

The Multi-Dimensional Frobenius Problem

J. Amos^a I. Pascu^b V. Ponomarenko^{c,*} E. Treviño^d Y. Zhang^e

^a*Department of Mathematics, Kansas State University*

^b*Department of Mathematics, Wellesley College*

^c*Department of Mathematics, San Diego State University*

^d*Department of Mathematics, Dartmouth College*

^e*Department of Mathematics, Harvard University*

Research supported in part by NSF grant 0097366.

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 .

Key words: Frobenius, coin-exchange, linear Diophantine system

* Corresponding author: vadim123@gmail.com

1 Introduction

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 the book [1], 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 [2] and call the cone *volume*. If each column of B lies in the volume 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. For $x \in \mathbb{R}^n$, we call $x + M_{\mathbb{R} \geq 0} = x + A_{\mathbb{R} \geq 0}$ the cone at x , writing $\text{cone}(x)$.

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, $u \geq v$ 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 $Q = (1/|A|)\mathbb{Z} \subseteq \mathbb{Q}$. 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 *Let $v \in \mathbb{R}^n$. There exists $v^* \in Q^n$ with $[\succ v] = [\succ Av^*]$ and $v \geq Av^*$.*

PROOF. We choose $v^* \in Q^n$ such that $A^{-1}v - v^* = \epsilon = (\epsilon_1, \epsilon_2, \dots, \epsilon_n)$ with $0 \leq \epsilon_i < 1/|A|$. Multiplying by A we get $v - Av^* = A\epsilon$; hence $v \geq Av^*$. We will now show that for $u \in \mathbb{Z}^n$, $u \succ v$ if and only if $u \succ Av^*$. If $u \succ v$, then $u \succ Av^*$ because $u \succ v \geq Av^*$. On the other hand, suppose that $u \succ Av^*$ and $u \not\succ v$. Hence $u - Av^* \in A_{\mathbb{R} > 0}$ and $u - v \in A_{\mathbb{R}} \setminus A_{\mathbb{R} > 0}$. Multiplying by A^{-1} we get $A^{-1}u - v^* \in I_{\mathbb{R} > 0}$ and $A^{-1}u - A^{-1}v \in I_{\mathbb{R}} \setminus I_{\mathbb{R} > 0}$. Therefore, there is some coordinate i with $(A^{-1}u - v^*)_i > 0$ and $(A^{-1}u - A^{-1}v)_i \leq 0$. Because $u \in \mathbb{Z}^n$ and A is an integer matrix, we have $A^{-1}u \in Q^n$; hence in fact $(A^{-1}u - v^*)_i \geq 1/|A|$. Now, $0 \geq (A^{-1}u - A^{-1}v)_i = (A^{-1}u - v^* - (A^{-1}v - v^*))_i = (A^{-1}u - v^*)_i - \epsilon_i \geq 1/|A| - \epsilon_i$. However, this contradicts $\epsilon_i < 1/|A|$.

Let $x, y \in M_{Q \geq 0}$. We write $x = Ax', y = Ay'$, with $x', y' \in (Q^{\geq 0})^n$, define z' via $(z')_i = \max((x')_i, (y')_i)$, and set $\text{lub}(x, y) = Az'$. We have $\text{lub}(x, y) \in M_{Q \geq 0}$, although in general $\text{lub}(x, y) \notin M_{\mathbb{N}_0}$ (even if $x, y \in M_{\mathbb{N}_0}$) because $A^{-1}B$ need not have integer entries.

For $u \in M_Q$, we set $V(u) = (u + A_{Q \cap (0,1]}) \cap \mathbb{Z}^n$. It was known to Dedekind [3] that $|V(u)| = |A|$, and that $V(u)$ is a complete set of coset representatives mod A (as restricted to \mathbb{Z}^n). Note that u is complete if and only if $V(u) \subseteq M_{\mathbb{N}_0}$.

The following equivalent conditions on M generalize the one-dimensional notion of relatively prime generators. Portions of the following have been repeatedly rediscovered [4,5,2,6,7]. We assume henceforth, unless otherwise noted, that M possesses these properties. We call such M *dense*.

Theorem 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.

PROOF. The proof follows the plan (1) \leftrightarrow (4) \leftrightarrow (3) \leftrightarrow (2) \leftrightarrow (6) \leftrightarrow (5).

(1) \leftrightarrow (4): Let $g \in G$. Choose $v \in [\succ g]$ far enough from the boundaries of the cone so that $v + e_i$ is also in $[\succ g]$ for all unit vectors e_i . Because g is complete, v and $v + e_i$ are all in $M_{\mathbb{N}_0}$. The other direction is proved in [2].

