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 the non-negative integers $\mathbb{N}_0$. Georg Frobenius focused attention on determining the maximal integer 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 [1]. In this paper, we consider the problem of determining maximal vectors g such that the system of linear Diophantine equations $Mx = g$ has no solutions.

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. We write X_1 for the vector in $X_{\{1\}}$. We fix $M \in \mathbb{Z}_{n\times(n+m)}$, 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 is a square matrix; but still the cardinality of A, if A is a set. 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 $n \leq 2$ and there is some halfspace containing all the columns of M, 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 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, $u \gneq v$ does not necessarily imply that $u \succ v$. For $v \in \mathbb{R}^n$, we write $(v)_i$ for the i^{th} coordinate of v, and $[\succ v] = \{u \in \mathbb{Z}^n : u \succ v\}$. 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 work over Q rather than over $\mathbb{R}$.

Proposition 1 *Let $v \in \mathbb{R}^n$. There exists $v^\star \in Q^n$ with $[\succ v] = [\succ Av^\star]$ and $v \geq Av^\star$.*

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

Let $x, y \in M_{Q^{\geq 0}}$. We write $x = Ax', y = Ay'$, with $x', y' \in \left(Q^{\geq 0}\right)^n$, define z' via $(z')_i = \max((x')_i, (y')_i)$, and set $\mathrm{lub}(x, y) = Az'$. We have $\mathrm{lub}(x, y) \in M_{Q^{\geq 0}}$, although in general $\mathrm{lub}(x, y) \notin M_{\mathbb{N}_0}$ (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 $V(u) = \left(u + A_{Q\cap(0,1]}\right) \cap \mathbb{Z}^n$. 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 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 $v = (v_1, v_2, \ldots, v_n)$. 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 each one, then their product is one. Conversely, if their product is one, then

they must each be one since they are all nonnegative integers. $\square$

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

Call v *f-complete* if $[\succ v] \subseteq M_{\mathbb{N}}$.

Proposition 3 *Let F be the set of all $\geq$-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 the following conditions are equivalent for an integral vector u: (1) $u \in [\succ v + M_1]$, (2) $u \succ v + M_1$, (3) $(u - M_1) - v \in M_{\mathbb{R}\geq 0}$, (4) $(u - M_1) \succ v$, (5) $(u - M_1) \in [\succ v]$. 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. $\square$

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 the set 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 the cone at u, that are minimal mod A. Let $C(u) = \bigcup_{i\in[1,n]} C^i(u)$, which is a disjoint union of finite sets. We 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.

Theorem 4 *Let x be complete. The following statemements are equivalent.*

(1) $x \in G$

(2) Each face of 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 cone(x).
(1) → (2) If $S_i \subseteq M_{\mathbb{N}_0}$, then x^i is complete, which is violative of $x \in G$.
(2) → (3) Pick any minimal $y \in S_i \setminus M_{\mathbb{N}_0}$. Suppose that $\left(A^{-1}(y-x)\right)_j \notin (0,1]$ 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) → (1) If $x^\star < x$, then $x^\star \leq x^i$ for some i. But no x^i is complete; hence $x^\star$ is not complete. Thus x is $\geq$-minimal and complete and thus $x \in G$. □

Critical elements can also be used to test for uniqueness of Frobenius vectors. Set $\overline{e_i} = \overline{1} - e_i = (1,1,\ldots,1,0,1,1,\ldots,1)$.

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* $c^i + kA\overline{e_i} \notin M_{\mathbb{N}_0}$ *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 $c^i + kA\overline{e_i} \notin M_{\mathbb{N}_0}$ 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 $k \to \infty$, $(A^{-1}c^i + k\overline{e_i})_j \to \infty$ (for $j \neq i$), but also $(A^{-1}c^i + k\overline{e_i})_i = (A^{-1}g)_i$ for all k. Therefore, for some k we have $c^i + kA\overline{e_i} \succ g'$. Hence g' is not complete, which is violative of our 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 $c^i + k(i)A\overline{e_i} \in M_{\mathbb{N}_0}$. If $c^i + kA\overline{e_i} \in M_{\mathbb{N}_0}$, then $c^i + k'A\overline{e_i} \in M_{\mathbb{N}_0}$ for any $k' \geq k$; hence because $|C^i(g)| < \infty$ there is some $K \in \mathbb{N}_0$ with $c^i + KA\overline{e_i} \in M_{\mathbb{N}_0}$ for all $c^i \in C^i(g)$. Now, set $g^\star = g + (K+1)A\overline{e_i} - (1/|A|)Ae_i$ and $S = [\succ g^\star] \setminus [\succ g] \subseteq \{u \in \mathbb{Z}^n : (A^{-1}(u-g))_i = 0, (A^{-1}(u-g))_j \geq K+1 \ (j \neq i)\}$.

