1. *Let MIN^c denote the set of minimal elements in each residue class for $M_{\mathbb{N}}^c$.*

Lemma 8.2. *Let $M^c = \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & a & b & d \end{pmatrix}$ and $M^{c+i} = \begin{pmatrix} 1 & 0 & 0 & c+i \\ 0 & a & b & d \end{pmatrix}$ with $b_2 = \binom{c}{d}$ and $b_2' = \binom{c+i}{d}$. If $m = c_1b_1 + c_2b_2$ and $m' = c_1b_1 + c_2b_2$, then $m \in MIN^c \iff m' \in MIN^{c+1}$.*

Proof:
[$\Leftarrow$] It is equivalent to show that if $m \notin MIN^c$, then $m' \notin MIN^{c+i}$.

$m \notin MIN^c \Rightarrow \exists\ w \in MIN^c$, with $w < m$ and $w \equiv m \mod A$. Let $w = e_1b_1 + e_2b_2$. Consider $w' = e_1b_1 + e_2b_2 + e_2\binom{i}{0} = e_1b_1 + e_2b_2'$. $w' \equiv w \equiv m \equiv m'$ because the addition of a_1 does not change the residue class and $w \equiv m$.

$e_2 \leq c_2$ because $(w)_x \leq (m)_x$ because $w < m$ and b_1 has no x component. $e_2 \leq c_2 \Rightarrow e_2\binom{i}{0} \leq c_2\binom{i}{0}$. Hence,

$$\begin{aligned} w' &= e_1b_1 + e_2b_2 + e_2\tbinom{i}{0} < \\ &< c_1b_1 + c_2b_2 + e_2\tbinom{i}{0} \leq \\ &\leq c_1b_1 + c_2b_2 + c_2\tbinom{i}{0} = \\ &= c_1b_1 + c_2b_2' = m'. \end{aligned}$$

$w' \in M'_{\mathbb{N}}$ because $w' = e_1b_1 + e_2b_2'$, so $w' < m' \Rightarrow m' \notin MIN^{c+i}$.

[$\Rightarrow$] It is equivalent to show that if $m' \notin MIN^{c+i}$, then $m \notin MIN^c$.

$m' \notin MIN^{c+i} \Rightarrow \exists\ w' \in MIN^{c+i}$, with $w' < m'$ and $w' \equiv m' \mod A$. Let $w' = e_1b_1 + e_2b_2' = e_1b_1 + e_2b_2 + e_2\binom{i}{0}$. Consider $w = e_1b_1 + e_2b_2$. $w' \equiv w \equiv m \equiv m'$ because the addition of a_1 does not change the residue class and $w' \equiv m'$.

Claim: $e_2 \leq c_2$. $(w')_x \leq (m')_x$, and because the x coordinate is independent of b_1 and only dependent on b_2', if $(w')_x \leq (m')_x$, then $e_2 \leq c_2$. So $e_2b_2 \leq c_2b_2$, so $(w)_x \leq (m)_x$.

Now $(m)_y = (m')_y \geq (w')_y = (w)_y$, so $(m)_y \geq (w)_y$.

Now for m' and w' if $(m')_y = (w')_y$, then $(m')_x > (w')_x$, and if $(m')_x = (w')_x$, then $(m')_y > (w')_y$. If not, $m' = w'$, so $m' \in MIN^{c+i}$.

So we have that
$(m)_y > (w)_y$ and $(m)_x = (w)_x$,
$(m)_y = (w)_y$ and $(m)_x > (w)_x$ or
$(m)_y > (w)_y$ and $(m)_x > (w)_x$.

In any case, $w < m$, $w \equiv m \mod A$ and $w \in M_{\mathbb{N}}$. So $m \notin MIN^c$. $\square$

Lemma 8.3. *Consider M^c and M^{c+i} as above. Then for any $g_i \in G(M^c)$, there is some $g_i' \in G(M^{c+i})$ such that if $g_i + A_1 = lub\{w_k\}$, then $\exists\ g_i'$ with $g_i + A_1 = lub\{w_k'\}$ and vice versa. Hence, $|G(M^c)| = |G(M^{c+i})|$.*

Proof: Consider $g_i \in G(M^c)$. $g_i + A_1 = lub\{w_k\}$, with $\{w_k\} \subset MIN^c$. For each w_k, $\exists w_k' \in MIN^{c+i}$ with $w_k \equiv w_k'$ by lemma 8.2. Consider $\{w_k'\}$;

$\{w'_k\}$ is a complete set of coset representatives and $\{w'_k\} \subset MIN^{c+i}$, so $h = lub\{w'_k\}$ is g complete.

Suppose towards contradiction that h is not a g vector. Then $\exists\ g_\star$, with $g_\star < h$, and $g_\star$ complete. Then $g_\star + A_1 = lub\{u'_k\}$ for some $\{u'_k\} \subset MIN^{c+i}$.

Consider $\exists\ \{u_k\} \subset MIN^c$. $\{u_k\}$ is a complete set of coset representatives, and $lub\{u_k\} < lub\{w_k\}$ because $lub\{u'_k\} < lub\{w'_k\} \Rightarrow g_i \notin G(M)$, which is a contradiction. So $h = lub\{w'_k\} - A_1 \in G(M^{c+i})$.

We can follow a similar argument to show that if there is some $g'_j \in G(M')$ there must be a corresponding $g_j \in G(M^c)$. Hence, $|G(M^c)| = |G(M^{c+i})|$. $\square$

Theorem 8.4. *Let the submonoid $M^0 = [Ab_1]$ generate some frobenius vector, g_0. Let c=1. Then $(g_i)_x = i - 1$ for any $g_i \in G(M^c)$.*

Proof: Because b_1 is along the y axis, we know that $G(M^0) = |A|b_1 - A_1 = |A|\binom{0}{b} - \binom{1}{a} = \binom{-1}{|A|b-a} = \binom{-1}{a(b-1)}$. So $g_0 = \binom{-1}{a(b-1)}$.

Consider $b_2 = \binom{1}{d}$. If $b_2 \notin MIN$ then by lemma 6.3 $g_0 = G(M^c)$.

So $b_2 \in MIN \Rightarrow b_2 \equiv jb_1$ with b_2 incomparable to jb_1. Likewise, $hb_1 + b_2 \in MIN$ for $0 \leq h \leq |A| - j = a - j$.

There are $|A| = a$ equivalence classes, with the j^{th} through a^{th} represented by $hb_1 + b_2$ and the first through $j - 1^{th}$ represented by kb_1. Let the union of the two sets, $\{hb_1 + b_2 | 0 \leq h \leq a - j\} \cup \{kb_1 | 1 \leq k \leq j - 1\}$ be denoted $\{w_k\}$. Then $lub\{w_k\} - A_1 = \gamma$ is g-complete.

Likewise, there is no $g_\star \in G(M^c)$ with $g_\star < \gamma$ because then $(g_\star)_x = 0$ or -1. But the only g vector with $(g)_x = -1$ is not less than γ and γ is minimal for an x coordinate of 0 by construction. So γ is a g vector, g_1 with $(g_1)_x = 1 - 1 = 0$.

Suppose that you have two consecutive g vectors, g_i and g_{i+1} with $(g_i)_x = i - 1$. Suppose towards contradiction that $(g_i)_x < (g_{i+1})_x$ and $(g_i)_x + 1 \neq (g_{i+1})_x$.

$g_i + A_1 = lub\{u_k\}$ with some u_k with $u_k = \alpha b_1 + (i-1)b_2$ because $(g_i)_x = (i-1)$. However, by lemma 6.4, $u_k \in MIN \Rightarrow (i-1)b_2 \in MIN$. $g_{i+1} \in G(M^c) \Rightarrow sb_2 \in MIN$ for some $s > i-1$.

However, for any value of s, by lemma 6.4, $ib_2 \in MIN$. Then if $ib_2 \in MIN$, $ib_2 \equiv j'$. By a similar argument to the one above, $h'b_1 + ib_2 \in MIN$ for $0 \leq h' \leq |A| - j'$. Then we have some $\{w'_k\}$ say with $\{w'_k\} = \{c_1b_1 + c_2b_2 | w'_k \in MIN, c_2 \leq i\}$. By a similar argument to $\gamma \in G(M^c)$, $lub\{w'_k\} - A_1 = g_\star \in G(M^c)$. But $(g_{star})_x < (g_{i+1})_x \Rightarrow g_i$ and g_{i+1} are not consecutive. This is a contradiction. Therefor, $(g_i)_x + 1 = (g_{i+1})_x$.

So by the principle of mathematical induction, our claim holds. $\square$

Lemma 8.5. *If there is some $g_i \in G(M^1)$, then there is $g'_i \in G(M^c)$ such that $g'_i = g_i + i\binom{c-1}{0}$.*

Proof: Let $g_i + A_1 = lub\{w\}$ for some $\{w\} \subset MIN^1$. Let $\{w_e\}$ be the set of elements of $\{w\}$ with the greatest x coordinate. We then have that $(lub\{w\})_x = (w_e)_x = i$ by lemma 8.4.

We have from lemma 8.2 that for each $w \in MIN^1$, there is some $w' \in MIN^c$ such that if $w = c_1b_1 + c_2b_2$, then $w' = c_1b_1 + c_2b_2 + c_2\binom{c-1}{0}$. By lemma 8.3 there is some $g'_i \in G(M^c)$ with $g'_i + A_1 = lub\{w'\}$.

$(lub\{w\})_y = (lub\{w'\})_y$ because $c_2\binom{c-1}{0}$ does not change the y coordinate.

If w_e has a maximum x coordinate for $\{w\}$, then w'_e will for $\{w'\}$. $w'_e = w_e + c_2\binom{c-1}{0} = w_e + i\binom{c-1}{0}$ because $c_2 = i$ by lemma 8.4. So $(lub\{w'\})_y = (lub\{w\})_y$ and $(lub\{w'\})_x = (lub\{w\})_x + i(c-1)$. Therefor $g'_i = g_i + i\binom{c-1}{0}$. $\square$.

Theorem 8.6. *Suppose* $M^1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & a & b & d \end{pmatrix}$ *and* $M^c = \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & a & b & d \end{pmatrix}$ *and $G(M^1) = \{g_0, g_1, \ldots, g_k\}$. Then $G(M^c) = \{g_j + j\binom{c-1}{0}\}$ for $0 \leq j \leq k$.*

Proof: By lemma 8.3, for any $g_j \in G(M^1)$ there is some $g'_j \in G(M^c)$ and vice versa. By lemma 8.5 $g'_j = g_j + j\binom{c-1}{0}$. $\square$

9 All b_i Lying on Boundary

Define a "prime" vector as an integer vector whose coordinates have gcd 1. It is evident that we may express any integral vector as a product of an integer scalar and a prime vector

Theorem 9.1. *Let all the prime vectors that define the A-cone as $\alpha_1, \alpha_2, \ldots, \alpha_n$ (ie, all A-vectors can be expressed as $z_{i,j}\alpha_i$, where $z_{i,j}$ is an integer scalar and i, j are integers). If all the generating vectors can be expressed as integer scalar multiples of the α_i, then if there is a frobenius vector, it is unique and equal to $F = \sum_{i=1}^{n} f_j\alpha_j$, where f_i is the frobenius number of all the $z_{i,j}$, where j varies. If, for any α_i f_i does not exist, then no frobenius vector exists.*

Proof. If one of the f_i does not exist, wlog f_1, this means that all the generating vectors with prime vector α_1 may be expressed as $m_j k\alpha_1$, for positive integers m_j, and some positive integer $k \neq 1$. It is evident that any integral vector whose α_1-component is an integer not congruent to 0 mod k is not in the monoid- hence no frobenius vector can exist.

Assume there exists a complete vector, F' which is incomparable or smaller than F. Express F' as $[c_1c_2...c_n] \cdot [\alpha_i\alpha_2 \ldots \alpha_n]$ (the c_i are positive, but not necessarily integers). For at least one i, $c_i < f_i$. Wlog, let $c_1 < f_1$. Consider the vector $[(f_1)(c_2+1)(c_3+1)...(c_n+1)] \cdot [\alpha_i\alpha_2 \ldots \alpha_n]$. This vector is not in the monoid- the term $f_1\alpha_1$ cannot be expressed as a sum of the generating vectors who have α_1 as their prime vector, by the definition of f_1. Thus we have a vector larger than F' that is not in the monoid. We claim that the gcd of the generating vectors is equivalent to $\det[\alpha_1\alpha_2 \ldots \alpha_n]$. Say that p^d is the highest power of some prime p to divide the gcd. Say that p^e is the highest power of p to divide $\det[\alpha_1\alpha_2 \ldots \alpha_n]$. Select vectors where none is a scalar multiple of the other; that is, one multiple each of each α_i. The determinant of any other collection of vectors will have one vector a rational scalar multiple of the other, and that determinant is 0 and may be disregarded in the gcd. It is possible to make a selection such that none of the scalar multiples is a multiple of p. Otherwise, if this is impossible for a certain α_i, wlog say α_1, then all generating vectors that are a multiple of α_1 also have a scalar factor of p, so f_1 does not exist. Hence $d = e$.

If the gcd of the generating vectors is 1 then the determinant of the α_i is 1- meaning that every integral lattice point can also be expressed as an integral lattice point of the α_i-basis. But by the definition of the frobenius number, every vector whose α_i component exceeds f_i for every i is representable in the

monoid. Thus every vector in the α_i lattice larger than F is in the monoid. Since every integral lattice point larger than F corresponds to vector in the α_i lattice larger than F, it follows that F is a complete vector. Since we also know that every vector smaller than or incomparable to F is not complete, it follows that F is the unique Frobenius vector. □

10 Selmer Lattice: Properties and Applications

The Selmer Lattice is a construct invented by Ernst Selmer to solve the 1-dimensional Frobenius problem in 3 generators. In this paper we generalize the tools he uses to the vector case, in an attempt to learn more about the higher-dimensional analogues of the 1-dimensional problem.

10.1 Properties

10.1.1 Definitions

1. We are considering the set of points $xb_1 + yb_2$ where x and y are non-negative integers. We arrange the elements in a cartesian lattice in the first quadrant, where the x-axis represents b_2 and the y-axis represents b_1.

2. We have the relation $x_1b_1 + x_2b_2 \geq_B y_1b_1 + y_2b_2$ if $x_i \geq y_i$ for $i = 1, 2$. We refer to this relation as being "B-greater".

3. The zero vector is the *trivial* zero.

4. A *zero* is a vector that is congruent to the zero vector.

5. An element is *insignificant* if it is $\geq_B$ than a nontrivial zero. An element that is not insignificant is *significant*.

6. We define the *Selmer Lattice* to be the set of significant vectors.

7. The element $1b_1 + 0b_2$ belongs to the residue class 1. The residue class s is the residue class where $0b_1 + 1b_2$ belongs.

8. Given $ib_1 + jb_2$, we define it's *contained set* to be the set of elements in the Selmer diagram that are $\leq_B ib_1 + jb_2$.

9. We call an element of the Selmer diagram *good* when it's contained set contains a complete residue set mod $|A|$.

10. Define the *Minimal Selmer Diagram* to be the diagram including only the elements in MIN.

11. v $\succcurlyeq$ w means that the vectors v and w are congruent and that v is greater or equal than w.

12. v$\preccurlyeq$w means that the vectors v and w are congruent and that v is lesser or equal than w.

13. v$\nparallel$w means that the vectors v and w are congruent and that v is incomparable to w.

14. Let $g \in G$. We know that there exist a complete set of residues $N \in MIN$ such that $lub(N) - A_1 = g$. Now add the constraint that N is contained in the first k rows of the Selmer lattice. Let m be the minimal value of k for which such an N exist. We now define $Low(g) = m$ and say N is a *minimal representation* for g if it is contained in the first $Low(g)$ rows of the Selmer lattice.

10.1.2 Purple Chomps

Theorem 10.1. *$x_1b_1 + y_1b_2 \geq_B x_2b_1 + y_2b_2$ implies $x_1b_1 + y_1b_2 \geq x_2b_1 + y_2b_2$*

Proof. Since $x_1b_1+y_1b_2 \geq_B x_2b_1+y_2b_2$, we have $x_1b_1+y_1b_2$-$x_1b_1+y_1b_2=(n_1, n_2)$ for some nonnegative integers n_1, n_2. Thus $x_1b_1+y_1b_2$-$x_1b_1+y_1b_2=n_1b_1+n_2b_2$. Given that b_1 and b_2 can both be expressed as positive sums of the a-vectors, we know that $x_1b_1 + y_1b_2$-$x_1b_1 + y_1b_2$ can be expressed as positive sums of the a-vectors. Thus $x_1b_1 + y_1b_2 \geq x_2b_1, y_2b_2$

□

Theorem 10.2. *If $(x_1, y_1) \geq_B (x_2, y_2)$ for some (x_2, y_2) in the first quadrant of the Selmer Lattice, then (x_1, y_1) is not significant*

Proof. $(x_1, y_1) \geq_B (x_1, y_1) - (x_2, y_2)$, which is a zero. □

Theorem 10.3. *All points in the MIN set are significant.*

Proof. Given $xb_1 + yb_2$ an insignificant point. There exists a nontrivial zero $z_1b_1 + z_2b_2 \leq_B xb_1 + yb_2$. Thus, $(x - z_1)b_1 + (y - z_2)b_2$ is a point on the first quadrant of the Selmer Lattice. Since $z_1b_1 + z_2b_2 \equiv 0$, $(x - z_1)b_1, (y - z_2)b_2 \equiv xb_1 + yb_2$. Also, since $(x - z_1)b_1 + (y - z_2)b_2 + z_1b_1 + z_2b_2 = xb_1 + yb_2$, $xb_1 + yb_2 \geq_B (x - z_1, y - z_2)$ and by Theorem 10.1 $(x - z_1)b_1 + (y - z_2)b_2 \leq xb_1 + yb_2$. In fact $(x - z_1)b_1 + (y - z_2)b_2 < xb_1 + yb_2$ since $z_1b_1 + z_2b_2$ is a nontrivial zero. Thus $(x - z_1)b_1 + (y - z_2)b_2 \lneqq xb_1 + yb_2$ and so $xb_1 + yb_2$ is not in the MIN set. □

Theorem 10.4. *Order the nontrivial significant zeroes according to increasing b_2-coordinate. The zeroes will then also be ordered according to decreasing b_1-coordinate.*

Proof. We prove this by induction. $(|A|, 0)$ is the first element in this ordering. Consider the Z_k, the kth zero of the ordering. It has a larger b_2 coordinate than the Z_{k-1} zero. If Z_k's b_1-coordinate were greater than or equal to Z_{k-1}'s b_1 coordinate, Z_k would be B-greater than Z_{k-1}, contradicting its significance. □

Note that this proves that each row of the Selmer Lattice of significant elements contains no more elements than the row above it.