(Proposition 5).

(4) \leftrightarrow (3): For one direction, write $e_i = Mf_i$. Set $k = \max_i \|f_i\|_{\infty}$. Set $v = Mk^n$. We see that $v + e_i = M(k^n + f_i) \subseteq M_{\mathbb{N}_0}$. For the other direction, let $1 \leq i \leq n$. Write $v = Mw$, $v + e_i = Mw'$, where $w, w' \in \mathbb{N}_0^n$. Hence, $e_i = M(w' - w) \subseteq M_{\mathbb{Z}}$.

(3) \leftrightarrow (2): Let $v \in \mathbb{Z}^n$; write $v = (v_1, v_2, \dots, v_n)$. Write $e_i = Mf_i$, for $f_i \in \mathbb{Z}^n$. Then $v = M \sum v_i f_i$, as desired. The other direction is trivial.

(2) \leftrightarrow (6): We place M in Smith normal form: write $M = LNR$, where N is a

diagonal matrix of the same dimensions as M , and L, R are square matrices, invertible over the integers. The diagonal entries of N are the elementary divisors of M . We therefore have that (2) $\leftrightarrow N = [I|0] \leftrightarrow$ (6).

(6) \leftrightarrow (5): The product of the elementary divisors is known (see, for example, [8]) to be the absolute value of the GCD of all $n \times n$ minors of M . If they are all one, their product is one. Conversely, if their product is one, then they must all be one since they are all nonnegative integers.

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; in [9] it was shown that $f = g + m^T 1$. A similar situation holds in the vector context.

Proposition 3 *Call v f-complete if $[\succ v] \subseteq M_{\mathbb{N}}$. Set F to be the set of all \succeq -minimal f-complete vectors. Then $F = G + M_1$.*

PROOF. It suffices to show that $v \in Q^n$ is complete if and only if $v + M_1$ is f-complete. Note that an integral vector $u \in [\succ v + M_1]$ if and only if $u \succ v + M_1$ if and only if $(u - M_1) - v \in M_{\mathbb{R} \geq 0}$ if and only if $(u - M_1) \succ v$ if and only if $(u - M_1) \in [\succ v]$. Now, suppose that v is complete. Let $u \in [\succ v + M_1]$; hence $(u - M_1) \in [\succ v] \subseteq M_{\mathbb{N}_0}$ and therefore $u \in M_{\mathbb{N}}$. So $v + M_1$ is f-complete. On the other hand, suppose that $v + M_1$ is f-complete. Let $(u - M_1) \in [\succ v]$; hence $u \in [\succ v + M_1] \subseteq M_{\mathbb{N}}$. Hence $u - M_1 \subseteq M_{\mathbb{N}} - M_1 = M_{\mathbb{N}_0}$, and v is complete.

Having established the notation and basic groundwork for the problem, we now present two useful techniques: the method of critical elements, and the MIN method. Each will be shown to characterize G .

2 The Method of Critical Elements

For a vector u and $i \in [1, n]$, let $C^i(u) = \{v : v \in \mathbb{Z}^n \setminus M_{\mathbb{N}_0}, v = u + Aw, (w)_i = 0, (w)_j \in (0, 1] \text{ for } j \neq i\}$. This set captures all lattice points missing from the monoid, in the i^{th} face of $\text{cone}(u)$, that are minimal mod A . Let $C(u) = \bigcup_{i \in [1, n]} C^i(u)$, a disjoint union of finite sets. 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 4 *Let x be complete. The following are equivalent.*

- (1) $x \in G$
- (2) *Each face of $\text{cone}(x)$ contains at least one lattice point not in the monoid.*
- (3) $C^i(x) \neq \emptyset, \forall i \in [1, n]$.

PROOF. We write $x = Ax'$. For each $i \in [1, n]$, set $x^i = x - (1/|A|)Ae_i$ and $S_i = [\succ x^i] \setminus [\succ x]$. Observe that $S_i = \{Au \in \mathbb{Z}^n : (u)_j > (x')_j \text{ (for } j \neq i), (u)_i = (x')_i\}$; the S_i are the lattice points in the i^{th} face of $\text{cone}(x)$.