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 $u' + KA\overline{e_i} \in M_{\mathbb{N}_0}$ and hence $u \in M_{\mathbb{N}_0}$ since $u - (u' + KA\overline{e_i}) \in A_{\mathbb{N}_0}$. Hence $S \subseteq M_{\mathbb{N}_0}$ and $g^\star$ is complete. Now take $g' \in G$ with $g' \leq g^\star$. We have $(A^{-1}g')_i \leq (A^{-1}g^\star)_i < (A^{-1}g)_i$ and hence $g' \neq g$, which is violative of our hypothesis. $\square$

Our next result 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 us an analogous assumption in general.

Theorem 6 *Let $d \in \mathbb{N}$ and let $M = [A|B]$ be simplicial. 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, and hence M is dense. Further, d divides all minors of N apart from $|A|$, and hence $\gcd(|A|, d) = 1 = \gcd(|A|^2, d)$. We can therefore pick $d^\star \in \mathbb{N}$ with $d^\star d \in 1 + |A|^2\mathbb{N}_0$. For any $v \in Q^n$, we observe that $d^\star dv - v \in \mathbb{N}_0|A|^2Q^n = \mathbb{N}_0|A|\mathbb{Z}^n \subseteq A_\mathbb{Z}$; hence $d^\star dv \equiv v$. 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 $y \in \mathbb{N}_0^n$, and $z \in \mathbb{N}_0^m$. We observe that $x + A1^n = A(1/d)(y + 1^n) + Bz$, so $x + A1^n \geq Bz$. Also, $d^\star d(x + A1^n) = Ad^\star(y + 1^n) + d^\star dBz$, and 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 $\omega = d(1^n - \epsilon') + (\epsilon - 1^n)$. Because $u \equiv du'$ we also have $u - du' = A\alpha$ with $\alpha \in \mathbb{Z}^n$. Since $|A| \neq 0$, we have $\omega = \alpha \in \mathbb{Z}^n$. Further, since $\epsilon, \epsilon' \in (0, 1]^n$, each coordinate of $d(1^n - \epsilon') + (\epsilon - 1^n)$ is strictly greater than -1 and hence $\omega \in \mathbb{N}_0^n$. 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 $\theta^{-1}(g) \in G(M)$. $\square$

3 The MIN Method

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 in [9]; the following result shows that it characterizes the set G.

Theorem 7 *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 $lub(N) = lub(N')$.*

PROOF. Observe that $V(g) \subseteq [\succ g]$, and hence $V(g) \subseteq M_{\mathbb{N}_0}$ since g is complete. Let 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 $\mathrm{lub}(N') = \mathrm{lub}(N)$ for any N with $N' \subseteq N \subseteq \mathrm{MIN}'$. Finally, we note that $|N'| \leq n$ but also we may insist that $|N'| \leq |A|$ because $|V(g)| = |A|$. $\square$

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

Theorem 8 *$MIN \subseteq \{Bx : x \in \mathbb{N}_0^m, ||x||_1 \leq |A| - 1\}$.*

PROOF. Let $v \in \mathrm{MIN} \subseteq M_{\mathbb{N}_0}$. 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 that $v \in \mathrm{MIN}$. Hence $\mathrm{MIN} \subseteq B_{\mathbb{N}_0}$. Let $z = Bx \in \mathrm{MIN}$. Suppose that $||x||_1 \geq |A|$. Start with 0 and increment one coordinate at a time, building a sequence $B0 = Bv_0 \lneq Bv_1 \lneq Bv_2 \lneq \cdots \lneq Bv_{||x||_1} = z$ 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 $Bv_a \lneq Bv_b$) are congruent mod A. We have $z - Bv_b \in M_{\mathbb{N}_0}$ and so $y = z - (Bv_b - Bv_a) \in M_{\mathbb{N}_0}$, but $y \lneq z$ and $y \equiv z$. This violates that $z \in \mathrm{MIN}$. $\square$

Corollary 9 *$|G|$ is finite.*

The following result, proved first in [11] and rediscovered in [12], generalizes the classical one-dimensional result on two generators that $g(a_1, a_2) = a_1a_2 - a_1 - a_2$. Note that in the special case where $m = 1$, we must have that $|G| = 1$ and $G \subseteq \mathbb{Z}^n$. Neither of these necessarily holds for $m > 1$.