10.1.3 Wavy Cuts

Theorem 10.5. *Given two significant zeroes, $z_1b_1 + o_1b_2$ and $z_1b_1 + o_1b_2$ iff $(z_1, o_1) \leq (z_2, o_2)$ and $o_1 < o_2$, all elements of the MIN set have b_2-coordinate less than $o_2 - o_1$. Iff $(z_1, o_1) \leq (z_2, o_2)$ and $o_1 > o_2$ then all elements of MIN have b_1-coordinate less than $z_2 - z_1$.*

Proof. Say $o_1 < o_2$. Given any $xb_1 + yb_2$ with $y \geq o_2 - o_1$, we know that $xb_1 + yb_2 \equiv (z_1b_1 + o_1b_2) - (z_2b_1 + o_2b_2) + (xb_1 + yb_2)$. This is true because $z_1b_1 + o_1b_2$ and $z_1b_1 + o_1b_2$ both belong to residue class 0. $(z_1b_1 + o_1b_2) - (z_2b_1 + o_2b_2) + (xb_1 + yb_2)$ is a point on the first quadrant of the Selmer Lattice because $y \geq o_2 - o_1$, and since $o_2 > o_1$, $z_2 < z_1$ (Theorem 10.4). But since $(z_2b_1 + o_2b_2) - (z_1b_1 + o_1b_2) > 0$, we have $(z_1b_1 + o_1b_2) - (z_2b_1 + o_2b_2) + (xb_1 + yb_2) < (xb_1 + yb_2)$ and so $(z_1b_1 + o_1b_2) - (z_2b_1 + o_2b_2) + (xb_1, yb_2) \lneqq xb_1 + yb_2$. Thus $xb_1 + yb_2$ is not in MIN.

If instead $o_1 > o_2$, then $z_1 < z_2$ (Theorem 10.4). Given any $xb_1 + yb_2$ with $x \geq z_2 - z_1$, we know that $(x, y) \equiv z_1b_1 + o_1b_2 - z_2b_1 + o_2b_2 + xb_1 + yb_2$. This is true because $z_1b_1 + o_1b_2$ and $z_1b_1 + o_1b_2$ both belong to residue class 0. $(z_1b_1 + o_1b_2) - (z_2b_1 + o_2b_2 + xb_1 + yb_2$ is a point on the Selmer Lattice because $x \geq z_2 - z_1$ and $o_1 > o_2$. But since $z_2b_1 + o_2b_2 - (z_1b_1 + o_1b_2 > 0$, we have $(z_1b_1 + o_1b_2) - (z_2b_1 + o_2b_2) + (xb_1 + yb_2) < (xb_1 + yb_2)$ and so $(z_1b_1 + o_1b_2) - (z_2b_1 + o_2b_2) + (xb_1 + yb_2) \lneqq xb_1 + yb_2$. Thus $xb_1 + yb_2$ is not in MIN. □

Theorem 10.6. *Given two congruent significant elements* (x_1, y_1) *and* (x_2, y_2) *where* $x_2 > x_1$ *there exists a zero* (z, o) *where* $z, o \in [0, |A|]$ *and where* $(x_2, y_2) - (x_1, y_1) = (|A|, 0) - (z, o)$

Proof. Since $x_2 > x_1$ we have also $y_2 < y_1$, otherwise (x_2, y_2) cannot be significant, by Theorem 10.2. $(x_1, y_1) - (x_2, y_2) \equiv 0$ we have also $(|A|, 0) + (x_1, y_1) - (x_2, y_2) \equiv 0$. Also, since $x_2 > x_1$ and $y_2 < y_1$ $(|A|, 0) + (x_1, y_1) - (x_2, y_2) \equiv 0$ lies in the first quadrant and has b_1-value less than $|A|$. Thus, we need only set $(z, o) = (|A|, 0) + (x_1, y_1) - (x_2, y_2)$ □

Theorem 10.7. *Let* (z_1, o_1) *be a zero other than* $(|A|, 0)$ *such that* $(z_1, o_1) \lneqq (|A|, 0)$ *and* o_1 *is minimal. Let* (z_2, o_2) *be a zero other than* $(|A|, 0)$ *such that* $(z_2, o_2) \gneqq (|A|, 0)$ *and* $|A| - z_2$ *is minimal. The MIN set is comprised of all significant elements with* b_1*-value less than* $|A| - z_2$ *and* b_2*-value less than* o_1.

Proof. By Theorem 10.5 we know that all elements with b_1-value greater than or equal to $|A| - z_2$ and b_2-value greater than or equal to o_1 cannot be in the MIN set. It remains to show that the significant elements that are left

comprise the MIN set. It suffices to show that any two congruent significant elements in this reduced set are incomparable. Suppose instead there exist a pair of significant elements, $(x_1, y_1), (x_2, y_2)$ in this set that are comparable. Wlog let $x_2 > x_1$. Then also $y_2 < y_1$, otherwise (x_2, y_2) is insignificant by Theorem 10.2. We have both $x_2 - x_1 < |A| - z_2$ and $y_1 - y_2 < o_1$. By Theorem 10.7 there exists (z, o) such that $(|A|, 0) - (z, o) = (x_2, y_2) - (x_1, y_1)$.Since (x_2, y_2), (x_1, y_1) are comparable, it must follow that $(x_2, y_2) - (x_1, y_1)$ equals a sum of A-vectors with either all positive or all negative coefficients. $(|A|, 0) - (z, o)$ must equal that same sum, and so $(|A|, 0), (z, o)$ are comparable. But $|A| - z = x_2 - x_1 < |A| - z_2$ and $o = y_2 - y_1 < o_1$, contradicting the minimality of either $|A| - z_2$ or o_1.
Hence, given any congruence class, we know all its minimal elements must lie in this minimal Selmer Lattice, and we know that all elements of this congruence class in this reduced set are mutually incomparable. Thus they are all minimal. □

We want to find the $(z_1, z_2) \cong (|A|, 0)$ where z_2 is minimum.

Theorem 10.8. *In the Selmer Lattice bounded by b_1 and b_2-values $\in [0, |A|]$, there exists one zero a row because b_1 is a generator. The zeroes are $\{(|A| - (is \mod |A|), i)\}$ where i ranges from 0 to $|A|$.*

Proof. Since $s_b 1 \equiv b_2$, we know that for any zero Z, $Z + (-s, 1)$ is also a zero. Also, for any zero Z, $Z + (|A|, 0)$ is a zero. Since $|A|, 0)$ is a zero, for the $b_2 = i$ row the element $(|A| - is, i)$ is a zero. If $|A| - is$ is negative we can add $(|A|, 0)$ to $(|A| - is, i)$ enough times so the b_1-coordinate lies in $[0, |A|)$. This will imply $(|A| - (is \mod |A|), i)$ is a zero, as we required. □

Theorem 10.9. *There exists two real numbers, μ and ν such that for any two positive integers c and d so*

1. $\frac{c}{d} \leq \nu \leftrightarrow (x, y) < (x, y) + (-c, d)$,
2. $\mu > \frac{c}{d} > \nu \leftrightarrow (x, y)$ *is incomparable to* $(x, y) + (-c, d)$
3. $\frac{c}{d} \geq \mu \leftrightarrow (x, y) > (x, y) + (-c, d)$

for all elements (x, y).

Proof. It suffices to prove this assertion true for $(0,0)$. This is because $(0,0)-(-c,d) = (x,y) - ((x,y)-(-c,d))$ for all x, y and thus the relation between $(0,0)$ and $(-c,d)$ would be the same as the relation between (x,y) and $(x,y)-(-c,d)$.
Define μ as the smallest real number so $b_2 < \mu \cdot b_1$. Define ν as the largest real number so $b_2 > \nu \cdot b_1$. If $\frac{c}{d} \leq \nu$ then

$$-cb_1 + db_2 = d(-\frac{c}{d}b_1 + b_2) \geq d(-\nu b_1 + b_2) > c(-b_2 + b_2) = 0$$

If $(-c,d) > (0,0)$ then $-cb_1 + db_2 > 0$ and $b_2 > \frac{c}{d}b_1$. Since ν is the largest number that $b_2 > \nu b_1$, we must have $\frac{c}{d} \leq \nu$. Thus $\frac{c}{d} \leq \nu \leftrightarrow (-c,d) > 0$.
If $\frac{c}{d} \geq \mu$ then

$$-cb_1 + db_2 = d(-\frac{c}{d}b_1 + b_2) \leq d(-\mu b_1 + b_2) < c(-b_2 + b_2) = 0$$

If $(-c,d) < (0,0)$ then $-cb_1 + db_2 < 0$ and $b_2 < \frac{c}{d}b_1$. Since μ is the smallest number that $b_2 < \mu b_1$, we must have $\frac{c}{d} \geq \mu$. Thus $\frac{c}{d} \geq \mu \leftrightarrow (-c,d) < 0$.
$(-c,d) = 0$ is impossible, otherwise $db_2 = cb_1$ and so b_2 is a scalar multiple of b_1, a case we are not considering. Hence if $(-c,d) \not< 0$ and $(-c,d) \not> 0$ then $(-c,d)$ must be incomparable to 0. By elimination we have $\mu > \frac{c}{d} > \nu \leftrightarrow (x,y)$ is incomparable to $(x,y) + (-c,d)$ □

If we want to find the "height" of the MIN set then we must identify the zero in $\{(|A| - (is \mod |A|), i)\}$ so that $\frac{(is \mod |A|)}{i} \leq \nu$ and i is minimal. The zero that i refers to will be the zero larger than $(|A|, 0)$ with the minimal b_2-coordinate.

We use a continued fraction algorithm to determine the proper i. Set s_{-1} as $|A|$ and s_0 as s and we have

$$\begin{aligned} s_{-1} &= q_1 s_0 - s_1 \quad && 0 \leq s_1 < s_0 \\ s_0 &= q_2 s_1 - s_2 \quad && 0 \leq s_2 < s_1 \\ s_1 &= q_3 s_2 - s_3 \quad && 0 \leq s_3 < s_2 \\ &\cdots \\ s_{k-2} &= q_k s_{k-1} \quad && 0 \leq s_k < s_{k-1} \\ s_{k-1} &= q_{k+1} s_k \quad && 0 = s_{k+1} < s_k \end{aligned} \tag{1}$$

If $s_0 = 0$ we set $m = -1$. We also define integers P_i by $P_{-1} = 0$, $P_0 = 1$ and $P_{i+1} = q_{i+1}P_i - P_{i-1}, i = 0, 1, 2, \ldots k$.

Since $q_i \geq 2$ it follows by induction that $P_i + 1 > P_i$. Also $s_i > s_i + 1$. Hence

$$0 = \frac{s_{k+1}}{P_{k+1}} < \frac{s_k}{P_k} < \ldots < \frac{s_0}{P_0} < \frac{s_{-1}}{P_{-1}} = \infty \tag{2}$$

There are unique integers λ and ξ such that $\frac{s_{\lambda+1}}{P_{\lambda+1}} < \mu \leq \frac{s_\lambda}{P_\lambda}$ and $\frac{s_\xi}{P_\xi} \leq \nu < \frac{s_{\xi-1}}{P_{\xi-1}}$.

Theorem 10.10. *$P_{i+1}s_0 \equiv s_{i+1} \mod |A|$ for all $i \in [0...|A| - 1]$*

Proof. We induct on i. We have $P_1 = q_1P_0 - P_{-1} = q_1$. Thus $P_1s_0 = q_1s_0 = |A| + s_1 \equiv s_1 \mod |A|$. Also, similarly

$$P_2s_0 = (q_2P_1 - P_0)s_0 = (q_2q_1 - 1)s_0 = q_2(|A| + s_1) - s_0 \equiv q_2s_1 - s_0 = s_2$$

Assume this proposition holds up to i. $P_{i+1}s_0 = (q_{i+1}P_i - P_{i-1})s_0 \equiv q_{i+1}s_i - s_{i-1} = s_{i+1}$ by the induction hypotheses and (1). □

Theorem 10.11. *Among the integers $s_0, 2s_0, \ldots, (P_i - 1)s_0$ taken modulo $|A|$, the smallest among these is $P_{i-1}s_0 \mod |A|$.*

Proof. Using the fact that $P_{i-1}s_0 = s_i < s_j = P_js_0$ for $i < j$, by Theorem 10.10,we prove this proposition by induction. This assertion is trivially true for $i = 1$. $P_0 = 1$, and so $s_0, 2s_0, \ldots (P_1 - 1)s_0$ are all less than $|A| = q_1s_0 - s_1 = P_1s_0 - s_1$. Thus s_0 is the smallest among these $\mod |A|$. Let us assume the assertion is true for some $i = k - 1$. For the equation $js_0 \mod |A|$, if $j < P_k - 1$ then using the induction hypothesis

$$P_{k-1}s_0 \mod |A| < P_{k-2}s_0 \mod |A| \leq js_0 \mod |A| \tag{3}$$

If $j > P_{k-1}$ then we may express j as $qP_{k-1} - r$ for positive integers $2 \leq q$ and $0 \leq r < P_{k-1}$. We claim that $j = P_k$, so $js_0 = P_ks_0 = (q_kP_{k-1} - P_{k-2})s_0$ is the smallest value of js_0 so $js_0 < P_{k-1}s_0$, taken $\mod |A|$. Assume that there is a smaller $j = j'$ that fulfills $js_0 < P_{k-1}s_0$ taken $\mod |A|$. Say first that $j' = q_kP_{k-1} - r$, where $r > P_{k-2}$. If $q_kP_{k-1}s_0 - rs_0 < P_{k-1}s_0 \mod |A|$, because we have $q_kP_{k-1}s_0 - P_{k-2}s_0 < P_{k-1}s_0 \mod |A|$ as well then

we must have $rs_0 - P_{k-2}s_0 < P_{k-1}s_0$ in $\mod |A|$; recall that $rs_0 > P_{k-2}s_0$ in $\mod |A|$ by the induction hypothesis. But $rs_0 - P_{k-2}s_0 = (r - P_{k-2})s_0$, and $(r - P_{k-2})$ is less than P_{k-1}. But we know that if n is any integer less than P_{k-1}, $P_{k-1}s_0 < ns_0 \mod |A|$ using (3).
Consider instead $j' = qP_{k-1} - r$ where $q = q_k - t$, where t is a positive integer. If $r = P_{k-2}$, we can see that $j's_0 \equiv P_k s_0 - tP_{k-2}s_0$. Note that $tP_{k-1}s_0$ must lie between $P_{k-1}s_0$ and $|A|$. This is because

$$tP_{k-1}s_0 \equiv ts_{k-1} \leq (q_k - 1)s_{k-1} = s_k + s_{k-2} - s_{k-1} < s_{k-2} \leq |A|.$$

Thus, $j's_0 \equiv P_k s_0 - tP_{k-1}s_0 \mod |A| > P_k s_0 \mod |A|$ (recall that $P_{k-1}s_0 > P_k s_0 \mod |A|$). If $r \neq P_{k-2}$ then necessarily $P_{k-2}s_0 < rs_0 < |A|$. Thus $j's_0 = qP_{k-1}s_0 - rs_0$ lies between $qP_{k-1}s_0 - P_{k-2}s_0 \mod |A|$, and $qP_{k-1}s_0 \mod |A|$ (both greater than $P_k s_0 \mod |A|$). Thus $j's_0 \mod |A|$ cannot be less than $P_k s_0 \mod |A|$. Hence the smallest possible j where js_0 is less than P_{k-1} is P_k □

Theorem 10.12. *The MIN set is the set of significant elements with b_1-value less than s_λ and b_2-value less than P_ξ.*

Proof. We use Theorem 10.7 and look for the zero (z, w) where $(|A|, 0) \preccurlyeq (z, w)$ and w is minimum. By Theorem 10.9 we must have $\frac{|A|-z}{w} \leq \nu$ so we are looking for the zero with the smallest w that fulfills this condition. We claim that this zero has $w = P_\xi$.
By Theorem 10.8 $\frac{|A|-z}{w} \leq \nu$ is equivalent to $\frac{(ws \mod |A|)}{w} \leq \nu$. We know that $P_w s_0 \equiv s_w$ by Theorem 10.12. Thus $\frac{(ws \mod |A|)}{w} \leq \nu$ is equivalent to $\frac{s_w}{P_w} \leq \nu$ (remembering that $s_0 = s$) , which is true for $w = P_\xi$.
Furthermore, no w less than P_ξ will fulfill this condition. It is evident that no P_i with $i < \xi$ fulfills this condition, otherwise we have $\frac{s_i}{P_i} \leq \nu$, contradicting $\nu < \frac{s_{\xi-1}}{P_{\xi-1}}$. Also, no w between some P_{i+1} and P_i can fulfill this condition. For this, it suffices to show that $P_i s_0 \mod |A|$ is the minimum value of $js_0 \mod |A|$ for $j = 1, 2 \ldots P_{i+1} - 1$. This is proven in Theorem 10.11. Hence if a value w lies between some $P_i - 1$ and P_i with $i < \xi$ we have $ws > P_i s \mod |A|$ and so $\frac{(ws \mod |A|)}{w} > \frac{(P_i s \mod |A|)}{P_i} > \nu$. Thus P_ξ is the smallest value of w where the zero on the row $b_2 = w$ is larger than $(|A|, 0)$. An analogous argument will show that s_λ will be the smallest element z where zero in column $|A| - z$ is smaller than $(|A|, 0)$. □

Theorem 10.13. *The important zeroes are* $(s_{i-1} - ks_i, kP_i - P_{i-1})$ *for* i *ranging from -1 to and* k *ranging from 1 to* q_i*.*

Proof. We know that the first q_1 rows have significant zeroes.$(|A|, 0)$ is obviously an important zero, and since this list of the first q_1 zeroes has decreasing b_1-value and increasing b_2-value, all of them are important. Say, for some i that the list of all important zeroes before the row $P_i - P_{i-1}$ is given as in the proposition. We wish to show that the sequence of important zeroes between row $P_i - P_{i-1}$ and row $P_{i+1} - P_i$ is $(s_{i-1} - ks_i, kP_i - P_{i-1})$, where k ranges from 1 to □

10.1.4 Other Important Properties

Theorem 10.14. *If row* i *has fewer elements than row* $i-1$ *for* $1 \leq i \leq |A|$*, then the last element of row* i *is* $|A| - 1$*.*

Proof. Given a row i that has fewer elements than row $i-1$, let row i contain p elements and let row $i-1$ contain $p+q$, where $p, q \in \mathbf{N}$. Since $i\mathbf{b_1}+(p+1)\mathbf{b_2}$ is not in the Selmer diagram, there must be an element within the first $p+1$ rows and i columns of the Selmer diagram that has the same congruence class as it. Also, since $i\mathbf{b_1} + p\mathbf{b_2}$ is in the Selmer diagram, there is no other element within the first p rows and i columns that is congruent to it.

This means that the element congruent to the $i\mathbf{b_1} + (p+1)\mathbf{b_2}$ within the first $p+1$ rows and i columns of the Selmer diagram must be in the first column - otherwise, the element in the same row and one column before it is congruent to $i\mathbf{b_1} + p\mathbf{b_2}$. Furthermore, the element congruent to $i\mathbf{b_1} + (p+1)\mathbf{b_2}$ must be in the first row, otherwise $(i-1)\mathbf{b_1} + (p+1)\mathbf{b_2}$ is congruent to something else within the first $i-1$ rows and $p+1$ columns, which contradicts our assumption. Thus, $i\mathbf{b_1} + (p+1)\mathbf{b_2} \equiv 0 \bmod |A|$, and so $i\mathbf{b_1} + p\mathbf{b_2} \equiv p - 1 \bmod |A|$.

Analogously, if column i contains fewer elements than column $i-1$, then the last element of column $i \equiv p - s \bmod |A|$. □

Theorem 10.15. *If there is a Frobenius vector* $\mathbf{g}$ *such that* $\mathbf{g} + \mathbf{A_1} \geq$ *some good element* $\mathbf{v}$*, then* $\mathbf{g} + \mathbf{A_1} = \mathbf{v}$*.*

Proof. Recall that $\exists \omega_1, ..., \omega_{|A|} \in MIN$, a complete set of residue classes, such that $\mathbf{g} + \mathbf{A_1} = \text{lub}(\omega_1, ..., \omega_{|A|})$. But since $\mathbf{v}$ is $\geq$ a complete set of residue classes, we can choose these elements to take the lub of, which will yield $\mathbf{v}$. Thus $\mathbf{v} - \mathbf{A_1}$ is a complete vector, so $\mathbf{g} + \mathbf{A_1}$ cannot be greater than $\mathbf{v}$.