- (1) \rightarrow (2) If $S_i \subseteq M_{\mathbb{N}_0}$, then x^i is complete, which is violative of $x \in G$.
- (2) \rightarrow (3) Pick any minimal $y \in S_i \setminus M_{\mathbb{N}_0}$. Suppose that $(A^{-1}(y - x))_j \notin (0, 1]$ for $j \neq i$; in this case, $y - Ae_j$ would also be in $S_i \setminus M_{\mathbb{N}_0}$, violating the minimality of y . Hence $y \in C^i(x)$, and thus $C^i(x) \neq \emptyset$.
- (3) \rightarrow (1) If $x^* < x$, then $x^* \leq x^i$ for some i . But no x^i is complete; hence x^* is not complete. Thus x is \geq -minimal complete and thus $x \in G$.

Critical elements can also test for uniqueness of Frobenius vectors. Set $\bar{e}_i = \bar{1} - e_i = (1, 1, \dots, 1, 0, 1, 1, \dots, 1)$.

Theorem 5 *Let $g \in G$. Then $|G| = 1$ if and only if for each $i \in [1, n]$ there*

is some $c^i \in C^i(g)$ with $c^i + kA\bar{e}_i \notin M_{\mathbb{N}_0}$ for all $k \in \mathbb{N}_0$.

PROOF. Suppose that for each $i \in [1, n]$ there is some $c^i \in C^i(g)$ with $c^i + kA\bar{e}_i \notin M_{\mathbb{N}_0}$ for all k . Let $g' \in G$. If $g' \neq g$, then for some i we must have $(A^{-1}g')_i < (A^{-1}g)_i$. As $k \rightarrow \infty$, $(A^{-1}c^i + k\bar{e}_i)_j \rightarrow \infty$ (for $j \neq i$). But also $(A^{-1}c^i + k\bar{e}_i)_i = (A^{-1}g)_i$ for all k . Therefore, for some k we have $c^i + kA\bar{e}_i \succ g'$. Hence g' is not complete, which is violative of assumption. Hence $|G| = 1$.

Now, let $g \in G$ be unique, let $i \in [1, n]$ be such that each $c^i \in C^i(g)$ has some $k(i)$ with $c^i + k(i)A\bar{e}_i \in M_{\mathbb{N}_0}$. If $c^i + kA\bar{e}_i \in M_{\mathbb{N}_0}$, then $c^i + k'A\bar{e}_i \in M_{\mathbb{N}_0}$ for any $k' \geq k$; hence because $|C^i(g)| < \infty$ there is some $K \in \mathbb{N}_0$ with $c^i + KA\bar{e}_i \in M_{\mathbb{N}_0}$ for all $c^i \in C^i(g)$. Now, set $g^* = g + (K + 1)A\bar{e}_i - (1/|A|)Ae_i$ and $S = [\succ g^*] \setminus [\succ g] \subseteq \{u \in \mathbb{Z}^n : (A^{-1}(u - g))_i = 0, (A^{-1}(u - g))_j \geq K + 1 (j \neq i)\}$.

We now show that $S \setminus M_{\mathbb{N}_0}$ is empty; otherwise, choose u therein. Set $u' = u - Aa$, where $(a)_i = 0$ and $(a)_j = \begin{cases} \lfloor (A^{-1}(u - g))_j \rfloor & (A^{-1}(u - g))_j \notin \mathbb{Z} \\ (A^{-1}(u - g))_j - 1 & (A^{-1}(u - g))_j \in \mathbb{Z} \end{cases}$ (for $j \neq i$). We must have $u' \in \mathbb{Z}^n \setminus M_{\mathbb{N}_0}$, since otherwise $u \in M_{\mathbb{N}_0}$. We also have $(A^{-1}(u' - g))_i = 0, (A^{-1}(u' - g))_j \in (0, 1]$ for $j \neq i$; hence $u' \in C^i(g)$. But then $u' + KA\bar{e}_i \in M_{\mathbb{N}_0}$ and hence $u \in M_{\mathbb{N}_0}$ since $u - (u' + KA\bar{e}_i) \in A_{\mathbb{N}_0}$. Hence $S \subseteq M_{\mathbb{N}_0}$ and g^* is complete. Now take $g' \in G$ with $g' \leq g^*$. We have $(A^{-1}g')_i \leq (A^{-1}g^*)_i < (A^{-1}g)_i$ and hence $g' \neq g$, which is violative of hypothesis.

We now give two more results using this method. The first generalizes a one-dimensional reduction result in [10] which is very important because it allows the assumption that the generators are pairwise relatively prime. The vector generalization unfortunately does not permit an analogous assumption in general.