As a consequence of this theorem, for any good vector $\mathbf{v}$, if $\mathbf{v} - \mathbf{A_1}$ is not a Frobenius vector, then $\nexists$ vectors $\omega_1, ..., \omega_{|A|-1} \in MIN$ such that $lub(\omega_1, ..., \omega_{|A|-1}, \mathbf{v}) - \mathbf{A_1}$ is a Frobenius vector. It is also easy to see that if some good element is in $\square$

Theorem 10.16. *if row i contains more elements than row $i+1$ (for $1 \leq i \leq |A| - 1$), then the last element of row i is good.*

Proof. Assume that row $i+1$ contains p elements, and that row i contains $p+q$ elements, where $p, q \in \mathbf{N}$. To show that $(i, p+q)$ is good, it is easy to see that it suffices to show that every number of the form $(i+1)\mathbf{b_1} + k\mathbf{b_2}$ for $1 \leq k \leq p+q$ is congruent to some element in the contained set of $(i, p+q)$.

By property 1, we know that $(i+1)\mathbf{b_1} + (p+1)\mathbf{b_2} \equiv 0 \mod |A|$, and so all elements of the form $(i+1)\mathbf{b_1} + (p+j)\mathbf{b_2} \equiv j - 1$ for $1 \leq j \leq q$. It is clear that each of these elements is congruent to something in the contained set of $(i, p+q)$ (in fact, they correspond to the first q elements of the first row).

Also by property 1, we have that the element $(i+1, p) \equiv |A| - 1$, from which it follows that the elements $(i+1, 1), (i+1, 2), ...(i+1, p) \equiv |A| - p + 1, |A| - p + 2, ...|A| - 1$. But by property 1, we know that the first row that contains exactly $p+q$ elements ends with $|A|$, and so this row must contain elements of the congruence classes $(i+1, 1), (i+1, 2), ...(i+1, p)$. Since this row is clearly in the contained set of $(i, p+q)$, we obtain the desired result.

Analogously, if column i contains more elements than row $i+1$ (for $1 \leq i \leq |A| - 1$), then the last element of column i is good. $\square$

Theorem 10.17. *For the case where there are two B-vectors b_1, b_2, we label them so b_1 is not greater than b_2. If $gcd(A|b_1)$ is 1 (as we are assuming), there exists an integer $0 \leq s < |A|$ so $s \cdot b_1 \equiv b_2 \mod A$*

Proof. The gcd of the matrix $(A|b_1)$ is 1. Thus for every congruence class of A, there will be an integer n which is at most $|A|$ where $n \cdot b_1$ is in that congruence class. Thus there must exist $s < |A|$ so $s \cdot b_1 \equiv b_2 \mod A$

□

10.2 Applications

10.2.1 Solving the $m = 2$ Case

In this section we attempt to generalize the partial solutions to the 3 generator Frobenius problem found in the papers "On the Linear Diophantine Problem of Frobenius" (1977) and "'On the Linear Diophantine Problem of Frobenius in Three Variables"(1978). we are looking at the cases governed by the conditions $(q+1)a_2 \geq (s-r)a_1$ and $(qm+1)a_2 \geq pa_1$ in the notation of those two papers. Generalizing the first case to more than one dimension is fairly straightforward; generalizing the second is a bit more complicated. In all the following we will be assuming $sb_1 \gtrless b_2$; the case where $sb_1 \# b_2$ has been completely solved, and we can choose to number b_1, b_2 so $sb_1 \lneqq b_2$ is impossible. By an earlier result, we can, and do assume that both b_1 and b_2 are generators.

Theorem 10.18. *For the case where there are two B-vectors b_1, b_2, we label them so b_1 is not greater than b_2. If gcd$(A|b_1)$ is 1 (as we are assuming), there exists an integer $0 \leq s < |A|$ so $s \cdot b_1 \equiv b_2 \mod A$*

The gcd of the matrix $(A|b_1)$ is 1. Thus for every congruence class of A, there will be an integer n which is at most $|A|$ where $n \cdot b_1$ is in that congruence class. Thus there must exist $s < |A|$ so $s \cdot b_1 \equiv b_2 \mod A$
$sb_1 \geq b_2$

Theorem 10.19. *Given four vectors where the gcd of $(A|b_1)$ is 1 and the integer s is defined as in Theorem 10.17. We define q,r such that $|A| = qs+r$, where $0 < r \leq s$. If $s \cdot b_1 \geq b_2$ and $(q+1)b_2 \geq (s-r)b_1$ then $|MIN| = |A|$ and there exists only one Frobenius vector, lub$((r-1)b_1+qb_2, (s-1)b_1+(q-1)b_2)$-A.*

We use the Selmer Lattice. As shorthand for x·b_1+y·b_2, we write (x,y). We mark the MIN set on the Selmer Lattice. Given the conditions set out in the statement of the theorem, we claim that all the elements of the MIN set are in the following table:

0	b_1	$2b_1$	$\dots$	$(s-1)b_1$
b_2	b_1+b_2	$2b_1+b_2$	$\dots$	$(s-1)b_1+b_2$
$2b_2$	b_1+2b_2	$2b_1+2b_2$	$\dots$	$(s-1)b_1+2b_2$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$(q-1)b_2$	$b_1+(q-1)b_2$	$\dots$	$\dots$	$(s-1)b_1+(q-1)b_2$
qb_2	b_1+qb_2	$\dots$	$(r-1)b_1+qb_2$	

Consider any point (x, y). This point represents $xb_1 + yb_2$. If $x \geq s$ then $xb_1+yb_2 \gtrdot (x-s)b_1+(y+1)b_2$. Thus any point with an x-value greater than s-1 cannot be minimal in its residue class. Also, there are no elements of MIN obtained by extending the last line to the right. Since the diagram contains representatives of $qs + r = |A|$ obtained from each other by addition of b_1, $rb_1+qb_2 \equiv (qs+r)b_1 \equiv 0 \mod A$, so we have $rb_1+qb_2 \gtrdot 0$. Thus extending the last line to the right will get us s-r elements congruent to and larger than the first s-r elements in the first row. Thus, $(q+1)b_2 \equiv sb_1+(qb_2 \equiv (s-r)b_1$. This means there will also be no elements of MIN with y-coordinate larger than q. By $(q+1)b_2 \gtrdot (s-r)b_1$, we know that any point (x, y) with $y > q$ will not be minimal since $xb_1 + yb_2 \gtrdot (x + s - r)b_1 + (y - q - 1)b_2$. We know that every residue class is represented in this diagram since the points, read from left to right and then from top to bottom ,are congruent to 0, $b_1, 2b_1, \dots (|A|-1)b_1$, due to the fact that $s \cdot b_1 \equiv b_2 \mod A$. Thus these the entire MIN set is expressed by this diagram. All the points in the diagram are smaller than (r-1,q) or (s-1,q-1). This is because we may obtain one of these two points from any point in the diagram by adding some b_1 and b_2 vectors. The Frobenius vector is thus lub$((r-1)b_1 + qb_2, (s-1)b_1 + (q-1)b_2)$-A.

Corollary: When $s \cdot b_1 \geq b_2$ and s divides $|A|$, the unique Frobenius vector is $(s-1)b_1 + (q-1)b_2 - A$.

If s s divides $|A|$ then we just set $r = s$ in Theorem 10.19. This yields us the answer lub$((s-1)b_1+qb_2, (s-1)b_1+qb_2)$-A. Since $(s-1)b_1+(q-1)b_2)$-A $\geq (s-1)b_1 + (q-1)b_2)$-A the frobenius vector is $(s-1)b_1 + (q-1)b_2$-A.

Theorem 10.20. *Given four pairwise relatively prime vectors and the integer s defined in Theorem 10.17. We define q,r,m,p such that* $|A| = qs + r$ *and* $s = mr + p$. *If* $s \cdot b_1 \geq b_2$ *and* $(qm + 1)b_2 \leq pb_1$, *the set* $\{lub((s-1-(i-1)r)b_1 + (q-1)b_2, (r-1)b_1 + iqb_2) - A\}$ *where i varies from 1 to m+1*

only contains complete vectors. Furthermore, all of the Frobenius vectors are contained within this set.

Define S to be the set of points where $x \in [0, r-1]$and $y \in [0, q-1]$. We define for natural number i the sets A_i as $S + (p + mr - ir, 0)$ and B_i as $S + (0, 1 + qi)$. Furthermore, define

$$\alpha_i = (s - 1 - (i-1)r)b_1 + (q-1)b_2$$

$$\beta_i = (r-1)b_1 + (i+1)qb_2$$

Note that $\alpha_i \in A_i$ and $\beta_i \in B_i$. The congruence $\alpha_i \equiv \beta_i$ is a consequence of $s \cdot b_1 \equiv b_2 \mod A$ and $|A| = qs + r$. This is because $\alpha_i - \beta_i = b_1(s - ir) - b_2(iq + 1) \equiv -b_1 ir - b_2 iq \equiv -i(qs + r)b_1 \equiv 0$ Also, we note that α_i and β_i are the members of A_i and B_i respectively where the x and y values are maximum. Thus, any point in A_i may be expressed as $\alpha_i - (X, Y)$ for some X, Y where X is in $[0, r-1]$ and Y is in $[0, q-1]$. $\beta_i - (X, Y)$ is a point in B_i that is congruent to it. We can see that corresponding elements of A_i and B_i are congruent.

(r, q) is congruent to 0 since $rb_1 + qb_2 \equiv (qs + r)b_1$. We have $s = rm + p$, $p = s - rm$ and so $pb_1 \equiv (s - rm)b_1 \equiv b_2 - rmb_1 \equiv (qm + 1)b_2$ (since $-rb_1 \equiv qb_2$). Thus $(qm + 1)b_2 \gtrdot pb_1$
Any point (x, y) in the lattice with $x \geq q$ and $y \geq r$ cannot be minimal by Theorem 10.3. Since we have the condition $(qm + 1)b_2 \gtrdot pb_1$, $(r, q) \lessdot (r + qm + 1, q - p)$ and by Theorem 10.5 any point (x, y) with $y \geq qm+1$ cannot be in MIN. Thus we need only consider B_i up to $i = m-1$.

Furthermore, given A_i, A_j where $1 \leq i < j \leq m$ no element in A_i is congruent to an element in A_j. This is because all the elements of A_i and A_j lie within the bounds $y < q$, $x < s$ which is a subset of the set of points referenced in Theorem 10.19. The set of points in Theorem 10.19 all belonged to different congruence classes, thus the set of points in A_i and A_j all belong in different congruence classes as well. Also, within any A_i or A_j distinct points belong to distinct congruence classes. Hence the points in the sets A_1, $A_2 \ldots A_m$ all belong to distinct congruence classes. Since the points in A_i are congruent

to the points in B_i, it is also true that the points in B_1, $B_2 \ldots B_m$ all belong to distinct congruence classes

We know all qs+r congruence classes are represented in the set of points that we have not ruled out. If we include the condition $y < q + 1$, the set of points remaining is equivalent to the set represented in Theorem 10.19 which contains members of all qs+r congruence classes. Since we have ruled out the points that satisfy both $x \geq q$ and $y \geq r$, and the points where $y \geq qm + 1$, the only points excluded by the condition $y < q + 1$ will be elements of the B_i where $i > 0$. Thus every residue class represented by an element in the B_i where $i \in [1, m-1]$ has exactly two representatives in the set of points that we have not ruled out. This leaves us with the residues that are not in the A_i or B_i. If we exclude the B_i where $0 < i < m$ we get the set of points defined in Theorem 10.19. In the Theorem 10.19 setup each residue is represented once. Thus residues not represented in the A_i and B_i are represented once each in the set of points that we have not excluded.

Also, we should note that all these points are less than α_i for $i \in [1, m]$ and β_i for $i \in [0, m-1]$. This is because all these points are not in the A_i or B_i and are not in the set $\{(x, y) | x \geq q, y \geq r\}$, and so these points all have x-values less than q and y-values less than p.
We consider all minimal residue systems, that is sets of $|A|$ elements, each representing a different residue class and each minimal in its residue class. We put the minimal residue systems into m subcollections, which we label the 1^{st}, 2^{nd} 3^{rd}... mth subcollection. A minimal residue system is in the i^{th} subcollection when the β_{i-1} is an element of that minimal residue system and for any integer n larger than i-1, β_n is not an element of that minimal residue system. Note that a minimal residue system cannot contain both α_j and β_j for any j, since those two elements are congruent. Consider all the least upper bounds of the minimal residue system in the ith subcollection. We claim that there is a minimum least upper bound, and that is lub(α_i, β_{i-1}). This value is achieved in the residue system that contains no element of $A_1, A_2, \ldots, A_{i-1}$ but contains every element of $A_i, A_{i+1}, A_{i+2}, \ldots, A_m$. Every minimal residue system in this class contains the points β_{i-1}, and α_i since they do not contain β_i. Thus the minimum possible lub is at least lub(α_i, β_{i-1}). This is sufficient to show that the minimum possible lub *is* lub(α_i, β_{i-1}) for this subcollection.

If we work in two dimensions, we can do a little better. By a theorem proved last summer, the lub of any minimal system is equal to $v + A$, where v is a complete vector. Thus lub(α_i, β_{i-1})-A is a complete vector for all $i \in \{0, 1, ..., m-1\}$. Thus the Frobenius vectors are the minimal vectors in this collection.

Theorem 10.21. *Given the conditions in Theorem 10.20, and if there are two A-vectors, a_1 and a_2, the Frobenius Vectors are $\{lub((s-1-(i-1)r)b_1 + (q-1)b_2, (r-1)b_1 + iqb_2) - A\}$, where i ranges from δ_χ to δ_γ inclusive, where the δ_j are the value of i where $lub((s-1-(i-1)r)b_1+(q-1)b_2, (r-1)b_1+iqb_2)$ when expressed as $x'_1a_1 + x'_2a_2 \ldots + x'_n$, has the minimum x'_j-value. δ_χ and δ_γ are the largest and smallest δ_js respectively.*

Express b_1 as $\sum_{i=1}^n \kappa_i a_i$ and ϕ_2 as $\sum_{i=1}^n q_i a_i$, where the p_i and q_i are positive reals. Translate all the points α_i and β_i by $\alpha'_i = \alpha_i - (r-1)b_1 - (q-1)b_2$ and $\beta'_i = \beta_i - (r-1)b_1 - (q-1)b_2$. Since we're translating the points the same way, the ordering of the lubs remains the same, and in particular the minimal lubs remain the same. Express all the lubs in the form $\sum_{i=1}^n x'_i a_i$. The a_j-value of lub$(\alpha'_{i+1}, \beta'_i)$, that is, δ_j is equal to $\max((s-r)\kappa_j - ir\kappa_j, \phi_j + iq\phi_j)$. As i increases from 0 to m, this value is either monotonically increasing, monotonically decreasing, or monotonically decreasing and then monotonically increasing. Label the a_i such that the $delta_i$ are monotonically increasing. Thus, every lub$(\alpha'_{i+1}, \beta'_i)$ for $i < \delta_1$ has all the $a_1, a_2, \ldots a_n$ coordinate-values greater than lub$(\alpha'_{\delta_1+1}, \beta'_{\delta_1})$ and every lub $(\alpha'_i + 1, \beta'_i)$ for $i > \delta_n$ has all the coordinate values greater than lub$(\alpha'_{\delta_n+1}, \beta'_{\delta_n})$. Given any k, j where $\delta_1 \leq k < j \leq \delta_\gamma$, lub$(\alpha'_{k+1}, \beta'_k)$ has a smaller x'- value and a greater y'-value compared to lub$(\alpha'_{j+1}, \beta'_j)$. Thus any two elements from the set $\{$ lub $(\alpha'_{i+1}, \beta'_i)\}$ as i ranges from δ_χ to δ_γ, are incomparable. Hence any two elements from the set $\{\text{lub}(\alpha_{i+1}, \beta_i)\}$ as i ranges from δ_χ to δ_γ are incomparable. Thus the set $\{\text{lub}(\alpha_{i+1}, \beta_i) - A\}$)as i ranges from δ_χ to δ_γ is the set of Frobenius vectors.

The values δ_χ and δ_γ can be determined easily. We have to first solve the equation $(s-r)m_1 - irm_1 = n_1 + iqn_1$. δ_χ equals either $\lfloor i \rfloor$ or $\lceil i \rceil$. Solving the equation $(s-r)m_2 - jrm_2 = n_2 + jqn_2$ will similarly get us two candidates for δ_γ, $\lfloor j \rfloor$ or $\lceil j \rceil$.

Soli Deo Gloria

$sb_1 \# b_2$

This subsection contains some facts and insights about the Frobenius problem in the case where $m = n = 2$ and $s\mathbf{b_1}$ is incomparable to $\mathbf{b_2}$. Throughout the article, we will assume WLOG that $P_1(s\mathbf{b_1}) < P_1(\mathbf{b_2})$, and $P_2(s\mathbf{b_1}) > P_2(\mathbf{b_2})$.

Preliminary Facts: Recall that for $1 \leq i \leq \lfloor |A|/s \rfloor + 1$, we know that the i^{th} row of the Selmer lattice is: $(i*s, i*s+1, i*s+2, ..., |A|-1)$. In addition, since $s\mathbf{b_1}$ is incomparable to $\mathbf{b_2}$, we know that these first $\lfloor |A|/s \rfloor + 1$ rows are in MIN. This is because the zeroes $\{|A| - i, i|$ where i ranges from 0 to $\lfloor |A|/s \rfloor$ are all mutually incomparable, and also using Theorem 10.5

Some notation: Let l_i denote the last element in the i^{th} row of the Selmer diagram. Let S_i denote the set of all elements in row i or above.

Theorem 10.22. *For any i such that the i^{th} row of the Minimal Selmer Diagram is non-empty, $\forall \mathbf{v} \in S_i$, $P_1(l_i) \geq P_1(\mathbf{v})$.*

Proof. We induct on i. The base case when $i = 1$ is clearly true. Assume the claim is true for $i = k$, and we will prove it for $i = k + 1$. It suffices to show that $P_1(l_{k+1}) \geq P_1(l_k)$. Here we split the proof into two cases.

Case 1: For $1 \leq k \leq \lfloor |A|/s \rfloor$, we have that $l_{k+1} - l_k = \mathbf{b_1} - s\mathbf{b_2}$, and so $P_1(l_{k+1} - l_k) = P_1(\mathbf{b_1} - s\mathbf{b_2}) \geq 0$ by our assumption that $P_1(s\mathbf{b_1}) > P_1(\mathbf{b_2})$.