Theorem 6 *Let $d \in \mathbb{N}$ and let simplicial $M = [A|B]$. Suppose that $N = [A|dB]$ is dense. Then M is dense, and $G(N) = dG(M) + (d-1)A_1$.*

PROOF. Each $n \times n$ minor of M divides a corresponding minor of N ; hence M is dense. Further, d divides all minors of N apart from $|A|$; hence $\gcd(|A|, d) = 1 = \gcd(|A|^2, d)$. We can therefore pick $d^* \in \mathbb{N}$ with $d^*d \in 1 + |A|^2\mathbb{N}_0$. For any $v \in Q^n$, we observe that $d^*dv - v \in \mathbb{N}_0|A|^2Q^n = \mathbb{N}_0|A|\mathbb{Z}^n \subseteq A\mathbb{Z}$; hence $d^*dv \equiv v$. Set $\theta(x) = dx + (d-1)A1^n$. We will show for any $x \in Q^n$ that $x \in M_{\mathbb{N}_0}$ if and only if $\theta(x) \in N_{\mathbb{N}_0}$ (in particular, if $\theta(x) \in N_{\mathbb{N}_0}$, then $x \in \mathbb{Z}^n$). One direction is trivial; for the other, assume $\theta(x) \in N_{\mathbb{N}_0}$. We have $dx + dA1^n = A(y + 1^n) + dBz$, for $y \in \mathbb{N}_0^n, z \in \mathbb{N}_0^m$. We observe that $x + A1^n = A(1/d)(y + 1^n) + Bz$, so $x + A1^n \geq Bz$. Also, $d^*d(x + A1^n) = Ad^*(y + 1^n) + d^*dBz$; hence $x + A1^n \equiv Bz$. Therefore $x + A1^n - Bz = Aw$ for some $w \in \mathbb{N}_0^n$. Further, $w = (1/d)(y + 1^n)$ so in fact $w \in \mathbb{N}^n$. Hence, $x = A(w - 1^n) + Bz \in M_{\mathbb{N}_0}$.

Next, we show that x is M -complete if and only if $\theta(x)$ is N -complete. First suppose that $\theta(x)$ is N -complete. Let $u \in [\succ x]$; we have $\theta(u) \in [\succ \theta(x)] \subseteq N_{\mathbb{N}_0}$. Hence $u \in M_{\mathbb{N}_0}$ so x is M -complete. Now suppose that x is M -complete. Let $u \in V(\theta(x))$. Set $u' \in V(x)$ with $du' \equiv u$. We have $u = \theta(x) + A\epsilon, u' = x + A\epsilon'$, where $\epsilon, \epsilon' \in (0, 1]^n$. We compute $u - du' = A\omega$, where $\omega = d(1^n - \epsilon') + (\epsilon - 1)$. Because $u \equiv du'$ we have $\omega \in \mathbb{Z}^n$; further, the restrictions on ϵ, ϵ' force $\omega \in \mathbb{N}_0^n$. We have $u' \in M_{\mathbb{N}_0}$ since x is M -complete. But then $du' \in N_{\mathbb{N}_0}$, and thus $u = du' + A\omega \in N_{\mathbb{N}_0}$. Hence $V(\theta(x)) \subseteq N_{\mathbb{N}_0}$ and thus $\theta(x)$ is N -complete.

Let $g \in G(M)$; we will show that $\theta(g) \in G(N)$. Let $i \in [1, n]$; by Theorem 4, there is $u \in [0, 1]^n$ with $u_i = 0, u_j > 0$ (for $j \neq i$), such that $g + Au \in \mathbb{Z}^n \setminus M_{\mathbb{N}_0}$. We have $\theta(g + Au) \in \mathbb{Z}^n \setminus N_{\mathbb{N}_0}$. We write $\theta(g + Au) = d(g + Au) + (d-1)A1^n = \theta(g) + Adu$. Write $du = u' + u''$ where $(u')_i = 0, (u')_j \in (0, 1]$, and $u'' \in \mathbb{N}_0^n$.

We have $\theta(g) + Au' \in C^i(\theta(g))$; considering all i gives $\theta(g) \in G(N)$. Now, let $g \in G(N)$; we will show that $\theta^{-1}(g) = (1/d)(g - (d-1)A1^n) \in G(M)$. We again apply Theorem 4 to get an appropriate u with $g + Au \in \mathbb{Z}^n \setminus N_{\mathbb{N}_0}$. Note that $g + A(u + d1^n) \in N_{\mathbb{N}_0}$ hence $\theta^{-1}(g + A(u + d1^n)) = (1/d)(g + Au + dA1^n - (d-1)A1^n) = \theta^{-1}(g) + (1/d)Au + A1^n \in M_{\mathbb{N}_0} \subseteq \mathbb{Z}^n$. Thus, $\theta^{-1}(g + Au) = (1/d)(g + Au - (d-1)A1^n) = \theta^{-1}(g) + (1/d)Au \in \mathbb{Z}^n$. We therefore have $\theta^{-1}(g + Au) \in C^i(\theta^{-1}(g))$; considering all i gives $\theta^{-1}(g) \in G(M)$.