Case 2: For $k > \lfloor |A|/s \rfloor$: Recall that row $\lfloor |A|/s \rfloor + 1$ of the Selmer diagram has $|A| - \lfloor |A|/s \rfloor * s < s$ rows, so row $\lfloor |A|/s \rfloor + 1$ contains fewer than s elements. By (reference Darren's paper), we know that row k has $\leq s$ elements. This means that $l_{k+1} - l_k = \mathbf{b_1} - m\mathbf{b_2}$, where $m < s$. So, $P_1(l_{k+1} - l_k) = P_1(\mathbf{b_1} - m\mathbf{b_2}) \geq P_1(\mathbf{b_1} - m\mathbf{b_2}) \geq 0$. This completes the induction. □

Theorem 10.23. *For any i such that the $i^t h$ row of the Minimal Selmer Diagram is non-empty, there is a unique smallest vector $= lub(\omega_1, ..., \omega_{|A|})$, where $\omega_1 = l_i$ and the set of ω's are all in the first i rows of the Minimal Selmer Diagram.*

Proof. By Property 1, we have that $P_1(lub(\omega_1, ..., \omega_{|A|}) = P_1(l_i)$. In addition, there must be a unique minimal value for $lub(\omega_1, ..., \omega_{|A|})$. This implies the desired result. □

Theorem 10.24. *For any Frobenius vector* $\mathbf{g}$*, let* $lub(\omega_1, ..., \omega_{|A|}) - \mathbf{A_1}$ *be a minimal representation of* $\mathbf{g}$*, where* ω_i *is defined as usual, and let Low*($\mathbf{g}$) $= k$*. Then* $l_k = \omega_i$ *for some* i*.*

Assume the contrary. Let $S = \{\omega_i\}$. Let m_k be the last element of row k. WLOG, let ω_1 be the element in S that is congruent to l_k. We know that ω_1 is in a smaller row than l_k, and so it must be in a bigger column since ω_1 and l_k are incomparable. Thus, every element in row k is congruent to some element in the same row as ω_1 and in a smaller column than ω_1.

But this allows us to represent $\mathbf{g}$ using only the first $k-1$ rows: For every ω_i in the k^{th} row, $\exists$ an element $\omega_i^{'}$ in the same row as ω_1, where $\omega_i^{'} < \omega_1$. We form $S^{'}$ in the following way: for each element $\omega_i \in S$, if ω_i is not in the k^{th} row, then $\omega_i \in S^i$; if ω_i is in the k^{th} row, then $\omega_i^{'} \in S^i$. Notice that $lubS^{'} \leq lubS$. This cannot be a strict inequality, since $\mathbf{g}$ is assumed to be a Frobenius vector. So, we have that $lubS^{'} = lubS$, but this contradicts the fact that S is a minimal representation of $\mathbf{v}$.

Consequences of the above three properties: For a given k, let $m_{k,j}$ denote the minimal $P_2(\omega j)$, where $\omega j \equiv j$, and lies within the first k rows of the Minimal Selmer Diagram.

Each Frobenius vector can be represented in the following manner: $P_1(l_i)\mathbf{a_1} + \min\{m_{i,j}\}\mathbf{a_2}$, where j through all congruence classes mod $|A|$ except for the congruence class of l_i.

Comment: Note that this also proves that the number of Frobenius vectors $\leq$ the number of rows in the Minimal Selmer diagram, which is $\leq |A|$.

Theorem 10.25. *Let* $|A| = qs + r$*. Suppose that* $s\mathbf{b_1} \not\equiv \mathbf{b_2}$ *and that* $(q+1)\mathbf{b_2} \geq (s-r)\mathbf{b_1}$*. Then the Frobenius set is exactly:* $\{(|A|-1, 0)_b - A_1, (|A|-s-1, 1)_b - A_1, ..., (|A| - s(\lfloor |A|/s \rfloor - 1) - 1, \lfloor |A|/s \rfloor - 1)_b - A_1, lub((|A| - s(\lfloor |A|/s \rfloor) - 1, \lfloor |A|/s \rfloor)_b, (|A| - s(\lfloor |A|/s \rfloor - 1) - r - 1, \lfloor |A|/s \rfloor - 1)_b - A_1)\}$.

By the wavy cut theorem, we know that in this case the Minimal Selmer Lattice is exactly:

0	1			...	$\|A\| - 1$
s	$s+1$		...	$\|A\| - 1$	
$2s$	$2s+1$	...	$\|A\| - 1$		
.					
.					
.					
$\|A\| - r - s$		...	$\|A\| - 1$		
$\|A\| - r$	...	$\|A\| - 1$			

We know that the elements congruent to $|A|-1$ in all but the last row are good, which implies $(|A|-1,0)_b, (|A|-s-1,1)_b, ..., (|A|-s(\lfloor |A|/s \rfloor - 1)-1, \lfloor |A|/s \rfloor - 1)_b$ are all Frobenius vectors. The only remaining element congruent to $|A|-1$ is $(|A|-s(\lfloor |A|/s \rfloor)-1, \lfloor |A|/s \rfloor)_b$. Now, we assume WLOG that $P_1(s\mathbf{b_1} \text{ ¡ } P_1(b_2)$. This means that $P_1((|A|-s(\lfloor |A|/s \rfloor)-1, \lfloor |A|/s \rfloor)_b)$ ¿ $P_1(\mathbf{v})$ for any $\mathbf{v} \in MIN \equiv |A|-1$. Furthermore, it also means that $P_2((|A|-s(\lfloor |A|/s \rfloor - 1)-r-1, \lfloor |A|/s \rfloor - 1)_b) < P_2(\mathbf{u})$ for any $\mathbf{u} \in MIN \equiv |A|-r-1$. Finally, by 10.32 we know that $\{(|A|-s(\lfloor |A|/s \rfloor)-1, \lfloor |A|/s \rfloor)_b, (|A|-s(\lfloor |A|/s \rfloor - 1)-r-1, \lfloor |A|/s \rfloor - 1)_b\}$ is *lub*-complete. From this the desired result follows.

10.2.2 Convexity of MIN(z)

Note: The following definition and Lemma about the convexity of $MIN(z)$ was originally used in proving Vadim's conjecture, but they are no longer needed for that. However, I included it here because it is somewhat interesting by itself.

Definition 10.26. *For any set of incomparable points in the Selmer Lattice (not necessarily the Minimal Selmer Lattice), we can write the points as $\{(c_i,d_i)_b | i \in [1,k]\}$, where $c_i > c_j$ iff $i < j$ (from which it follows that $d_i < d_j$ iff $i < j$) (note: we let P_i denote $(c_i,d_i)_b$). We define such a set to be* convex *when $\frac{d_1-d_2}{c_1-c_2} > \frac{d_2-d_3}{c_2-c_3} > ... > \frac{d_{k-1}-d_k}{c_{k-1}-c_k}$.*

Lemma 10.27. *For each $z \in [0, |A|-1]$, $MIN(z)$ is a convex set.*

Proof. Assume the contrary. Then there exists i such that $\frac{d_i-d_{i+1}}{c_i-c_{i+1}} < \frac{d_{i+1}-d_{i+2}}{c_{i+1}-c_{i+2}}$. We assume WLOG that $i=1$.

We will show that there exists a vector $(p,q)_b \equiv z \bmod |A|$, with $p,q \in \mathbb{N}_0$, $c_3 < p < c_2$, and $d_1 < q < d_2$. But this will contradict our initial assumptions, because that $(p,q)_b$ must be in the Selmer lattice because $(p,q)_b <_B (c_2,d_2)_b$, which we assume is in the Selmer lattice, and $(p,q)_b >_B (0,0)_b$, so therefore $(p,q)_b$ must lie in the Selmer lattice. Furthermore, since $(p,q)_b <_B (c_2,d_2)_b$, we have that $(c_2,d_2)_b$ cannot be in MIN, which contradicts our original assumption.

To simplify the calculations we are about to do, we define a new coordinate system $(x,y)_{b'}$, where the point $(x,y)_b = (x-c_3, y-d_1)_{b'}$. Then $P_1 = (c_1-c_3, 0)_{b'}$, $P_2 = (c_2-c_3, d_2-d_1)_{b'}$, and $P_3 = (0, d_3-d_1)_{b'}$. Finally, let $a = c_2-c_3$, $b = d_2-d_1$, $x = (c_1-c_2)$, and $y = d_3-d_2$. So now we

have that $P_1 = (a + x, 0)_{b'}$, $P_2 = (a, b)_{b'}$, and $P_3 = (0, b + y)_{b'}$. Finally, let $\mathbf{u} = P_1 - P_2 = (a, -y)$ and $\mathbf{v} = P_2 - P_3 = (x, -b)$. Notice that $\mathbf{u} \equiv \mathbf{v} \equiv 0 \mod |A|$.

The condition that $\frac{d_1-d_2}{c_1-c_2} < \frac{d_2-d_3}{c_2-c_3}$ translates to $\frac{-b}{x} < \frac{-y}{a}$, or equivalently $xy < ab$. Showing the existence of the vector $(p, q)_b$ as defined above translates to finding a vector $(r, s)_{b'} \equiv z \mod |A|$, with $r, s \in \mathbb{N}_0$, $r < a$ and $s < b$. Consider vectors of the form $c\mathbf{u} + d\mathbf{v} + (a, b)_{b'}$, where $c, d \in \mathbb{Z}$. All of these vectors are congruent to z. Since every vector congruent to $z \mod |A|$ can be expressed in this form, finding the vector $(r, s)_{b'}$ described above is equivalent to finding c, d such that $c\mathbf{u} + d\mathbf{v} + (a, b)_{b'}$ satisfies the same conditions as $(r, s)_{b'}$. So, it suffices to find integers c, d such that $0 \leq ca + dx + a < a$ and $0 \leq -cy - db + b \leq b$, or equivalently:

$$-a \leq ca + dx < 0 \tag{4}$$

and

$$0 \leq cy + db \leq b \tag{5}$$

Solving equation (1) gives

$$c = -\lfloor \frac{dx}{a} \rfloor - 1 \tag{6}$$

and equation (2) is satisfied when

$$d = -\lfloor \frac{cy}{b} \rfloor \tag{7}$$

(note this is not always the unique solution, but this turns out not to matter). So in order to find $(r, s)_{b'}$, it suffices to find c, d that satisfy equations (3) and (4) simultaneously. Substituting d in equation (3), we get $c = -\lfloor \frac{-\lfloor \frac{cy}{b} \rfloor x}{a} \rfloor - 1$, or equivalently

$$c = \lfloor \frac{\lfloor \frac{cy}{b} \rfloor x}{a} \rfloor - 1 \tag{8}$$

.

When $c = 0$, the LHS of equation (5) $= 0$, and the RHS $= -1$, so in particular, the LHS $>$ the RHS. When $c = -ab$, the RHS $= xy - 1$, so in particular the LHS $\leq$ RHS. Notice that as c decreases by 1, the RHS is non-increasing and the LHS obviously decreases by 1. This means that for some

$0 > c \geq -ab$, we must have that the LHS and the RHS are exactly equal for that value of c.

□

10.2.3 Vadim's Theorem

In this article, we focus on the special case on the vector Frobenius problem when $n \geq 2$ and $m = 2$. We also assume that no $\mathbf{b}$ vector is parallel to any $\mathbf{a}$ vector. The main result is that for every element $\mathbf{v} \in MIN$, $\exists$ a Frobenius vector $\mathbf{g}$ and $|A| - 1$ elements $\{\omega_{\mathbf{1}}, \omega_{\mathbf{2}}, ...\omega_{\mathbf{|A|-1}}\}$ such that $lub(\mathbf{v}, \omega_{\mathbf{1}}, \omega_{\mathbf{2}}, ...\omega_{\mathbf{|A|-1}}) - A_1 = \mathbf{g}$. However, in my opinion, the lemmas and definitions used in proving this are just as interesting as the result itself.

Definition 10.28. *We call an element of the Selmer lattice* $\mathbf{v}$ *a* corner point *if* $\mathbf{v} + b_1$ *and* $\mathbf{v} + b_2$ *are both not in the Selmer lattice. We call an element* $\mathbf{u} \in MIN$ *a* minimal corner point *if* $\mathbf{u} + b_1$ *and* $\mathbf{u} + b_2$ *are both not in* MIN.

Note: recall that we proved in the midterm report that for every vector $\mathbf{v}$ that is both a corner point and a minimal corner point, $\mathbf{v} - A_1$ is a Frobenius vector.

Definition 10.29. *We call a set of points* $\{\mathbf{a_i} | i \in [1, k]$ *and* $\mathbf{a_i} \in MIN\}$ *lub complete if for every* $0 \leq j \leq |A| - 1$ *(*$j \in \mathbb{N}_0$*), there exists an element* $\mathbf{v_j} \equiv j \mod |A| - 1$ *such that* $\mathbf{v_j} \in MIN$ *and* $\mathbf{v_j} \leq \mathbf{a_i}$ *for some* i*, not necessarily the same* i *for each* j.

Definition 10.30. *For* $c_1, c_2, ...c_n \in \mathbb{N}_0$*, let* $(c_1, c_2, ...c_n)_a$ *denote* $c_1\mathbf{a_1} + c_2\mathbf{a_2} + ... + c_n\mathbf{a_n}$.

Definition 10.31. *For* $d_1, d_2 \in \mathbb{N}_0$*, let* $(d_1, d_2)_b$ *denote* $d_1\mathbf{b_1} + d_2\mathbf{b_2}$.

Lemma 10.32. *Let* r *be the largest natural number such that there exists an element of* MIN *with* b_1*-value* $= r$*, and no element of* MIN *has a greater* b_1*-value. Let* (r, s) *be the element in* MIN *with* b_1*-value* $= r$*, and with the largest* b_2*-value. Let the significant zero with the greatest* b_1*-value* $< r$ *be* $(x_1, y_1)_b$*, and let the significant zero with the greatest* b_1*-value* $< x_1$ *be* (x_2, y_2)*. Let* (p, q) *be element of* $MIN \equiv (r, s)$ *with the largest* b_1*-value not exceeding* r*. Then the set* $\{(p, q - 1), (r, s)\}$ *is lub-complete.*

(Note: we make the assumption here that both $(x_1, y_1)_b$ and $(x_2, y_2)_b$, but this is a harmless assumption because the case where one or both of them do not exist has been completely solved in Darren's article "Generalization of the first two steps of the Selmer algorithm," and the main theorem we wish to prove is clearly true in those two cases).

Proof. We first show that $p = x_1 - 1$. By the theorem that every corner point is complete, it follows that there exists an element congruent to $(r, s)_b$ with b_1-value $\leq x_1 - 1$ and $y_1 \leq b_2$-value $\leq y_2 - 1$. Now, we cannot have that $p < x_1 - 1$, because then $(p+1, q)_b$ is in MIN, which implies that $(r+1, s)_b$ is in MIN (since $(r+1, s)_b - (p+1, q)_b = (r, s)_b - (p, q)_b$.

Since $(x_1, y_1)_b \equiv 0$, we know $(-x_1, 0)_b \equiv (0, y_1)_b$. So, it follows that $(r - k * x_1, s) \equiv (x_1 - 1, q + k * y_1)$, where $k \in \mathbb{N}$. This means that every element satisfying $0 \leq b_1$-value $\leq x_1 - 1$ and $q \leq b_2$-value $\leq y_2 - 1$ is congruent to some element satisfying $0 \leq b_1$-value $\leq r$ and $0 \leq b_2$-value $\leq s$, that is, some element in the contained set of (r, s). Recall that the element $(x_1 - 1, y_2 - 1)$ is a corner point, and therefore it is good. From this the desired result follows.

□

Lemma 10.33. *Let* $\mathbf{b_1} = (x_1, x_2, ..., x_n)_a$, *and let* $\mathbf{b_2} = (y_1, y_2, ..., y_n)_a$, *and assume WLOG that* $\frac{x_1}{y_1} = \max\{\frac{x_i}{y_i}\}$ *and* $\frac{x_n}{y_n} = \min\{\frac{x_i}{y_i}\}$. *Then for any two distinct congruent elements* $\mathbf{u} = (c_1, c_2)_b, \mathbf{v} = (d_1, d_2)_b \in MIN$, $d_1 > c_1 \Rightarrow P_1(\mathbf{v}) < P_1(\mathbf{u})$ *and* $P_n(\mathbf{v}) > P_n(\mathbf{u})$.

Proof. This follows easily from Darren's vector division theorem.

□

Theorem 10.34. *For every element* $\mathbf{v} \in MIN$, $\exists$ *a Frobenius vector* $\mathbf{g}$ *and* $|A| - 1$ *elements* $\{\omega_\mathbf{1}, \omega_\mathbf{2}, ...\omega_{|\mathbf{A}|-\mathbf{1}}\}$ *such that* $lub(\mathbf{v}, \omega_\mathbf{1}, \omega_\mathbf{2}, ...\omega_{|\mathbf{A}|-\mathbf{1}}) - A_1 = \mathbf{g}$.

Proof. If an element $\mathbf{v} \in MIN$ has the desired property (that is, it is used in some *lub*), we call $\mathbf{v}$ *usable*. It is easy to see that if $\mathbf{v}$ is usable, then any vector $\leq_B$ to $\mathbf{v}$ is also usable.

By Darren's theorem of wavy cuts, we know that all but at most two minimal corner points are also corner points. If we can show that the remaining

minimal corner points (i.e. those that are not also corner points) are usable, then the proof is complete, since every element of MIN is $\leq_B$ some minimal corner point.

Notice that for an element to be a minimal corner point but not a corner point, it must lie on one of the two wavy cuts. We will only deal with the case where it lies on the vertical wavy cut, as the other case is analogous. Call this element $\mathbf{v}$, and let it be congruent to k mod $|A|$.

Since $\mathbf{v}$ lies in the rightmost column, as a result of Lemma 10.33, we may WLOG assume $P_1(\mathbf{v}) < P_1(\mathbf{u})$ for any $\mathbf{u} \in MIN(k)$, $\mathbf{u} \neq \mathbf{v}$. Let $\mathbf{w}$ be the element in $MIN(k)$ in the second largest column. By Lemma 10.32 , we know $\exists \mathbf{y}$ such that $\{\mathbf{v}, \mathbf{y}\}$ is *lub* complete and $P_1(lub(\mathbf{v}, \mathbf{z})) < P_1(\mathbf{w})$ (Notice that we need the assumption $\mathbf{b_i}$ is not parallel to $\mathbf{a_j}$ here to get the strict inequality. Since every P_1 of any *lub* complete set must be $\geq P_(z)$, we have shown that $\mathbf{v}$ is usable.

□

10.2.4 A bound for the cardinality of the MIN set in higher dimensions

For $n \geq 2$, the following theorem establishes a bound on the cardinality of $MIN(a)$ (the elements in MIN belonging to the same congruence class) as a function of $|A|$ and m:

Theorem 10.35. *For any* $a \leq |A|, |MIN(a)| \leq \binom{|A| + m - 2}{m - 1}$.

Proof. Recall that all elements of MIN can be represented as $\sum_{i=1}^{m} c_i \mathbf{b_i}$ where $c_i \in \mathbf{N}_0$ and $\sum_{i=1}^{m} c_i \leq |A| - 1$. Given such an element $\sum_{i=1}^{m} a_i \mathbf{b_i}$ of MIN, define the *k-column*, where $k \in [0, m]$, to be the set $\{c_1\mathbf{b_1} + ... + c_{k-1}\mathbf{b_{k-1}} + a_k\mathbf{b_k} + c_{k+1}\mathbf{b_{k+1}} + ... + c_m\mathbf{b_m} | a_k \in [0, |A|] \}$

Notice that all the elements of any k-column are comparable to each other. This means that in any k-column, there cannot be two congruent elements belonging to MIN. It is also easy to see that every element in MIN belongs to some k-column.

We will count the total number of possible m-columns. Notice that each m column can be uniquely represented by the numbers c_i, where $c_i \in \mathbf{N}_0$. Furthermore, we must have that $\sum_{i=1}^{m-1} c_i \leq |A| - 1$. It is well known that

the number of ways to choose $\{c_i\}$ under these conditions is $\binom{|A|+m-2}{m-1}$. The desired result follows. $\square$

Notice that when $m = 1$, this bound equals 1. This is reassuring, since we know that when $m = 1$, there is a unique Frobenius vector. Also, when $m = 2$, this bound equals $|A|$, which has been previously proven.