Our last result using critical elements generalizes the one-dimensional theorem $g(a, a+c, a+2c, \dots, a+kc) = a[(a-1)/k] + ac - a - c$, as proved in [11]. The following determines G , for M of a similarly special type.

Theorem 7 *Fix A and vector $c \geq 0$. Set $C = c(1^n)^T$, a square matrix, and fix $k \in \mathbb{N}$. Set $M = [A|A+C|A+2C|\dots|A+kC]$. Suppose that M is dense. Then $G(M) = \{Ax + |A|c - A_1 - c : x \in \mathbb{N}_0^n, \|x\|_1 = \lceil (|A| - 1)/k \rceil\}$.*

PROOF. We have $M_{\mathbb{N}_0} = \{\sum_{i=0}^k (A + iC)x^i : x^i \in \mathbb{N}_0^n\} = \{A \sum_{i=0}^k x^i + C \sum_{i=0}^k ix^i : x^i \in \mathbb{N}_0^n\} = \{A \sum_{i=0}^k x^i + c \sum_{i=0}^k i \|x^i\|_1 : x^i \in \mathbb{N}_0^n\} = \{Ax + c \sum_{i=0}^k i \|x^i\|_1 : x^i \in \mathbb{N}_0^n; x = \sum_{i=0}^k x^i\}$. Now, for fixed $x \in \mathbb{N}_0^n$, as we vary the decomposition $x = \sum_{i=0}^k x^i$ (for $x^i \in \mathbb{N}_0^n$), we find that $\sum_{i=0}^k i \|x^i\|_1$ takes on all values from 0 to $k\|x\|_1$. Hence $M_{\mathbb{N}_0} = \{Ax + c\gamma : x \in \mathbb{N}_0^n, \gamma \in \mathbb{N}_0, \gamma \leq k\|x\|_1\}$.

Choose any $x \in \mathbb{N}_0^n$ satisfying $\|x\|_1 = \lceil (|A| - 1)/k \rceil$. Set $T = \{Ax + c\gamma \in S : 0 \leq \gamma \leq |A| - 1\}$. By construction, we have $T \subseteq M_{\mathbb{N}_0}$. Further, the elements of T must be inequivalent mod A , since c is a generator of the cyclic group $\mathbb{Z}/A\mathbb{Z}$. Set $h = \text{lub}(T) - A_1 = Ax + (|A| - 1)c - A_1$. Note that each $t \in T$ either has $t \in V(h)$ or $t \leq t'$ (and $t \equiv t'$) for some $t' \in V(h)$; hence $V(h) \subseteq M_{\mathbb{N}_0}$ and h is complete. For any $i \in [1, n]$, $|A| - 1 > k\|x - e_i\|_1$, so $A(x - e_i) + (|A| - 1)c \in C^i(h)$, so $h \in G(M)$. Now, let $g \in G(M)$. By Theorem

8, we have $g \geq Ax + (|A| - 1)c - A_1$, for some $x \in \mathbb{N}_0^n$ with $|A| - 1 \leq k\|x\|_1$. By the previous, however, $Ax + (|A| - 1)c - A_1 \in G(M)$, so we have equality by the minimality of g .

3 The MIN Method

Let $\text{MIN} = \{x : x \in M_{\mathbb{N}_0}; \text{ for all } y \in M_{\mathbb{N}_0}, \text{ if } y \equiv x \text{ then } y \geq x\}$. 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 in [9]; the following result shows that it characterizes G .

Theorem 8 *Let $g \in G$. Then $g = \text{lub}(N) - A_1$ for some complete set of coset representatives $N \subseteq \text{MIN}$. Further, if $n < |A|$ then there is some $N' \subseteq N$ with $|N'| = n$ and $\text{lub}(N) = \text{lub}(N')$.*

PROOF. Observe that $V(g) \subseteq [\succ g]$; hence $V(g) \subseteq M_{\mathbb{N}_0}$ since g is complete. Let $\text{MIN}' = \{u \in \text{MIN} : \exists v \in V(g), u \equiv v, u \leq v\}$. Now, for $v \in C^i(g)$, we have $v + Ae_i \in V(g)$. Let $v_{\text{MIN}} \in \text{MIN}'$ with $v_{\text{MIN}} \equiv v + Ae_i$ and $v_{\text{MIN}} \leq v + Ae_i$. We must have $(A^{-1}v_{\text{MIN}})_i \geq (A^{-1}v)_i + 1 = (A^{-1}g)_i + 1$ because otherwise $v \in v_{\text{MIN}} + A_{\mathbb{N}_0}$ and therefore $v \in M_{\mathbb{N}_0}$, which is violative of $v \in C^i(g)$. Set $N' = \{v_{\text{MIN}} : i \in [1, n]\}$; we have $\text{lub}(N') \geq g + A_1$. But also we have $g + A_1 = \text{lub}(V(g)) \geq \text{lub}(\text{MIN}') \geq \text{lub}(N')$. Hence all the inequalities are equalities, and in fact $\text{lub}(N') = \text{lub}(N)$ for any N with $N' \subseteq N \subseteq \text{MIN}'$. Finally, we note that $|N'| \leq n$ but also we may insist that $|N'| \leq |A|$ because $|V(g)| = |A|$.

Elements of MIN have a particularly nice form; this is quite useful in computations.

Theorem 9 $MIN \subseteq \{Bx : x \in \mathbb{N}_0^m, \|x\|_1 \leq |A| - 1\}$.

PROOF. Let $v \in MIN \subseteq M_{\mathbb{N}_0}$. Write $v = Mv'$, where $v' \in \mathbb{N}_0^{n+m}$. Suppose that $(v')_i > 0$, for $1 \leq i \leq n$. Set $w' = v' - e_i$, and $w = Mw'$. We see that $w \equiv v$, $w \leq v$, and $w \in M_{\mathbb{N}_0}$; this contradicts $v \in MIN$. Hence $MIN \subseteq B_{\mathbb{N}_0}$. Let $z = Bx \in MIN$. Suppose $\|x\|_1 \geq |A|$; then we start with 0 and increment one coordinate at a time, building a sequence $B0 = Bv_0 \preceq Bv_1 \preceq Bv_2 \preceq \dots \preceq Bv_{\|x\|_1} = z$ where each $v_i \in \mathbb{N}_0^m$. We may do this since M is simplicial. Because there are at least $|A| + 1$ terms, two (say $Bv_a \preceq Bv_b$) are congruent mod A . $z - Bv_b \in M_{\mathbb{N}_0}$ and so $y = z - (Bv_b - Bv_a) \in M_{\mathbb{N}_0}$. But $y \preceq z$ and $y \equiv z$; this violates $z \in MIN$.

Corollary 10 $|G|$ is finite.

The following result, proved first in [12] and rediscovered in [13], generalizes the classical one-dimensional result on two generators $g(a_1, a_2) = a_1a_2 - a_1 - a_2$. Note that in this special case of $m = 1$, we must have $|G| = 1$ and $G \subseteq \mathbb{Z}^n$; neither of these necessarily holds for $m > 1$.

Corollary 11 If $m = 1$ then $G = \{|A|B - A_1 - B\}$.

PROOF. By Theorem 9, we have $MIN = \{0, B, 2B, \dots, (|A| - 1)B\}$, a complete set of coset representatives. By Theorem 8, any $g \in G$ must have $g + A_1 = \text{lub}(MIN) = (|A| - 1)B$.

Corollary 11 can be extended to the case where the column space of B is one dimensional, using as an oracle function the (one-dimensional) Frobenius number. In this special case we again have $|G| = 1$ and $G \subseteq \mathbb{Z}^n$.

Theorem 12 Consider dense $M = [A|B]$ with B a column vector ($m = 1$).

Let $C = [c_1, c_2, \dots, c_m] \in \mathbb{N}^m$. Suppose that $P = [|A| \mid C]$ is dense. Then

$N = [A|BC]$ is dense, and $G(N) = \{G(P)B + |A|B - A_1\}$.