Theorem 10.36. *When $n = m$, this bound is always achievable.*

Proof. When all $\mathbf{b_i}$ are congruent mod $|A|$ (say WLOG they are all congruent to 1), then all elements of the set $S = \{\sum_{i=1}^{m} c_i \mathbf{b_i} | \sum_{i=1}^{m} c_i = |A| - 1\}$ are congruent to $|A| - 1$, and furthermore there are exactly $\binom{|A|+m-2}{m-1}$ elements in this set. If we can choose $\{\ \mathbf{b_i}\ \}$ so that all the elements in S are incomparable, then every element in S must be in MIN, and we would have $|MIN(|A| - 1) = \binom{|A|+m-2}{m-1}$.

Define the map $P_i(\mathbf{v})\ \forall i \in [1, m]$ which projects $\mathbf{v}$ onto the $\mathbf{a_i}$ axis. Pick $\mathbf{b_i}$ such that $P_i(\mathbf{b_i}) > |A| * \max_i \{P_i(\mathbf{b_k}) | k \neq i\}$. We know we can always do this because given any vector $\mathbf{v}$, $\mathbf{v} + \mathbf{a_i} \equiv \mathbf{v}$. Now, for any two elements $\mathbf{u}$ and $\mathbf{w} \equiv |A| - 1$, we can write their difference as $\mathbf{u} - \mathbf{w} = \sum_{i=1}^{m} d_i \mathbf{b_i}$, where $\sum_{i=1}^{m} d_i = 0$ and $\sum_{i=1}^{m} |d_i| \leq |A|$. Assuming $\mathbf{u}$ and $\mathbf{w}$ are not equal, we must have at least one i such that $|d_i| > 0$, and therefore we must have some i, j such that $d_i > 0$ and $d_j < 0$. Then it follows that $P_i(\mathbf{u} - \mathbf{w}) > 0$ because $P_i(d_i \mathbf{b_i}) \geq P_i(\mathbf{b_i}) \geq |A| * \max_i \{P_i(\mathbf{b_k}) | k \neq i\} \geq P_i(\sum_{k=1, k\neq i}^{m} |d_k \mathbf{b_k}|)$. Similarly, we have that $P_j(\mathbf{u} - \mathbf{w}) < 0$. So, every two elements in S are also in MIN, and from this the desired result follows. $\square$

Corollary 10.37. *Given any n x n matrix A, it is possible to find m* $\mathbf{b}$*-vectors which yield exactly* $\binom{|A|+m-2}{m-1}$ *different Frobenius vectors.*

Proof. We will show that using the same construction for $\mathbf{b_i}$ as in the proof for 10.36, each vector in the set S (defined in the proof for theorem 2) is good. For any $\mathbf{v} \in S$, $\mathbf{v} = \sum_{i=1}^{m} c_i \mathbf{b_i}$ where $\sum_{i=1}^{m} c_i = |A| - 1$, define the set $S_{\mathbf{v}} = \{\sum_{i=1}^{m} d_i \mathbf{b_i} | d_i \leq c_i\}$. It is clear that all elements of $S_{\mathbf{v}}$ are less than $\mathbf{v}$ in cone ordering. Also, since $\mathbf{b_i} \equiv 1 \forall i$, we have that $\sum_{i=1}^{m} d_i \mathbf{b_i} \equiv$

$\sum_{i=1}^{m} d_i$, and thus this set contains at least one element in each equivalence class mod $|A|$. This means that each element of S is good and therefore each such element subtracted by A_1 is a Frobenius vector, yielding exactly $\binom{|A|+m-2}{m-1}$ different Frobenius vectors. □

11 Induced Cone Ordering and lub-complete vectors

11.1 Definitions

Definition 11.1. *Call a vector* lub-complete *if it is greater than a complete set of coset representatives. Call a minimal lub-complete vector with respect to cone ordering* minimal lub-complete*. The set of all minimal lub-complete is* $G + \mathbf{A_1}$ *and for each minimal lub-complete vector there is a corresponding g-vector which is less than it by exactly* $\mathbf{A_1}$*.*

Definition 11.2. *Call* $\mathbf{v_s}$ *a supporting vector of lub-complete* $\mathbf{v}$ *with respect to* $\leq$*-ordering when* $\mathbf{v_s} \leq \mathbf{v}$*,* $\mathbf{v_s} \not\equiv \mathbf{v}$ *and* $\nexists \mathbf{v_s'} \equiv \mathbf{v_s}$ *with* $\mathbf{v_s'} \leq \mathbf{v}$*.*

Definition 11.3. *Call two vectors of the same congruence class* neighboring *if there is no vector of their congruence class between their lub and glb.*

Definition 11.4. *Denote* $\leq$*-relation with respect to* B*-basis as* $\underset{B}{\leq}$

Definition 11.5. *Define* B*-plane to be the plane spanned by* B*-vectors.*

11.2 Induced cone ordering for $m = 2$

In the same way as A-vectors define cone ordering in $\mathbb{R}^n$, there exist two vectors defining the induced cone ordering on the B-plane. If B-vectors are colinear, cone ordering defines a total ordering on $B_{\mathbb{N}_0}$. Here we are assuming that B-vectors are not colinear.

Definition 11.6. *On the* B*-plane define* induced cone ordering *to be the ordering equivalent to the cone ordering on the* B*-plane. Below we find some properties of this ordering. This ordering enables us to use arguments from the 2-dimensional case in n-dimensions.*

Below we find the vectors defining the induced cone ordering:

First define $\frac{b_{2,i\,max}}{b_{1,i\,max}} = max(\frac{b_{2,i}}{b_{1,i}})$ and $\frac{b_{2,i\,min}}{b_{1,i\,min}} = min(\frac{b_{2,i}}{b_{1,i}})$ where i can only be such that $b_{1,i} \neq 0$. Analogously define $\frac{b_{1,i\,max}}{b_{2,i\,max}}$ and $\frac{b_{1,i\,min}}{b_{2,i\,min}}$.

1. If for all i, $b_{1,i} \neq 0$ or both $b_{1,i} = b_{2,i} = 0$, then the induced cone ordering is defined by the vectors $\tilde{\mathbf{a}}_\mathbf{1} = \frac{b_{2,i\,max}}{b_{1,i\,max}}\mathbf{b_1} - \mathbf{b_2}$ and $\tilde{\mathbf{a}}_\mathbf{2} = -\frac{b_{2,i\,min}}{b_{1,i\,min}}\mathbf{b_1} + \mathbf{b_2}$.
2. If for all i, $b_{2,i} \neq 0$ or both $b_{1,i} = b_{2,i} = 0$, then the induced cone ordering is defined by the vectors $\tilde{\mathbf{a}}_\mathbf{1} = \frac{b_{1,i\,max}}{b_{2,i\,max}}\mathbf{b_2} - \mathbf{b_1}$ and $\tilde{\mathbf{a}}_\mathbf{2} = -\frac{b_{1,i\,min}}{b_{2,i\,min}}\mathbf{b_2} + \mathbf{b_1}$.
3. If there exist i and j with $b_{1,i} = 0$, $b_{2,i} \neq 0$ and $b_{2,j} = 0$ and $b_{1,j} \neq 0$, then the induced cone ordering is defined by the vectors $\tilde{\mathbf{a}}_\mathbf{1} = \mathbf{b_1}$ and $\tilde{\mathbf{a}}_\mathbf{2} = \mathbf{b_2}$.

Definition 11.7. *Denote $\leq$-relation defined by the induced cone ordering as $\underset{\sim}{\leq}$ and $\prec$-relation as $\underset{\sim}{\prec}$. Henceforth $\tilde{A}$ will refer to $\tilde{\mathbf{a}}_\mathbf{1}$ and $\tilde{\mathbf{a}}_\mathbf{2}$.*

Lemma 11.8. *If for all i, $b_{1,i} \neq 0$ or both $b_{1,i} = b_{2,i} = 0$, then $\frac{b_{2,i\,max}}{b_{1,i\,max}} \neq \frac{b_{2,i\,min}}{b_{1,i\,min}}$. It then follows $\frac{b_{2,i\,max}}{b_{1,i\,max}} \neq 0$.*

Proof. If we suppose the opposite, we have $\frac{b_{2,i_0}}{b_{1,i_0}} = \frac{b_{2,i}}{b_{1,i}}$ (assuming that there is i_0 with $b_{1,i_0} \neq 0$) which means that $b_{2,i} = \frac{b_{2,i_0}}{b_{1,i_0}} b_{1,i}$ for all i with $b_{1,i} \neq 0$. The equality still holds when $b_{1,i} = 0$ as then we also have $b_{2,i} = 0$ from the assumptions of the lemma. Thus, we reach contradiction as B vectors are assumed to be not colinear. □

Lemma 11.9. *In all cases $\mathbf{b_1}, \mathbf{b_2} \underset{\sim}{\geq} 0$*

Proof. When $\tilde{\mathbf{a}}_\mathbf{1} = \mathbf{b_1}$ and $\tilde{\mathbf{a}}_\mathbf{2} = \mathbf{b_2}$ the claim is obvious. When $\tilde{\mathbf{a}}_\mathbf{1} = \frac{b_{2,i\,max}}{b_{1,i\,max}}\mathbf{b_1} - \mathbf{b_2}$ and $\tilde{\mathbf{a}}_\mathbf{2} = -\frac{b_{2,i\,min}}{b_{1,i\,min}}\mathbf{b_1} + \mathbf{b_2}$ we see that

$$\mathbf{b_1} = \frac{\tilde{\mathbf{a}}_\mathbf{1} + \tilde{\mathbf{a}}_\mathbf{2}}{\frac{b_{2,i\,max}}{b_{1,i\,max}} - \frac{b_{2,i\,min}}{b_{1,i\,min}}} \underset{\sim}{\geq} 0$$

and (as by Lemma 11.8 $\frac{b_{2,i\,max}}{b_{1,i\,max}} \neq 0$ and $\frac{b_{2,i\,max}}{b_{1,i\,max}} > \frac{b_{2,i\,min}}{b_{1,i\,min}}$)

$$\mathbf{b_2} = \frac{\tilde{\mathbf{a}}_\mathbf{2} + \frac{b_{1,i\,max}}{b_{2,i\,max}} \frac{b_{2,i\,min}}{b_{1,i\,min}} \tilde{\mathbf{a}}_\mathbf{1}}{1 - \frac{b_{1,i\,max}}{b_{2,i\,max}} \frac{b_{2,i\,min}}{b_{1,i\,min}}} \underset{\sim}{\geq} 0$$

as claimed. □

Theorem 11.10. *The induced cone ordering and the cone ordering are equivalent on the B-plane.*

Proof. It is sufficient to show that ≥ 0 is equivalent to $\underset{\sim}{\geq} 0$.

For every $c_1\mathbf{b_1} + c_2\mathbf{b_2}$ for it to be ≥ 0 it is necessary and sufficient to satisfy $c_1 b_{1,i} + c_2 b_{2,i} \geq 0$ for all i. Next, in separate cases we obtain more specific criteria: If $b_{1,i} = 0$ and $b_{2,i} = 0$ the inequality holds trivially. If $b_{1,i} \neq 0$ it is equivalent to $c_1 \geq -c_2 \frac{b_{2,i}}{b_{1,i}}$ which is in turn equivalent to $c_1 \geq -c_2 \frac{b_{2,i\,min}}{b_{1,i\,min}}$ when $c_2 \geq 0$ and $c_1 \geq -c_2 \frac{b_{2,i\,max}}{b_{1,i\,max}}$ when $c_2 \leq 0$. If $b_{1,i} = 0$ and $b_{2,i} \neq 0$ it is equivalent to $c_2 \geq 0$. Finally, if $b_{2,i} = 0$ and $b_{1,i} \neq 0$ it is equivalent to $c_1 \geq 0$.

We need to show that $d_1\tilde{\mathbf{a_1}} + d_2\tilde{\mathbf{a_2}} \geq 0$ iff $d_1, d_2 \geq 0$ where $\tilde{\mathbf{a_1}}$ and $\tilde{\mathbf{a_1}}$ are as defined above.

First case: there doesn't exist i with $b_{1,i} = 0$ and $b_{2,i} \neq 0$.

We rewrite $d_1\tilde{\mathbf{a_1}} + d_2\tilde{\mathbf{a_2}} = (d_1 \frac{b_{2,i\,max}}{b_{1,i\,max}} - d_2 \frac{b_{2,i\,min}}{b_{1,i\,min}})\mathbf{b_1} + (d_2 - d_1)\mathbf{b_2} = c_1\mathbf{b_1} + c_2\mathbf{b_2}$. Now let's check when our criterion is satisfied: If $d_2 - d_1 = c_2 \geq 0$, $c_1 \geq -c_2 \frac{b_{2,i\,min}}{b_{1,i\,min}}$ is equivalent to $d_1 \frac{b_{2,i\,max}}{b_{1,i\,max}} - d_2 \frac{b_{2,i\,min}}{b_{1,i\,min}} \geq -(d_2 - d_1) \frac{b_{2,i\,min}}{b_{1,i\,min}}$ equivalent to $d_1(\frac{b_{2,i\,max}}{b_{1,i\,max}} - \frac{b_{2,i\,min}}{b_{1,i\,min}}) \geq 0$ by Lemma 11.8 equivalent to $d_1 \geq 0$ which with $d_2 - d_1 \geq 0$ implies $d_2 \geq 0$. If $d_2 - d_1 = c_2 \leq 0$, $c_1 \geq -c_2 \frac{b_{2,i\,max}}{b_{1,i\,max}}$ is equivalent to $d_1 \frac{b_{2,i\,max}}{b_{1,i\,max}} - d_2 \frac{b_{2,i\,min}}{b_{1,i\,min}} \geq -(d_2 - d_1) \frac{b_{2,i\,max}}{b_{1,i\,max}}$ equivalent to $d_1(\frac{b_{2,i\,max}}{b_{1,i\,max}} - \frac{b_{2,i\,min}}{b_{1,i\,min}}) \geq 0$ which is analogous to the $d_2 - d_1 \geq 0$ case.

Second case: there doesn't exist i with $b_{2,i} = 0$ and $b_{1,i} \neq 0$. This case is analogous to the first case.

Third case: there exist i and j with $b_{1,i} = 0$, $b_{2,i} \neq 0$ and $b_{2,j} = 0$, $b_{1,j} \neq 0$.

In this case $d_1\tilde{\mathbf{a_1}} + d_2\tilde{\mathbf{a_2}} = d_1\mathbf{b_1} + d_2\mathbf{b_2} \geq 0$ iff $c_1 = d_1 \geq 0$ and $c_2 = d_2 \geq 0$ as claimed. □

Lemma 11.11. *For any* $\mathbf{v}$ *on the B-plane all of its supporting vectors with respect to the induced cone ordering are also its supporting vectors with respect to the cone ordering.*

Proof. Let $\mathbf{v_s}$ be a supporting vector of $\mathbf{v}$ with respect to the induced cone ordering: $\mathbf{v_s} \underset{\sim}{\leq} \mathbf{v}$, $\mathbf{v_s} \not\underset{\sim}{\leq} \mathbf{v}$ and $\nexists \mathbf{v_s'} \equiv \mathbf{v_s}$, $\mathbf{v_s'} \underset{\sim}{\leq} \mathbf{v}$. If $\mathbf{v_s} = \tilde{A} \begin{bmatrix} \tilde{v}_{s,1} \\ \tilde{v}_{s,2} \end{bmatrix}$ and $\mathbf{v} = \tilde{A} \begin{bmatrix} \tilde{v}_1 \\ \tilde{v}_2 \end{bmatrix}$, then either $\tilde{v}_{s,1} = \tilde{v}_1$ or $\tilde{v}_{s,2} = \tilde{v}_2$. As the cases are analogous let's deal with $\tilde{v}_{s,1} = \tilde{v}_1$. When for all i, $b_{1,i} \neq 0$ or both $b_{1,i} = b_{2,i} = 0$, $\tilde{v}_{s,1} = \tilde{v}_1$ means $\mathbf{v} - \mathbf{v_s}$ is a multiple of $\tilde{\mathbf{a}}_\mathbf{2} = -\frac{b_{2,i\,min}}{b_{1,i\,min}}\mathbf{b_1} + \mathbf{b_2}$ which implies that $\mathbf{v} - \mathbf{v_s}$ has a zero coordinate in the i-th dimension where i is the one at which $-\frac{b_{2,i}}{b_{1,i}}$ reaches its minimum. Cases when for all i, $b_{2,i} \neq 0$ or both $b_{1,i} = b_{2,i} = 0$ and when there exist i and j with $b_{1,i} = 0$, $b_{2,i} \neq 0$ and $b_{2,j} = 0$ and $b_{1,j} \neq 0$ are analogous. □

11.3 Clustering of minimal lub-complete in n-dimensions

Definition 11.12. *Define lub-cluster to be a minimal lub-complete vector with respect to the induced cone ordering.*

The following lemma justifies the choice of the term lub-cluster:

Lemma 11.13. *For every lub-cluster* $\mathbf{v}$ *there exists a minimal lub-complete* $\mathbf{w}$ *with* $\mathbf{w} \leq \mathbf{v}$ *and for every such* $\mathbf{w}$ *its set of supporting vectors includes the set of supporting vectors of* $\mathbf{v}$.

Proof. As the $\mathbf{v}$ is minimal lub-complete with respect to the induced cone ordering it is lub-complete with respect to the cone ordering. Then there exists a minimal lub-complete $\mathbf{w}$ with $\mathbf{w} \leq \mathbf{v}$.

Suppose there exists a supporting vector $\mathbf{v_s}$ of $\mathbf{v}$ which isn't a supporting vector of $\mathbf{w}$. If $\mathbf{v_s} \not\leq \mathbf{w}$, then there exists a MIN vector $\mathbf{w_s}$ with $\mathbf{w_s} \equiv \mathbf{v_s}$

and $\mathbf{w_s} \leq \mathbf{w} \leq \mathbf{v}$ which contradicts with $\mathbf{v_s}$ being a supporting vector of $\mathbf{v}$. If $\mathbf{v_s} \prec \mathbf{w} \leq \mathbf{v}$, we have $\mathbf{v_s} \prec \mathbf{v}$ which is in contradiction with $\mathbf{v_s}$ being a supporting vector of $\mathbf{v}$. Thus, we can only have $\mathbf{v_s} \leq \mathbf{w}$ while $\mathbf{v_s} \not\prec \mathbf{w}$. Also by previous argument we cannot have $\mathbf{w_s} \equiv \mathbf{v_s}$ and $\mathbf{w_s} \leq \mathbf{w}$, so $\mathbf{v_s}$ is a supporting vector of $\mathbf{w}$. □

Lemma 11.14. *There exists a sequence of lub-clusters* $\mathbf{l_i} = \tilde{A} \begin{bmatrix} l_{i,1} \\ l_{i,2} \end{bmatrix}$ $(i = 1, ..., i_{last})$ *such that*

1. $l_{i,1} < l_{i+1,1}$ *for* $1 \leq i \leq i_{last} - 1$
2. *There doesn't exist an lub-cluster* $l' = \begin{bmatrix} l'_1 \\ l'_2 \end{bmatrix}$ *with* $l'_1 < l_{1,1}$ *or* $l'_1 > l_{i_{last},1}$
3. *There exist two neighboring supporting vectors* $\mathbf{s_1(i)} = \begin{bmatrix} s_{1,1} \\ s_{1,2} \end{bmatrix}$ *and* $\mathbf{s_2(i)} = \begin{bmatrix} s_{2,1} \\ s_{2,2} \end{bmatrix}$ *with* $s_{1,2} = l_{i,2}$, $s_{1,1} \leq l_{i,1}$, $s_{2,1} = l_{i+1,1}$, $s_{2,2} \leq l_{i+1,2}$ *for* $1 \leq i \leq i_{last} - 1$
4. *There exist supporting points* $\mathbf{s_1}$ *and* $\mathbf{s_{i_{last}}}$ *of* $\mathbf{l_1}$ *and* $\mathbf{l_{i_{last}}}$ *respectively, such that* $s_{1,1} = l_{1,1}$, $s_{i_{last},2} = l_{i_{last}}$ *and* $\nexists \mathbf{s'_1}, \mathbf{s'_{i_{last}}}$ *congruent to them with* $s'_{1,1} < s_{1,1}$, $s'_{i_{last},1} > s_{i_{last},1}$.