PROOF. By Theorem 9, we have $\text{MIN}(M) = \{0, B, \dots, (|A| - 1)B\}$. Hence $\mathbb{Z}^n/A\mathbb{Z}^n$ is cyclic, and B is a generator. Let S denote the set of all $n \times n$ minors of M , apart from $|A|$. We have $\gcd(|A|, \{c_i s : 1 \leq i \leq m, s \in S\}) = \gcd(|A|, \gcd(c_1, c_2, \dots, c_m) \gcd(S)) = \gcd(|A|, \gcd(S)) = 1$, where we have used the denseness of M and P . Hence N is dense. By Theorem 9 again, we have $\text{MIN}(N) \subseteq B_{\mathbb{N}_0}$. We now show that $G(P)B \notin M_{\mathbb{N}_0}$. Suppose otherwise; we then write $G(P)B = Ax + BCy$ and hence $Ax = Bq$ for $q = (G(P) - Cy)$. We conclude that $q \equiv 0 \pmod{A}$ and hence $q = k|A|$ for some $k \in \mathbb{N}$ ($k > 0$ since M is simplicial) since B generates $\mathbb{Z}^n/A\mathbb{Z}^n$. We now have $BG(P) = Bk|A| + BCy$, hence $G(P) = k|A| + Cy$. But now $G(P) - 1$ is complete (with respect to P), which violates the definition of $G(P)$. Therefore $G(P)B \notin M_{\mathbb{N}_0}$. On the other hand, if $\alpha \in \mathbb{Z}$ and $\alpha > G(P)$ we have $\alpha = k|A| + Cy$, for some $k, y \in \mathbb{N}_0$. Therefore, we have $B\alpha = k|A|B + BCy = A(k|A|A^{-1}B) + BCy \in M_{\mathbb{N}_0}$ (note that $A^{-1}B \in Q^{\geq 0}$ since M is simplicial). Hence, $T = \{G(P)B + kB : k \in [1, |A|]\} \subseteq M_{\mathbb{N}_0}$, with $\text{lub}(T) = G(P)B + |A|B = \beta$. Let $g \in G(N)$, and let M be chosen as in Theorem 8 with $|M| = |A|$. Since T is a complete set of coset representatives and both T and $\text{MIN}(N)$ lie on $B\mathbb{R}$, we have $\text{lub}(M) \leq \text{lub}(\text{MIN}(N)) \leq \text{lub}(T) = G(P)B + |A|B = \beta$. However, the coset of β is precisely $\{G(P)B + k|A|B : k \in \mathbb{Z}\}$. Therefore, β is the unique representative of its equivalence class in MIN , and thus $\beta \in M$ and $\text{lub}(M) = \beta$. Hence $g + A_1 = \beta$ for all $g \in G$, as desired.

We give two more results using this method. First, we present a \leq -bound of G ; this generalizes a one dimensional bound, attributed to Schur in [14]: $g(a_1, a_2, \dots, a_k) \leq a_1 a_k - a_1 - a_k$ (where $a_1 < a_2 < \dots < a_k$). Note that Corollary 11 shows that equality is sometimes achieved.

Theorem 13 $G \leq \text{lub}(\{|A|b - A_1 - b : b \text{ a column of } B\})$.

PROOF. Let $x \in \text{MIN}$, fix $1 \leq i \leq n$, and write $(A^{-1}x)_i = (A^{-1}Bx')_i = (\sum_b (x')_b A^{-1}b)_i$, where b ranges over all the columns of B . Set b^* to be a column of B with $(A^{-1}b^*)_i$ maximal; we have $(A^{-1}x)_i \leq (A^{-1}b^*)_i \|x'\|_1 \leq (A^{-1}b^*)_i (|A| - 1)$, applying Theorem 9. By the choice of b^* , and by varying i , we have shown that $x \leq \text{lub}(\{|A| - 1\}b)$ and hence $\text{lub}(\text{MIN}) \leq \text{lub}(\{|A| - 1\}b)$. For any $g \in G$, we apply theorem 8 and have $g + A_1 \leq \text{lub}(\text{MIN}) \leq \text{lub}(\{|A| - 1\}b)$.

Finally, we characterize possible G in our context for the special case $m = 1$. This generalizes a one-dimensional construction found in [15]; it is an open problem to determine if all G are possible if we allow $m = 2$.

Theorem 14 *Let $g \in \mathbb{Z}^n$. There exists a simplicial, dense, M with $m = 1$ and $G = \{g\}$ if and only if $(1/2)g \notin \mathbb{Z}^n$.*

PROOF. Suppose $(1/2)g \notin \mathbb{Z}^n$. By applying an invertible change of basis if necessary, we assume without loss that $g \in \mathbb{N}^n$ and that $(1/2)(g)_1 \notin \mathbb{Z}$. Set $A = \text{diag}(2, 1, 1, \dots, 1)$, and set $B = A_1 + g$. For $i \in [1, n]$, define $A^{\hat{i}}$ to be A with the i^{th} column replaced by B . Note that $\det A = 2$ and $\det A^{\hat{1}} = 2 + (g)_1$ (which is odd); hence M is dense. We now apply Corollary 11 to get $G = \{g\}$, as desired. Suppose now that we have a simplicial dense M , with $G = \{g\}$ and $(1/2)g \in \mathbb{Z}^n$. Applying Corollary 11 again, we get that $g + A_1 = (|A| - 1)B$.

Suppose that $|A|$ were odd. Then each coordinate of $(|A| - 1)B$ is even, as is each coordinate of g ; hence so is each coordinate of A_1 . Considering the integers mod 2, we have $|A| = 1$ but $A_1 = 0^n$, a contradiction. Therefore we must have $|A|$ even. We now consider the system $A(x_1, x_2, \dots, x_n)^T = B$. We may apply Cramer's rule since $|A| \neq 0$ and $B \neq 0^n$; we find that, uniquely, $\det A^{\dot{i}} = x_i |A|$. We now consider the system reduced mod 2 (working in $\mathbb{Q}/2\mathbb{Q}$) and find that 1^n solves the reduced system, as $B = |A|B - g - A_1 \equiv -A1^n \equiv A1^n \pmod{2}$. Hence, each x_i is in fact an odd integer, and thus $\det A^{\dot{i}}$ is an even integer. Consequently, all $n \times n$ minors of M are even, which is violative of the denseness of M .

The authors would like to gratefully acknowledge the helpful comments of an anonymous referee.

References

- [1] J. Ramirez Alfonsin, *The Diophantine Frobenius Problem*, Oxford Lecture Series in Mathematics and Its Applications, Oxford University Press, New York, 2006.
- [2] B. V. Novikov, On the structure of subsets of a vector lattice that are closed with respect to addition, *Ukrain. Geom. Sb.* (35) (1992 (translation in *J. Math. Sci.* 72 (1994), no. 4, 3223–3225)) 99–103, 164.
- [3] R. Dedekind, *Theory of algebraic integers*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1996, translated from the 1877 French original and with an introduction by John Stillwell.
- [4] M. A. Frumkin, On the number of nonnegative integer solutions of a system of linear Diophantine equations, in: *Studies on graphs and discrete programming*

- (Brussels, 1979), Vol. 11 of *Ann. Discrete Math.*, North-Holland, Amsterdam, 1981, pp. 95–108.
- [5] N. N. Ivanov, V. N. Ševčenko, The structure of a finitely generated semilattice, *Dokl. Akad. Nauk BSSR* 19 (9) (1975) 773–774, 857.
- [6] A. Rycerz, The generalized residue classes and integral monoids with minimal sets, *Op. Math.* 20 (2000) 65–69.
- [7] B. Vizvári, An application of Gomory cuts in number theory, *Period. Math. Hungar.* 18 (3) (1987) 213–228.
- [8] B. L. van der Waerden, *Algebra. Teil II, Unter Benutzung von Vorlesungen von E. Artin und E. Noether. Fünfte Auflage. Heidelberger Taschenbücher, Band 23*, Springer-Verlag, Berlin, 1967.
- [9] A. Brauer, J. E. Shockley, On a problem of Frobenius, *J. Reine Angew. Math.* 211 (1962) 215–220.
- [10] S. M. Johnson, A linear diophantine problem, *Canad. J. Math.* 12 (1960) 390–398.
- [11] J. B. Roberts, Note on linear forms, *Proc. Amer. Math. Soc.* 7 (1956) 465–469.
- [12] M. J. Knight, A generalization of a result of Sylvester’s, *J. Number Theory* 12 (3) (1980) 364–366.
- [13] R. J. Simpson, R. Tijdeman, Multi-dimensional versions of a theorem of Fine and Wilf and a formula of Sylvester, *Proc. Amer. Math. Soc.* 131 (6) (2003) 1661–1671 (electronic).
- [14] A. Brauer, On a problem of partitions, *Amer. J. Math.* 64 (1942) 299–312.
- [15] J. C. Rosales, P. A. García-Sánchez, J. I. García-García, Every positive integer is the Frobenius number of a numerical semigroup with three generators, *Math. Scand.* 94 (1) (2004) 5–12.

- [16] M. Beck, S. Zacks, Refined upper bounds for the linear Diophantine problem of Frobenius, *Adv. in Appl. Math.* 32 (3) (2004) 454–467.