Proof. Choose l_{min} to be the least number such that there exists a complete set of coset representatives $\{\mathbf{w_i}\}_{i=1}^{i=|A|}$ with $w_{i,1} \leq l_{min}$. From minimality of l_{min} we must have *4*. Property *4* for the last $\mathbf{l_i}$ in the sequence can be proved analogously. As the number of residue classes is finite, there exists $max(\{w_{i,2}\})$ so that $\begin{bmatrix} l_{min} \\ max(\{w_{i,2}\}) \end{bmatrix}$ is lub-complete. Then there exists an lub-cluster $\mathbf{l_1} \leq \begin{bmatrix} l_{min} \\ max(\{w_{i,2}\}) \end{bmatrix}$ which also satisfies $l_{1,1} = l_{min}$ and *2* by the choice of l_{min}.

Now let's define the rest of the sequence by induction. If we have $\mathbf{l_i}$ let's define $\mathbf{l_{i+1}}$. Let $\{\mathbf{w_j}\}$ is the set of all supporting vectors of $\mathbf{l_i}$ such that $w_{j,2} = l_{i,2}$ for all $\mathbf{w_j}$. If for some of $\mathbf{w_j}$ there doesn't exist a neighboring $\mathbf{w'_j} \equiv \mathbf{w_j}$ such that $w'_{j,1} > w_{j,1}$ we reached the last vector in our sequence because for

any $\mathbf{l_{i+1}}$ with $l_{i+1,1} > l_{i,1}$ we have $l_{i+1,2} < l_{i,2} = w_{j,2}$ and we cannot have a complete set of coset representatives less than $\mathbf{l_{i+1}}$. Otherwise there exists the set $\{\mathbf{w_j'}\}$ of neighboring vectors with $w'_{j,1} > w_{j,1}$. Let $l_{i+1,1} = max(\{\mathbf{w_j'}\})$ and j be the index of one of $\mathbf{w_j'}$ for which the max is achieved. Then $\begin{bmatrix} l_{i+1,1} \\ l_{i,2} \end{bmatrix}$ is lub-complete, there are no supporting vectors $\mathbf{w_j}$ with $w_{j,2} = l_{i,2}$ so there must exist an lub-cluster $\mathbf{l_{i+1}} = \begin{bmatrix} l_{i+1,1} \\ l_{i+1,2} \end{bmatrix}$ with $l_{i+1,2} < l_{i,2}$. Then $\mathbf{w_j}$ and $\mathbf{w_j'}$ are supporting vectors of $\mathbf{l_i}$ and $\mathbf{l_{i+1}}$ respectively. Also as $\mathbf{w_j}$ and $\mathbf{w_j'}$ are neighboring, *3* is satisfied and *1* is obviously satisfied by construction of the $\mathbf{l_i}$ sequence. □

11.4 Vadim's Theorem

Here we show an application of the tools developed above in an alternate proof of Vadim's Theorem.

For the case $m = 2$ we want to show that for every element $\mathbf{w} \in$ MIN, $\mathbf{w} \leq \mathbf{g} + \mathbf{A_1}$ where $g \in G$.

Set $b_{1,i}$ and $b_{2,i}$ be i-th coordinates of corresponding B-vectors with respect to the A-basis. As all B-vectors are in the cone spanned by A-vectors all $b_{j,i}$ are nonnegative. If B vectors are colinear, then the MIN set lies on the line spanned by the B vectors. As B vectors are inside the A cone, cone ordering defines total ordering on the line spanned by the B vectors. It follows that $|\text{MIN}| = |A|$ and we have a unique minimal lub-complete vector which is greater than the entire MIN. Therefore, we can assume that B vectors are not colinear.

Define $\tilde{B} = \begin{bmatrix} \tilde{b}_{1,1} & \tilde{b}_{2,1} \\ \tilde{b}_{1,2} & \tilde{b}_{2,2} \end{bmatrix}$ as follows: $\mathbf{b_1} = \tilde{b}_{1,1}\mathbf{\tilde{a}_1} + \tilde{b}_{1,2}\mathbf{\tilde{a}_2}$ and $\mathbf{b_2} = \tilde{b}_{2,1}\mathbf{\tilde{a}_1} + \tilde{b}_{2,2}\mathbf{\tilde{a}_2}$. As all B-vectors are in the cone spanned by $\tilde{A}$-vectors all $\tilde{b}_{i,j}$ are nonnegative. As B vectors are not colinear we have $|\tilde{B}| \neq 0$ and by swapping B-vectors if needed we will always have $|\tilde{B}| > 0$.

We will need the following lemma:

Lemma 11.15. *Let two vectors* $\mathbf{v_1} = \tilde{A}\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \tilde{A}\tilde{B}\begin{bmatrix} x_{1\,b} \\ y_{1\,b} \end{bmatrix}$ *and* $\mathbf{v_2} = \tilde{A}\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \tilde{A}\tilde{B}\begin{bmatrix} x_{2\,b} \\ y_{2\,b} \end{bmatrix}$ *be such that* $x_1 < x_2$ *and* $y_1 > y_2$. *Then* $x_{1b} < x_{2b}$ *and* $y_{1b} > y_{2b}$. *If we start from non-strict inequalities the same proof yields non-strict inequalities.*

Proof. First $\begin{bmatrix} x_{1,b} \\ y_{2,b} \end{bmatrix} = \tilde{B}^{-1}\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \frac{1}{|\tilde{B}|}\begin{bmatrix} \tilde{b}_{2,2}x_1 - \tilde{b}_{2,1}y_1 \\ -\tilde{b}_{1,2}x_1 + \tilde{b}_{1,1}y_1 \end{bmatrix}$ and analogously $\begin{bmatrix} x_{2,b} \\ y_{2,b} \end{bmatrix} = \frac{1}{|\tilde{B}|}\begin{bmatrix} \tilde{b}_{2,2}x_2 - \tilde{b}_{2,1}y_2 \\ -\tilde{b}_{1,2}x_2 + \tilde{b}_{1,1}y_2 \end{bmatrix}$.

As $\tilde{b}_{2,2}(x_2 - x_1) \geq 0 \geq \tilde{b}_{2,1}(y_2 - y_1)$ we have $|\tilde{B}|x_{1b} = \tilde{b}_{2,2}x_1 - \tilde{b}_{2,1}y_1 < \tilde{b}_{2,2}x_2 - \tilde{b}_{2,1}y_2 = |B|x_{2b}$ (the inequality becomes strict since one of the $\tilde{b}_{2,2}$ and $\tilde{b}_{2,1}$ is non-zero and one of the inequalities above is strict) and as $\tilde{b}_{1,2}(x_2 - x_1) \geq 0 \geq \tilde{b}_{1,1}(y_2 - y_1)$ we have $|B|y_{1b} = -\tilde{b}_{1,2}x_1 + \tilde{b}_{1,1}y_1 > -\tilde{b}_{1,2}x_2 + \tilde{b}_{1,1}y_2 = |B|y_{2b}$. As $|B| > 0$ the claim follows. □

Now let $\mathbf{w_1} = \tilde{A}\begin{bmatrix} w_{1,1} \\ w_{1,2} \end{bmatrix} \in$ MIN. Suppose for contradiction that $\mathbf{w_1}$ isn't less than any minimal lub-complete. Because $\mathbf{w_1}$ is in MIN, it isn't greater than any lub-cluster or else by Lemma 11.13 it will be greater than some minimal lub-complete which must be greater than some MIN vector of the same equivalence class as $\mathbf{w_1}$ which contradicts $\mathbf{w_1} \in$ MIN. Our proof will be broken into two cases: when there exists an i such that $l_{i,1} \leq w_{1,1} \leq l_{i+1,1}$ and when $w_{1,1} < l_{1,1}$ (case when $w_{1,1} > l_{i_{last},1}$ is analogous). First we prove the latter case:

Proof. Let $\mathbf{g} = \tilde{A}\begin{bmatrix} g_1 \\ g_2 \end{bmatrix} = \tilde{A}\tilde{B}\begin{bmatrix} g_{1\,b} \\ g_{2\,b} \end{bmatrix} = \mathbf{l_1}$ and $\mathbf{g_s} = \tilde{A}\begin{bmatrix} g_{s,1} \\ g_{s,2} \end{bmatrix} = \tilde{A}\tilde{B}\begin{bmatrix} g_{s,1\,b} \\ g_{s,2\,b} \end{bmatrix}$ be a supporting vector of $\mathbf{g}$ with $g_{s,1} = g_1$ and $\nexists \mathbf{g_s'} \equiv \mathbf{g_s}$ such that $g_{s,1}' < g_{s,1}$ (such $\mathbf{g_s}$ exists by *4* of Lemma 11.14). Now add to $\mathbf{w_1}$ enough copies of $\mathbf{b_1}$ and $\mathbf{b_2}$ so that it remains in MIN while neither $\mathbf{w_1} + \mathbf{b_1}$ nor $\mathbf{w_1} + \mathbf{b_2}$ is in MIN (this is possible as all MIN elements can be expressed as linear combinations of B vectors with coefficients $< |A|$). After this $\mathbf{w_1}$ will increase and there still will be no minimal lub-complete vectors greater than it. If $w_{1,1} \geq g_1$, we reach the contradiction in the second part of our proof. By Lemma 11.13 for any minimal lub-complete $\mathbf{v} \leq \mathbf{g}$, $\mathbf{g_s}$ is also a supporting vector of $\mathbf{v}$ and

$\mathbf{l_s} \leq \mathbf{v}$. We cannot have $\mathbf{w_1} \leq \mathbf{l_s}$ as this implies $\mathbf{w_1} \leq \mathbf{v}$ which contradicts our assumption about $\mathbf{w_1}$. Then from $w_{1,1} < g_{s,1}$, we have $w_{1,2} > g_{s,2}$:

$$w_{1,1} < g_{s,1} \; and \; w_{1,2} > g_{s,2} \tag{9}$$

From this by Lemma 11.15 we have

$$w_{1,1\,b} < g_{s,1\,b} \; and \; w_{1,2\,b} > g_{s,2\,b} \tag{10}$$

If $\mathbf{w_1} \equiv \mathbf{g_s}$ we reach contradiction with the choice of $\mathbf{g_s}$ as $w_{1,1} < g_{s,1}$.

Since $\mathbf{g}$ is an lub-complete there is at least one vector $\mathbf{w_2} = \tilde{A} \begin{bmatrix} w_{2,1} \\ w_{2,2} \end{bmatrix} = \tilde{A}\tilde{B} \begin{bmatrix} w_{2,1\,b} \\ w_{2,2\,b} \end{bmatrix} \in$ MIN such that $\mathbf{w_2} \equiv \mathbf{w_1}$ and $\mathbf{w_2} \leq \mathbf{g}$. Among all vectors $\mathbf{w_2}$ such that $\mathbf{w_2} \equiv \mathbf{w_1}$ ($\mathbf{w_2} \neq \mathbf{w_1}$) and $w_{2,1} \leq g_{s,1}$ choose the one with minimal $w_{2,1}$ and denote it $\mathbf{w_2}$. Note that our choice of $\mathbf{w_2}$ doesn't anymore require that $\mathbf{w_2} \leq \mathbf{g}$.

If $w_{2,1} < w_{1,1}$, we must have $w_{2,2} > w_{1,2}$. From this by Lemma 11.15 we have $w_{2,1\,b} < w_{1,1\,b}$ and $w_{2,2\,b} > w_{1,2\,b}$. Vector

$$\mathbf{w_2} + (\mathbf{g_s} - \mathbf{w_1}) = \tilde{A}\tilde{B} \begin{bmatrix} w_{2,1\,b} + g_{s,1\,b} - w_{1,1\,b} \\ w_{2,2\,b} + g_{s,2\,b} - w_{1,2\,b} \end{bmatrix} \underset{B}{\geq} 0$$

by (10) and $w_{2,2\,b} > w_{1,2\,b}$. By $0 < g_{s,1} - w_{1,1} < w_{2,1} + g_{s,1} - w_{1,1} < g_{s,1}$ (by (9) and $w_{2,1} < w_{1,1}$) we found that $\mathbf{w_2} + (\mathbf{g_s} - \mathbf{w_1}) \in B_{\mathbb{N}_0}$ and as $\mathbf{w_2} + (\mathbf{g_s} - \mathbf{w_1}) \equiv \mathbf{g_s}$ we reach contradiction with the choice of $\mathbf{g_s}$.

Then we are left with:

$$w_{1,1} < w_{2,1} < g_{s,1}, \; w_{1,2} > w_{2,2} \; and \; w_{1,2} > g_{s,2} \tag{11}$$

From (11) by Lemma 11.15 we have

$$w_{1,1b} < w_{2,1b} \; and \; w_{1,2b} > w_{2,2b} \tag{12}$$

If $w_{2,1\,b} \leq g_{s,1\,b}$, then the vector

$$\mathbf{w_1} + (\mathbf{g_s} - \mathbf{w_2}) = \tilde{A}\tilde{B} \begin{bmatrix} w_{1,1\,b} + g_{s,1\,b} - w_{2,1\,b} \\ w_{1,2\,b} + g_{s,2\,b} - w_{2,2\,b} \end{bmatrix} \underset{B}{\geq} 0$$

(by $w_{2,1\,b} \leq g_{s,1\,b}$ and (11)) is in $B_{\mathbb{N}_0}$ while $w_{1,1} + (g_{s,1} - w_{2,1}) < g_{s,1}$ (by (11)) and $\mathbf{g_s} \equiv \mathbf{w_1} + (\mathbf{g_s} - \mathbf{w_2})$ which again contradicts with the choice of $\mathbf{g_s}$.

Also if $w_{2,1b} > g_{s,1b}$ we cannot have $w_{2,2b} \geq g_{s,2b}$ as this would imply $\mathbf{w_2} \geq \mathbf{g_s}$ while we know that $w_{2,1} < g_{s,1}$. So we are left with the case

$$w_{2,1\,b} > g_{s,1\,b} \; and \; w_{2,2\,b} < g_{s,2\,b} \tag{13}$$

Vectors $\mathbf{v_1} = \mathbf{w_1} + \mathbf{b_2}$ and $\mathbf{v_2} = \mathbf{w_1} + \mathbf{b_1}$ cannot be in MIN by the choice of $\mathbf{w_1}$. Therefore there exist $\mathbf{v_{1\,s}} = \tilde{A}\tilde{B} \begin{bmatrix} v_{1,1\,s\,b} \\ v_{1,2\,s\,b} \end{bmatrix}$ and $\mathbf{v_{2\,s}} = \tilde{A}\tilde{B} \begin{bmatrix} v_{2,1\,s\,b} \\ v_{2,2\,s\,b} \end{bmatrix}$ such that $\mathbf{v_{1\,s}} \equiv \mathbf{v_1}$, $\mathbf{v_{1\,s}} \lneq \mathbf{v_1}$ and $\mathbf{v_{2\,s}} \equiv \mathbf{v_2}$, $\mathbf{v_{2\,s}} \lneq \mathbf{v_2}$. We must have $v_{1,2\,b\,s} = v_{2,1\,b\,s} = 0$ or else we have contradiction with $\mathbf{w_1} \in$ MIN as $\mathbf{v_{1\,s}} - \mathbf{b_2} \in B_{\mathbb{N}_0}$ or $\mathbf{v_{2\,s}} - \mathbf{b_1} \in B_{\mathbb{N}_0}$. Let $\mathbf{x} = \mathbf{v_{1\,s}} - \mathbf{b_2} = \tilde{A}\tilde{B} \begin{bmatrix} x_{1\,b} \\ x_{2\,b} \end{bmatrix} = \tilde{A}\tilde{B} \begin{bmatrix} v_{1,1\,b\,s} \\ -1 \end{bmatrix}$ and $\mathbf{y} = \mathbf{v_{2\,s}} - \mathbf{b_1} = \tilde{A}\tilde{B} \begin{bmatrix} y_{1\,b} \\ y_{2\,b} \end{bmatrix} = \tilde{A}\tilde{B} \begin{bmatrix} -1 \\ v_{2,2\,b\,s} \end{bmatrix}$. As $\mathbf{v_{1s}} < \mathbf{v_1}$ and $\mathbf{v_{2s}} < \mathbf{v_2}$ we also have $\mathbf{x}, \mathbf{y} < \mathbf{w_1}$ while also $\mathbf{x} \equiv \mathbf{y} \equiv \mathbf{w_1} \equiv \mathbf{w_2}$.

If $x_{1\,b} \geq w_{2,1\,b}$ we reach contradiction as vector

$$\mathbf{x} + (\mathbf{g_s} - \mathbf{w_2}) = \tilde{A}\tilde{B} \begin{bmatrix} x_{1\,b} + g_{s,1\,b} - w_{2,1\,b} \\ x_{2\,b} + g_{s,2\,b} - w_{2,2\,b} \end{bmatrix}$$

is in $B_{\mathbb{N}_0}$ (by (13) and $x_{1\,b} \geq w_{2,1\,b}$), $\mathbf{x} + (\mathbf{g_s} - \mathbf{w_2}) \equiv \mathbf{g_s}$ and $x_1 + g_{s,1} - w_{2,1} < g_{s,1}$ as $x_1 < w_{1,1} < w_{2,1}$ which contradicts with the choice of $\mathbf{g_s}$. Hence

$$x_{1\,b} < w_{2,1\,b} \tag{14}$$

Let's examine possible cases:

Case when $\mathbf{y} \not\geq \mathbf{x}$: If $y_1 \geq x_1$, then we must have $y_2 < x_2$ or else $\mathbf{y} \geq \mathbf{x}$. Yet $y_1 \geq x_1$ and $y_2 < x_1$ by Lemma 11.15 imply $-1 = y_{1\,b} \geq x_{1\,b} \geq 0$ so we cannot have $y_1 \geq x_1$. Then the vector

$$\mathbf{y} + (\mathbf{w_2} - \mathbf{x}) = \tilde{A}\tilde{B} \begin{bmatrix} y_{1\,b} + w_{2,1\,b} - x_{1\,b} \\ y_{2\,b} + w_{2,2\,b} - x_{2\,b} \end{bmatrix} \underset{B}{\geq} 0$$

(by (14) and $x_{2\,b} = -1$) in $B_{\mathbb{N}_0}$, $\mathbf{y} + (\mathbf{w_2} - \mathbf{x}) \equiv \mathbf{w_1} \equiv \mathbf{w_2}$ and $y_1 + w_{2,1} - x_1 < w_{2,1}$ as $y_1 < x_1$. The parallelogram with congruent vertices $\{\mathbf{x}, \mathbf{y}, \mathbf{w_2}, \mathbf{y} + (\mathbf{w_2} - \mathbf{x})\}$ must contain a vector congruent to $\mathbf{g_s}$ as any vector on $B_{\mathbb{Z}}$ can be taken modulus the generating vectors of the parallelogram to obtain a vector inside the parallelogram congruent to it. As all vectors of $B_{\mathbb{Z}}$ on the segment $\mathbf{xy}$ are weighted averages of $\mathbf{x}$ and $\mathbf{y}$ their $\tilde{B}$ coordinates are at least 0 as

$x_{1,2\,b} = y_{2,1\,b} = -1$ (excepting $\mathbf{x}$ and $\mathbf{y}$). Then also all $B_{\mathbb{Z}}$ vectors inside the parallelogram have non-negative $\tilde{B}$ coordinates and so are the vectors on the segments between $\mathbf{y}$ and $\mathbf{y} + (\mathbf{w_2} - \mathbf{x})$ and between $\mathbf{x}$ and $\mathbf{w_2}$. Also as all vertices of the parallelogram have smaller first coordinates than that of $\mathbf{g_s}$, all vectors inside the parallelogram have smaller first coordinates than that of $\mathbf{g_s}$. Then the existing inside the parallelogram vector congruent to $\mathbf{g_s}$ is in $B_{\mathbb{N}_0}$ (it is not congruent to $\mathbf{x} \equiv \mathbf{y}$ as we proved that $\mathbf{w_1} \not\equiv \mathbf{g_s}$) and gives us contradiction with the choice of $\mathbf{g_s}$.

Case when $\mathbf{y} \geq \mathbf{x}$ and $y_{2\,b} \geq w_{1,2\,b}$: Vector

$$\mathbf{w_2} + (\mathbf{y} - \mathbf{w_1}) = \tilde{A}\tilde{B} \begin{bmatrix} w_{2,1\,b} + y_{1\,b} - w_{1,1\,b} \\ w_{2,2\,b} + y_{2\,b} - w_{1,2\,b} \end{bmatrix} \underset{B}{\geq} 0$$

(by (12) and $y_{2\,b} \geq w_{1,2\,b}$) is in $B_{\mathbb{N}_0}$ and is less than $\mathbf{w_2}$ (as $\mathbf{y} \leq \mathbf{w_1}$) which contradicts $\mathbf{w_2} \in$ MIN.

Case when $\mathbf{y} \geq \mathbf{x}$ and $y_{2\,b} < w_{1,2\,b}$: Vector

$$\mathbf{w_1} + (\mathbf{x} - \mathbf{y}) = \tilde{A}\tilde{B} \begin{bmatrix} w_{1,1\,b} + x_{1\,b} - y_{1\,b} \\ w_{1,2\,b} + x_{2\,b} - y_{2\,b} \end{bmatrix} \underset{B}{\geq} 0$$

(as $y_{1\,b} = -1$ and $y_{2\,b} < w_{1,2\,b}$) is in $B_{\mathbb{N}_0}$ and is less than $\mathbf{w_1}$ (as $\mathbf{x} \leq \mathbf{y}$) which contradicts with $\mathbf{w_1} \in$ MIN. □

Now for the second part when $w_{1,1}$ is between $l_{i,1}$ and $l_{i+1,1}$:

Proof. Again let

$$\mathbf{g_1} = \tilde{A} \begin{bmatrix} g_{1,1} \\ g_{1,2} \end{bmatrix} = \tilde{A}\tilde{B} \begin{bmatrix} g_{1,1\,b} \\ g_{1,2\,b} \end{bmatrix} = \mathbf{l_i}$$

$$\mathbf{g_2} = \tilde{A} \begin{bmatrix} g_{2,1} \\ g_{2,2} \end{bmatrix} = \tilde{A}\tilde{B} \begin{bmatrix} g_{2,1\,b} \\ g_{2,2\,b} \end{bmatrix} = \mathbf{l_{i+1}}$$

and

$$\mathbf{g_{s\,1}} = \tilde{A} \begin{bmatrix} g_{s\,1,1} \\ g_{s\,1,2} \end{bmatrix} = \tilde{A}\tilde{B} \begin{bmatrix} g_{s\,1,1\,b} \\ g_{s\,1,2\,b} \end{bmatrix}$$

$$\mathbf{g_{s\,2}} = \tilde{A} \begin{bmatrix} g_{s\,2,1} \\ g_{s\,2,2} \end{bmatrix} = \tilde{A}\tilde{B} \begin{bmatrix} g_{s\,2,1\,b} \\ g_{s\,2,2\,b} \end{bmatrix}$$

be neighboring supporting vectors of $\mathbf{g_1}$ and $\mathbf{g_2}$ respectively with $g_{s\,1,2} = g_{1,2}$ and $g_{s\,2,1} = g_{2,1}$ (that they exist follows from *3* of Lemma 11.14). We are assuming $g_{1,1} \leq w_{1,1} \leq g_{2,1}$.

Since $\mathbf{g_1}$ is an lub-cluster (by Lemma 11.13 and by the assumption on $\mathbf{w_1}$) there exists a MIN vector $\mathbf{w_2} \equiv \mathbf{w_1}$ such that $\mathbf{w_2} \leq \mathbf{g_1}$. Let's assume that $w_{2,1} < w_{1,1}$ as the other case is analogous. As $\mathbf{w_2}$ and $\mathbf{w_1}$ must be incomparable we also have $w_{2,2} > w_{1,2}$ and Lemma 11.15 yields $w_{2,1\,b} < w_{1,1\,b}$ and $w_{2,2\,b} > w_{1,2\,b}$.

It was shown in the previous case that we cannot have $\mathbf{w_1} \leq \mathbf{g_{s\,2}}$ so $w_{1,2} > g_{s\,2,2}$. By Lemma 11.15 this gives $w_{1,1\,b} \leq g_{s\,2,1\,b}$ and $w_{1,2\,b} \geq g_{s\,2,2\,b}$.

Vector

$$\mathbf{w_2} + (\mathbf{g_{s\,2}} - \mathbf{w_1}) = \tilde{A}\tilde{B} \begin{bmatrix} w_{2,1\,b} + g_{s\,2,1\,b} - w_{1,1\,b} \\ w_{2,2\,b} + g_{s\,2,2\,b} - w_{1,2\,b} \end{bmatrix} \underset{B}{\geq} 0$$

(as $w_{1,1\,b} \leq g_{s\,2,1\,b}$ and $w_{2,2\,b} \geq w_{1,2\,b}$) is in $B_{\mathbb{N}_0}$, congruent to $\mathbf{g_{s\,2}}$, $w_{2,1} + g_{s\,2,1} - w_{1,1} < g_{s\,2,1}$ and $w_{2,2} + g_{s\,2,2} - w_{1,2} < w_{2,2} < g_{s\ 1,2}$ (as $w_{2,1} < w_{1,1}$ and $w_{1,2} > g_{s\,2,2}$). So we have contradiction with the choice of $\mathbf{g_{s\,2}}$. □

12 Bounding $|G|$

The following theorem finds a bound on $|G(V)|$ where V is an $n \times (n+2)$ matrix.

Theorem 12.1. *Let j be the smallest positive integer such that $j \cdot b_2$ can be written as a non-negative integer linear combination of $a_1, \ldots, a_n$ and b_1. Then $|G(V)| \leq j$.*

In the case where 0, b_1, and b_2 are linear, it has been proven that $|G| = 1$. Thus we can assume that $B_{\mathbb{R}}$ is a plane.

Definition 12.2. *Given a vector $v \in B_{\mathbb{R}}$ we define the values $v_1, v_2, (v)_1, \ldots,$ and $(v)_n$ to be the real numbers such that $v_1 b_1 + v_2 b_2 = v = (v)_1 a_1 + \cdots (v)_n a_n$.*

Before we prove this theorem, we will prove the correctness of several geometric arguments which will be used. To avoid confusion between the orderings, in this section we will use $\leq_A$ to denote our cone partial ordering. We will now be algebraically defining several geometric concepts. These next several definitions do not depend on the condition $v||_B w$, but many of the proofs are simplified by only defining terms for this case.

Definition 12.3. *Suppose $u, v, w \in B_{\mathbb{R}}$ and $v||_B w$. We say u is* above line $\overleftrightarrow{vw}$ *if $u_2 - v_2 < -\frac{v_2 - w_2}{w_1 - v_1}(u_1 - v_1)$, and u is* below line $\overleftrightarrow{vw}$ *if the inequality is reversed, and u is* on line $\overleftrightarrow{vw}$ *if we have equality.*

From high school algebra, we can see that u is above $\overleftrightarrow{vw}$ if u and 0 lie on the same side of $\overleftrightarrow{vw}$ whether we are looking at the Selmer lattice, or the standard plane. Also, u is above $\overleftrightarrow{vw}$ iff u is above $\overleftrightarrow{wv}$. The naming of *above* is based on the orientation of the Selmer lattice; looking at the standard plane would suggest the opposite definition.

Definition 12.4. *Suppose $u, v, w \in B_{\mathbb{R}}$ and $v||_B w$. We say u is* above line segment $\overline{vw}$ *if u is above $\overleftrightarrow{vw}$, $u_1 \leq \max(v_1, w_1)$, and $u_2 \leq \max(v_2, w_2)$. Similarly, we say u is* below line segment $\overline{vw}$ *if u is below $\overleftrightarrow{vw}$, $u_1 \geq \min(v_1, w_1)$, and $u_2 \geq \min(v_2, w_2)$. Additionally, u is* on line segment $\overline{vw}$ *if u is on $\overleftrightarrow{vw}$, $\max(v_1, w_1) \geq u_1 \geq \min(v_1, w_1)$, and $\max(v_2, w_2) \geq u_2 \geq \min(v_2, w_2)$,*

This definition is best understood geometrically by looking at the Selmer lattice. We see that u is above $\overline{vw}$ iff it is above and to the left of some real point on $\overline{vw}$. Now we will algebraically prove the correctness of several geometric arguments.

Lemma 12.5. *Suppose $u, v, w \in B_{\mathbb{R}}$, $v||_B w$, and u is on or above $\overline{vw}$. Then $u \leq_A lub(v, w)$.*

Proof. WLOG assume $v_2 > w_2$, so that $v_1 < w_1$. If $u_1 < v_1$, then because $u_2 \leq \max(v_2, w_2) = v_2$ we have $u <_B v$ thus $u <_A v \leq_A \text{lub}(v, w)$. Now we can assume u_1 is between v_1 and w_1, and can write $u' = \frac{u_1 - v_1}{w_1 - v_1} w + \frac{w_1 - u_1}{w_1 - v_1} v$ as a weighted average of w and v with non-negative coefficients. Thus for $i = 1, \ldots, n$, we have $(u')_i \leq \max((v)_i, (w)_i)$. We also have $u' = \frac{u_1 - v_1}{w_1 - v_1} w + \frac{w_1 - u_1}{w_1 - v_1} v =$
$\frac{u_1 - v_1}{w_1 - v_1}(w_1 b_1 + w_2 b_2) + \frac{w_1 - u_1}{w_1 - v_1}(v_1 b_1 + v_2 b_2) =$
$\left(\frac{u_1 - v_1}{w_1 - v_1} w_1 + \frac{w_1 - u_1}{w_1 - v_1} v_1\right) b_1 + \left(\frac{u_1 - v_1}{w_1 - v_1} w_2 + \frac{w_1 - u_1}{w_1 - v_1} v_2\right) b_2 =$
$\left(\frac{u_1 w_1 - u_1 v_1}{w_1 - v_1} w_1\right) b_1 + \left(\frac{u_1 - v_1}{w_1 - v_1} w_2 - \frac{u_1 - v_1}{w_1 - v_1} v_2 + \frac{w_1 - v_1}{w_1 - v_1} v_2\right) b_2 =$
$u_1 b_1 + \left(v_2 + \frac{u_1 - v_1}{w_1 - v_1}(w_2 - v_2)\right) \geq_B u_1 b_1 + u_2 b_2 = u,$
where the inequality is because u is below $\overleftrightarrow{vw}$. Finally, we have $u \leq_B u' \leq_A \text{lub}(v, w)$, thus $u \leq_A \text{lub}(v, w)$. □

Lemma 12.6. *Suppose $u, v, w \in B_{\mathbb{R}}$, $v||_B w$, and u is below $\overline{vw}$. Then $v + w - u$ is above $\overline{vw}$. If u is instead on $\overline{vw}$, then $v + w - u$ is also on $\overline{vw}$.*

Proof. Let $u' = v + w - u$. We know that $u_2 > v_2 - \frac{v_2 - w_2}{w_1 - v_1}(v_1 - u_1)$, $v_2 = v_2 - \frac{v_2 - w_2}{w_1 - v_1}(v_1 - v_1)$, and $w_2 = v_2 - \frac{v_2 - w_2}{w_1 - v_1}(v_1 - w_1)$. Taking the last two minus the first, we see that $u_2' < v_2 - \frac{v_2 - w_2}{w_1 - v_1}(v_1 - u_1')$. Thus u' is above $\overleftrightarrow{vw}$. Also, for $i = 1, 2$ we are given that $u_i \geq \min(v_i, w_i)$, thus $u_i' = v_i + w_i - u_i = \max(v_i, w_i) + \min(v_i, w_i) - u_i \leq \max(v_i, w_i)$. Thus u' is above $\overline{vw}$.

Now suppose instead that u is on $\overline{vw}$. We still have $u_i' \leq \max(v_i, w_i)$, and are given that $u_i' \geq \min(v_i, w_i)$. We can add the same three relations as before, except in this case they are all three equalities. Thus $u_2' = v_2 - \frac{v_2 - w_2}{w_1 - v_1}(v_1 - u_1')$, and u' is on $\overline{vw}$. □

Definition 12.7. *We will define a complete ordering of the vectors, called the row ordering, in $B_{\mathbb{N}_0}$ where $c >_{row} c'$ if either $c_2 > c_2'$ or both $c_2 = c_2'$ and $c_1 > c_1'$. Define $\max_{row}(N)$ to be the element of N maximal with respect to $\leq_{row}$. Given $g \in G$ there are possibly many complete sets of residues N from $B_{\mathbb{N}_0}$ such that $g = lub(N) - A_1$. We call N a* minimal row representation *of g if $\max_{row}(N)$ is minimized.*

Lemma 12.8. *For all $g \in G$ there exists a row minimal representation of g contained in the Selmer lattice.*

Proof. By Theorem 1.6 there exists at least one complete set of residues N in $MIN \subset B_{\mathbb{N}_0}$ such that $g = \text{lub}(N) - A_1$. Let N be a row minimal representation of g. For each $w \in N$ associate a w' in the Selmer diagram from the same residue class such that $w \geq_B w'$. Such a w' will always exist because if w is significant, it is in the Selmer lattice, and if w is insignificant, we have $w \geq_B w - z$ for some zero z. Let N' be the set of these associates. Now $\text{lub}(N) - A_1 \geq \text{lub}(N') - A_1$ is complete. So $\text{lub}(N) - A_1 = \text{lub}(N') - A_1$, and N' is a row minimal representation for g from the Selmer lattice. □

Lemma 12.9. *If $lub(N_1) - A_1 \in G$ and for some complete set of residues $N_2 \subset B_{\mathbb{N}_0}$ we have $lub(N_2) \leq_A lub(N_1)$, then $lub(N_2) = lub(N_1)$.*

Proof. For each $w \in N_2$ associate a $w' \in MIN$ from the same residue class such that $w \geq_A w'$. Let $N_2' \subset MIN$ be the set of these associates. Now $\text{lub}(N_2) - A_1 \geq \text{lub}(N_2') - A_1$ is complete by Theorem 4.1. But $\text{lub}(N_1) - A_1$ is a minimal complete point, so we have $\text{lub}(N_2) = \text{lub}(N_1)$. □

Lemma 12.10. *Let g and $g' \in G$. Let N and N' be minimal row representations from the Selmer lattice of g and g' respectively. Suppose that $\max_{row}(N)$ and $\max_{row}(N')$ are in the same row. Then $g = g'$.*

Proof. By Lemma 12.8, such a N and N' exist. Suppose that N and N' are not equal but have k elements in common. We will show that N and N' could have been chosen to have $k+1$ elements in common. Let $m = \max_{\text{row}}(N)$ and $m' = \max_{\text{row}}(N')$. Let $v \in N \backslash N'$ and let $v' \in N'$ with $v' \equiv v$. We have $v||_B v'$ so WLOG assume that $v_1 > v_1'$.

Case 1: $m \neq m'$. Because $m_2 = m_2'$ we may assume WLOG, that $m <_B m'$. Let $w \in N$ such that $w \equiv m'$. Because $m' > \max_{\text{row}}(N)$ we have $m' \neq w$, and thus $m'||_B w$. Now $m_2' > w_2$ and $w_1 > m_1'$. Now consider $w' = w + m - m'$. Both $w_2' = w_2$ and $w_1' = m_1 + (w_1 - m_1')$ are in $\mathbb{N}_0$, so $w' \in B_{\mathbb{N}_0}$. Also $w' \leq w \leq \text{lub}(N)$. Thus $\text{lub}(w', N \backslash m) \leq \text{lub}(w', N) = \text{lub}(N)$. By Lemma 12.9, $\text{lub}(w', N \backslash m) = \text{lub}(N)$, which contradicts the row minimality of N.

Case 2: $m = m'$ and $v <_B m$. We can replace v' with v in N' without changing $\text{lub}(N')$, by Lemma 12.9. Now the new N' and N have $k+1$ elements in common. The case where $m = m'$ and $v' <_B m$ is equivalent.

Case 3: $m = m'$ and v' is above or on $\overleftrightarrow{mv}$. We have $v_2' \leq m_2$ and $v_1' \leq v_1$. Thus v' is above $\overline{mv}$. By Lemma 12.5, $v' \leq \text{lub}(m, v)$. Now $\text{lub}(N) = \text{lub}(v', N) \geq \text{lub}(v', N \backslash v)$, and by Lemma 12.9, $\text{lub}(N) = \text{lub}(v', N \backslash v)$. Now $\{v', N \backslash v\}$ and N' have $k+1$ elements in common.

Case 4: $m = m'$ and v' is below $\overleftrightarrow{mv}$. We can assume that we are not in case 2, so $v'||_B m$. Thus $v_1' > m_1$ and $v_2' < v_2$ so v' is below $\overline{mv}$. By Lemma 12.6, $m + v - v'$ is above $\overline{mv}$ and by Lemma 12.5, $m + v - v' \leq \text{lub}(m, v)$. Notice that $m \equiv m + v - v'$. Now $\text{lub}(N') = \text{lub}(m + v - v', N') \geq \text{lub}(m + v - v', N' \backslash m)$ and by Lemma 12.9, $\text{lub}(N') = \text{lub}(m + v - v', N' \backslash m)$, which contradicts the row minimality of N'.

Thus whenever N and N' are not equal, we can increase the cardinality of their intersection. Applying this argument repeatedly, we see that we can choose $N = N'$, and thus $g = g'$. □

Now we will prove Theorem 12.1.

Proof. Let $g \in G$. Let N be a row minimal representation of g. Let $m = \max_{\text{row}} N$. Suppose for contradiction that $m_2 \geq j$. We know that there exist non-negative integers c_1, c_2, c_3 such that $jb_2 = c_1a_1 + c_2a_2 + c_3b_1$. Now $m = m_1b_1 + m_2b_2 = c_1a_1 + c_2a_2 + (c_3 + m_1)b_1 + (m_2 - j)b_2$. By replacing m with $(c_3 + m_1)b_1 + (m_2 - j)b_2$, we see that N is not row maximal, and thus $m_2 < j$. The possible values for m_2 are $0, 1, \ldots, j-1$. But no two g-vectors can share an m_2 value by Lemma 12.10. Thus $|G| \leq j$. □

This bound is based on all of the generating vectors. As a corollary, we immediately see that $|A|$ alone can bound $|G|$.

Corollary 12.11. *Let $m = 2$. Then $|G| \leq |A|$.*

Proof. Addition mod A is a group of order $|A|$, so $|A|b_2 \equiv 0$, and $|A|b_2 \geq 0$. Thus $|A|b_2 \in A_{\mathbb{N}_0} \subset M_{\mathbb{N}_0}$. Defining j as in Theorem 12.1, we see that $|G| \leq j \leq |A|$. □

13 Clustering

Definition 13.1. *Define* h-vectors *to be minimal g-complete vectors with respect to cone ordering on $\mathbb{Z}^n$.*

Given coordinates of one g-vector we can find all h-vectors which are strictly inside its cone.

First we need some classification of lines parallel to $\mathbf{a_1}$ or $\mathbf{a_2}$ on the lattice. If either $\mathbf{a_1}$ or $\mathbf{a_2}$ have GCD of their coordinates not equal to 1, we factor this GCD out and obtain a pair of vectors with relatively prime coordinates. When coordinates are relatively prime, it is easier for us to describe the integral points on lines parallel to $\mathbf{a_1}$ and $\mathbf{a_2}$. To these vectors we shall further refer as $\mathbf{a_{1\,r}}$ and $\mathbf{a_{2\,r}}$. The matrix composed of these new vectors shall be referred to as reduced A matrix and denoted A^r. To avoid confusion with orientation, let $\mathbf{a_{2\,r}}$ have a steeper slope than $\mathbf{a_{1\,r}}$.

Equation of a line parallel to $\mathbf{a_{1\,r}}$ and passing through an integral point (x_1, y_1) is $a_{1,2\,r}(x - x_1) - a_{1,1\,r}(y - y_1) = 0$. This line intersects $0y$ axis at the point $(0, y_1 - \frac{a_{1,2\,r}x_1}{a_{1,1\,r}}) = (0, \frac{a_{1,1\,r}y_1 - a_{1,2\,r}x_1}{a_{1,1\,r}})$. Thus we can classify each line

parallel to $\mathbf{a_{1\,r}}$ by the integer N which we will call *id number* with respect to origin.

Line equation with id N can be rewritten as $a_{1,2\,r}x - a_{1,1\,r}(y - \frac{N}{a_{1,1\,r}}) = 0$. Then integral points on the line can be described as follows: $x = ka_{1,1\,r} - a_{1,2\,r}^{-1}N$ and $y = \frac{N}{a_{1,1\,r}} + \frac{a_{1,2\,r}(ka_{1,1\,r} - a_{1,2\,r}^{-1}N)}{a_{1,1\,r}} = ka_{1,2\,r} + N\frac{1-a_{1,2\,r}a_{1,2\,r}^{-1}}{a_{1,1\,r}}$ where the inverses are taken modulus $a_{1,1\,r}$ (and so we mean in later parts of the document; inverse exists as $GCD(a_{1,1\,r}, a_{1,2\,r}) = 1$) and $k \in \mathbb{Z}$. If we make the translation of basis to the one defined by reduced A matrix the points will be described as follows: $x = k - N\frac{a_{1,2\,r}^{-1}|A^r| + a_{2,1\,r}}{a_{1,1\,r}|A^r|}$, $y = \frac{N}{|A^r|}$ with $|A^r| = a_{1,1\,r}a_{2,2\,r} - a_{1,2\,r}a_{2,1\,r}$. Notice that $l = -\frac{a_{1,2\,r}^{-1}|A^r| + a_{2,1\,r}}{a_{1,1\,r}}$ is an integer. Thus $x = k + N\frac{l}{|A^r|}$, $y = \frac{N}{|A^r|}$!.

Let $g = \begin{bmatrix} g_1 \\ g_2 \end{bmatrix} = A^r \begin{bmatrix} g_1' \\ g_2' \end{bmatrix}$ denote a g-vector. It is straightforward to find the greatest integral point with the same $a_{2\,r}$ coordinate as g and less than g. First we find the id of the line parallel to $a_{1\,r}$ passing through g with respect to origin: $a_{1,1\,r}g_2 - a_{1,2\,r}g_1$. Denoting the point $\mathbf{h} = A^r \begin{bmatrix} h_1' \\ h_2' \end{bmatrix}$, h_1' must be maximal such that $h_1' = k + (a_{1,1\,r}g_2 - a_{1,2\,r}g_1)\frac{l}{|A^r|} \leq g_1'$. From this we have $k = \lfloor g_1' - (a_{1,1\,r}g_2 - a_{1,2\,r}g_1)\frac{l}{|A^r|} \rfloor$ so

$$\mathbf{h} = A^r \begin{bmatrix} h_1' \\ h_2' \end{bmatrix} = A^r \begin{bmatrix} \lfloor g_1' - (a_{1,1\,r}g_2 - a_{1,2\,r}g_1)\frac{l}{|A^r|} \rfloor + (a_{1,1\,r}g_2 - a_{1,2\,r}g_1)\frac{l}{|A^r|} \\ g_2 \end{bmatrix}$$

Analogously we find the greatest integral point less than $\mathbf{g}$ and with the same $a_{1\,r}$ coordinate as $\mathbf{g}$:

$$\mathbf{f} = A^r \begin{bmatrix} f_1' \\ f_2' \end{bmatrix} = A^r \begin{bmatrix} g_1' \\ \lfloor g_2' - (a_{2,2\,r}g_1 - a_{2,1\,r}g_2)\frac{m}{|A^r|} \rfloor + (a_{2,2\,r}g_1 - a_{2,1\,r}g_2)\frac{m}{|A^r|} \end{bmatrix}$$

where $m = -\frac{a_{2,1\,r}^{-1}|A^r| + a_{1,2\,r}}{a_{2,2\,r}}$ (this time only the inverse is taken modulus $a_{2,2\,r}$).

Now if we move origin to h for our convenience, it is easy to calculate coordinates of g with respect to h. Next with respect to this new origin we consider the lines parallel to $\mathbf{a_{1\,r}}$. They will be inside the cone of g if and only if their id number is positive as id has the same sign as the $a_{2\,r}$ coordinate of points on the line. Also the ids are bounded by the id of the line passing through $\mathbf{f} + \mathbf{a_{2\,r}}$ which is exactly $(f_2' + 1)|A^r| = M$. As we increase the id N

while $0 \leq N \leq (f_2^{'}+1)|A^r|$ for each line with the id we find the point suspect to be an h-vector – the least point on the line which is inside the cone: Recall that the general form of $a_{1\,r}$ coordinate of an integral point on the line with N id is $k + N\frac{l}{|A^r|}$. If the coordinate is greater than 1, which is the coordinate of $\mathbf{h} + \mathbf{a_{1\,r}}$, the point cannot be an h-vector. Also the coordinate cannot be negative and still! be inside the cone of $\mathbf{g}$. This leaves the $a_{1\,r}$ coordinate only to be $\frac{mod(lN,|A^r|)}{|A^r|}$. To decide whether the point is an h-vector, compare its $a_{1\,r}$ coordinate with the $a_{1\,r}$ coordinate of the previous h-vector obtained by this process (if this is the first line we need to compare with the $a_{1\,r}$ coordinate of $\mathbf{h} + \mathbf{a_{1\,r}} = 1$). If it is less than that of the previous and still greater than that of $\mathbf{f} + \mathbf{a_{2\,r}} = \frac{M}{|A^r|}$, it is an h-vector; otherwise it isn't an h-vector. So if we define the sequence of $a_{1\,r}$ coordinates of suspect h-vectors multiplied by $|A^r|$, $\{mod(lN, |A^r|)\}_{N=1}^{N<(f_2^{'}+1)|A^r|}$ (*mod* function here returns remainders from 1 to $|A^r|$), the strictly decreasing subsequence obtained from it by choosing only terms which are less than the previously chosen terms and greater than $M = (f_1^{'} + 1)|A^r|$, will correspond to the h-vectors which are strictly inside the cone of $\mathbf{g}$. As the number of terms in such sequences is bounded by $|A^r| - 2$ we can have no more than $|A^r| - 2$ h-vectors strictly inside the cone. However, $|A^r| - 2$ is not achievable for all A^r matrices and we can give a better bound if we use l: First $\lfloor \frac{|A^r|}{mod(-l,|A^r|)} \rfloor$ terms will be decreasing and the rest must be less than $mod(\lfloor \frac{|A^r|}{mod(-l,|A^r|)} \rfloor l, |A^r|)$ which yields:

Theorem 13.2. *Given a reduced matrix A^r, the number of h-vectors contained strictly inside a cone of a g-vector is bound by $\lfloor \frac{|A^r|}{d} \rfloor + mod(|A^r|, d) - 1$ where $d = mod(\frac{a_{1,2\,r}^{-1}|A^r| + a_{2,1\,r}}{a_{1,1\,r}}, |A^r|)$*

14 Unbound

Definition 14.1. *For a vector $\mathbf{v}$ let v_i denote i-th coordinate with respect to the standard orthonormal basis and let $v_i^{'} = (A^{-1}\mathbf{v})_i$. For example, for $\mathbf{g_k}$, $g_{k,i}^{'} = (A^{-1}\mathbf{g_k})_i$.*

Definition 14.2. *Define e-class to mean equivalence class with respect to A. If we have a generating vector $\mathbf{b_1}$ we can assign a residue number $t(x)$ $(0 \leq t(x) \leq |A| - 1)$ to each vector $\mathbf{x}$ so that $\mathbf{x} \equiv t(x)\mathbf{b_1}\, mod(A)$. This number will correspond to an e-class and we shall further refer to e-classes by these numbers.*

Definition 14.3. *For a vector* $\mathbf{g}$*, we say that it* contains *vector* $\mathbf{x}$ *when* $\mathbf{g} + \mathbf{A_1} \geq \mathbf{x}$ *which is equivalent to* $g_i^{'} + 1 \geq x_i^{'}$ *for every* i*. We say that it contains a residue class when it contains a vector from this residue class.*

Theorem 14.4. *Let* $\mathbf{b_1}$ *be a generator of all residue classes and* $\mathbf{b_2}$ *be such that* $\mathbf{b_2} \equiv t\mathbf{b_1}\, mod(A)\, (1 \leq t \leq |A| - 1)$ *while* $b_{2,2}^{'} > (|A| - 1)b_{1,2}^{'}$*. Then for* $k(0 < k \leq min(\frac{|A|}{|A|-t}, \frac{tb_{1,1}^{'}}{(|A|-t)b_{1,1}^{'}+b_{2,1}^{'}}))$ *the following will be g-vectors:*

$$\mathbf{g_0} = (|A| - 1)\mathbf{b_1} - \mathbf{A_1},$$

$$\mathbf{g_k} = lub((|A| - k(|A| - t) - 1)\mathbf{b_1}, k\mathbf{b_2} + (|A| - t - 1)\mathbf{b_1}) - \mathbf{A_1}$$

Proof. Define $s = |A| - t$.

From the restriction on k we have $k(sb_{1,1}^{'} + b_{2,1}^{'}) \leq (|A| - s)b_{1,1}^{'}$ or $kb_{2,1}^{'} + (s-1)b_{1,1}^{'} \leq (|A| - ks - 1)b_{1,1}^{'}$.

Also as $b_{2,2}^{'} > (|A| - 1)b_{1,2}^{'}$, $kb_{2,2}^{'} + (s-1)b_{1,2}^{'} \geq b_{2,2}^{'} \geq (|A| - 1)b_{1,2}^{'} \geq (|A| - ks - 1)b_{1,2}^{'}$.

Putting this together we have $\mathbf{g_k} = A \begin{bmatrix} g_{k,1}^{'} \\ g_{k,2}^{'} \end{bmatrix} = lub((|A| - k(|A| - t) - 1)\mathbf{b_1}, k\mathbf{b_2} + (|A| - t - 1)\mathbf{b_1}) - \mathbf{A_1} = A \begin{bmatrix} (|A| - ks - 1)b_{1,1}^{'} - 1 \\ kb_{2,2}^{'} + (s-1)b_{1,2}^{'} - 1 \end{bmatrix}$

First we prove that $\mathbf{g_k}$ are g-complete.

As $\mathbf{b_1}$ is a generator $(|A|-1)\mathbf{b_1} - \mathbf{A_1}$ is g-complete. Also since $\mathbf{g_k} + \mathbf{A_1} \geq (|A| - 1 - ks)\mathbf{b_1} \geq (|A| - 1 - ks - i)\mathbf{b_1}$, $(0 \leq i \leq |A| - 1 - ks)$, $\mathbf{g_k}$ contains the following e-classes: $\{0, 1, ..., |A| - 1 - ks\}$ and as $\mathbf{g_k} + \mathbf{A_1} \geq k\mathbf{b_2} + (s-1)\mathbf{b_1} \geq i\mathbf{b_2} + j\mathbf{b_1}$, $(1 \leq i \leq k,\, 0 \leq j \leq s-1)$, it also contains $\{|A| - ks, |A| - ks + 1, ..., |A| - (k-1)s - 1, |A| - (k-1)s, |A| - (k-1)s + 1, ..., |A| - (k-2)s - 1, ..., |A| - s, |A| - s + 1, ..., |A| - 1\}$ and is g-complete. (here we are using Theorem 4.1)

Second we prove that $\mathbf{g_k}$ are minimal g-complete.

For $\mathbf{g_0}$, $\mathbf{g_0} + \mathbf{A_1} \not\geq i\mathbf{b_2} + j\mathbf{b_1}$, $(i > 0)$ as $b_{2,2}^{'} > (|A| - 1)b_{1,2}^{'}$, so $\mathbf{g_0} = lub(\mathbf{0}, \mathbf{b_1}, ..., (|A| - 1)\mathbf{b_1}) - \mathbf{A_1}$ is a g-vector as any vector which is less than $\mathbf{g_0}$ will not contain $|A|$ elements from MIN.

For $\mathbf{g_k}$, elements $(k + i)\mathbf{b_2} + j\mathbf{b_1}$ $(i > 0)$ are not contained by $\mathbf{g_k}$ as $(k + i)b_{2,2}^{'} + jb_{1,2}^{'} \geq kb_{2,2}^{'} + b_{2,2}^{'} > kb_{2,2}^{'} + (|A| - 1)b_{1,2}^{'} > kb_{2,2}^{'} + (s-1)b_{1,2}^{'}$.

Now if we show that $(|A| - ks - 1)\mathbf{b_1}$ and $k\mathbf{b_2} + (s-1)\mathbf{b_1}$ are the only elements of their respective e-classes that are contained by $\mathbf{g_k}$, we will prove that $\mathbf{g_k}$ is a g-vector.

For $i \leq k$ elements $i\mathbf{b_2}+j\mathbf{b_1}$ congruent to $k\mathbf{b_2}+(s-1)\mathbf{b_1}$ are not contained by $\mathbf{g_k}$ because $i\mathbf{b_2}+j\mathbf{b_1} \equiv k\mathbf{b_2}+(s-1)\mathbf{b_1}$ implies $j \equiv s(i-k)+s-1\, mod(|A|)$ or $j = n|A| + s(i-k) + s - 1$ where $n > 0$ as $j \geq 0$ (except when $i = k$, $n \geq 0$). When $i < k$ we have $ib'_{2,1} + jb'_{1,1} \geq jb'_{1,1} \geq (|A| - ks + s - 1)b'_{1,1} > (|A| - ks - 1)b'_{1,1} = g'_{k,1} + 1$ and $\mathbf{g_k}$ doesn't contain $i\mathbf{b_2} + j\mathbf{b_1}$. When $i = k$ we have $i\mathbf{b_2} + j\mathbf{b_1} = k\mathbf{b_2} + (n|A| + s - 1)\mathbf{b_1} \geq k\mathbf{b_2} + (s-1)\mathbf{b_1}$ (for $n > 0$) which proves that $k\mathbf{b_2} + (s-1)\mathbf{b_1}$ is the only element of its e-class that is contained by $\mathbf{g_k}$.

Analogously, for elements $i\mathbf{b_2} + j\mathbf{b_1}$ congruent to $(|A| - ks - 1)\mathbf{b_1}$ are not contained by $\mathbf{g_k}$ because $i\mathbf{b_2} + j\mathbf{b_1} \equiv (|A| - ks - 1)\mathbf{b_1}$ implies $j \equiv s(i-k) - 1\, mod(|A|)$ or $j = n|A|+s(i-k)-1$ where $n > 0$ as $j \geq 0$. This in turn implies that $ib'_{2,1}+jb'_{1,1} \geq jb'_{1,1} \geq (|A|+s(i-k)-1)b'_{1,1} \geq (|A|-ks-1)b'_{1,1} = g'_{k,1}+1$ (we have strict inequality when $i > 0$) which shows that $(|A| - ks - 1)\mathbf{b_1}$ is the only element of its e-class that is contained by $\mathbf{g_k}$. □

Corollary 14.5. *If* $A = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix}$ *and* $\mathbf{b_1} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ *we can have* $max(a_1, a_2)$ *g-vectors.*

Proof. Use Theorem 1 with $t = |A| - 1$, $b_{2,1} = a_1 - 1$, $b_{2,2} = la_2 - 1$ where l is such that $b_{2,2} > (a_1a_2 - 1)b_{1,2}$. □

15 Further Possibilities

On the topic of adjacency:

Explore the structure of blocks in $n > 2$ dimensions.

It is not true, as we at one time considered, that all blocks are either of size n when $|G| \geq n$ or size $|G|$ otherwise. It may be worthwhile to attempt a characterization of these blocks.

On the topic of order and the MIN set:

Let $\alpha(b_i) \in \mathbb{N}$ be the smallest element such that $\alpha(b_i)b_i \in [M - b_i]_{\mathbb{N}_0}$. We define the following set:

$$S'_M = \left\{ \sum_{i=1}^{m} c_i b_i \mid 0 \leq c_i < \alpha(b_i) \right\}$$

Conjecture 15.1. $MIN \subseteq S'_M$

This result would be an improvement on Lemma 3.1. Furthermore, consider $x \in \mathbb{N}^m$ such that Bx is minimal and $Bx \equiv 0 \mod A$. Let X be the set of all such x. We denote the ith coordinate in x as $(x)_i$. Now consider the following set:

$$\overline{S}'_M = \left\{ \sum_{i=1}^{m} c_i b_i \mid (x)_i \leq c_i < \alpha(b_i), \forall x \in X \right\}$$

Consider this rough argument:

Let $v \in \overline{S}'_M \subseteq S'_M$. Then $v = s + \gamma Bx$ where $s \in S'_M \setminus \overline{S}'_M$. Thus

$$v = s + \gamma Bx \cong s + 0\gamma$$

implies that $v \notin MIN$. Therefore $MIN \subseteq S'_M \setminus \overline{S}'_M$.

The idea is that this set $\overline{S}'_M$ contains the elements in S'_M (or simply S_M) that are not in MIN due to this Bx element. We have the following two possible conjectures, the first being a weaker version of the second. In the $n = m = 2$ case, the second possibility seems to be true.

Conjecture 15.2.

- $MIN \subseteq S'_M \setminus \overline{S}'_M$
- $S'_M \setminus \overline{S}'_M = MIN$

On the topic of the Selmer Lattice:

Extend the Selmer Lattice to $m > 2$.

It may be possible to extend Theorem 12.1:

Conjecture 15.3. *Let $m = 3$. Let j_1 be the smallest integer such that $j_1 b_2$ is in $[A|b_1]_{\mathbb{N}_0}$ and let j_2 be the smallest integer such that $j_2 b_3$ is in $[A|b_1|b_2]_{\mathbb{N}_0}$. Then $|G| \leq j_1 j_2$.*

Other conjectures:

The following conjecture concerns the "shape" of the distribution of the g vectors in a monoid.

Conjecture 15.4. *Elements of G are either concave up (with respect to cone ordering) or lie along a line.*