Corollary 10 *If $m = 1$ then $G = \{|A|B - A_1 - B\}$.*

PROOF. By Theorem 8, we have $\mathrm{MIN} = \{0, B, 2B, \ldots, (|A| - 1)B\}$, a complete set of coset representatives. By Theorem 7, any $g \in G$ must have

$g + A_1 = \text{lub}(MIN) = (|A| - 1)B$. $\square$

Corollary 10 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 11 *Consider a dense $M = [A|B]$ with B a column ($n \times 1$) vector, i.e. the special case $m = 1$. Let $C = [c_1, c_2, \ldots, c_m] \in \mathbb{N}^m$. Suppose that $P = [\ |A|\ |\ C\ ]$ is dense. Then $N = [A|BC]$ is dense, and $G(N) = \{G(P)B + |A|B - A_1\}$.*

PROOF. By Theorem 8, we have $\text{MIN}(M) = \{0, B, \ldots, (|A| - 1)B\}$. 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 $|A|$. Using the denseness of M and P, we have $\gcd(|A|, \{c_i s : 1 \le i \le m, s \in S\}) = \gcd(|A|, \gcd(c_1, c_2, \ldots, c_m) \gcd(S)) = \gcd(|A|, \gcd(S)) = 1$, and hence N is dense. Again by Theorem 8, 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 $qB \equiv 0 \bmod A$ 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 $BG(P) = Bk|A| + BCy$, and 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 $A^{-1}B \in Q^{\ge 0}$ 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 7 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 $\text{lub}(M) \le$

$\mathrm{lub}(\mathrm{MIN}(N)) \le \mathrm{lub}(T) = G(P)B + |A|B = \beta$. 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 $\mathrm{lub}(M) = \beta$. Hence $g + A_1 = \beta$ for all $g \in G$, as desired. $\square$

Example 12 *Consider* $N = \left(\begin{smallmatrix} 5 & 0 & 84 & 105 \\ 0 & 4 & 84 & 105 \end{smallmatrix}\right)$*. We have* $N = [A|BC]$*, for* $A = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 4 \end{smallmatrix}\right)$*,* $B = \left(\begin{smallmatrix} 3 \\ 3 \end{smallmatrix}\right)$*, and* $C = (28, 35)$*. Following Theorem 11, we have* $P = (20, 28, 35)$*.* $\gcd(20, 28, 35) = 1$ *so* P *is dense; we now calculate* $G(P) = 197$ *using our one-dimensional oracle. Therefore* N *is dense and* $G(N) = \{\left(\begin{smallmatrix} 646 \\ 647 \end{smallmatrix}\right)\}$*.*

We give three more results using this method. First, we present a $\le$-bound for G. This generalizes a one dimensional bound, attributed to Schur in [13]: $g(a_1, a_2, \ldots, a_k) \le a_1 a_k - a_1 - a_k$ (where $a_1 < a_2 < \cdots < a_k$). Note that Corollary 10 shows that equality is sometimes achieved.

Theorem 13 *For all* $g \in G$*,* $g \le \mathit{lub}(\{|A|b - A_1 - b : b \text{ a column of } B\})$*.*

PROOF. Let $x \in \mathrm{MIN}$, fix $1 \le i \le n$, and write $(A^{-1}x)_i = (A^{-1}Bx')_i = \left(\sum_b (x')_b A^{-1} b\right)_i$, where b ranges over all the columns of B. Set $b^\star$ to be a column of B with $(A^{-1}b^\star)_i$ maximal. By Theorem 8, we have that $(A^{-1}x)_i \le (A^{-1}b^\star)_i ||x'||_1 \le (A^{-1}b^\star)_i(|A| - 1)$. By the choice of $b^\star$, and by varying i, we have shown that $x \le \mathrm{lub}(\{(|A|-1)b\})$ and hence $\mathrm{lub}(\mathrm{MIN}) \le \mathrm{lub}(\{(|A|-1)b\})$. For any $g \in G$, we apply Theorem 7 and have $g + A_1 \le \mathrm{lub}(\mathrm{MIN}) \le \mathrm{lub}(\{(|A|-1)b\})$. $\square$

Next, we characterize possible G in our context for the special case $m = 1$. This generalizes a one-dimensional construction found in [14]. If we allow $m = 2$, then it is an open problem to determine whether all G are possible.

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 $A = \operatorname{diag}(2, 1, 1, \ldots, 1)$, and set $B = A_1 + g$. For $i \in [1, n]$, define $A^{\underline{i}}$ to be A with the i^{th} column replaced by B. Note that $\det A = 2$ and $\det A^{\underline{1}} = 2 + (g)_1$ (which is odd), and hence M is dense. We now apply Corollary 10 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 10 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, and 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 that $|A|$ is even. We now consider the system $A(x_1, x_2, \ldots, x_n)^T = B$. We may apply Cramer's rule since $|A| \neq 0$ and $B \neq 0^n$; we find that, uniquely, $\det A^{\underline{i}} = x_i|A|$. 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 $\det A^{\underline{i}}$ is an even integer. Consequently, all $n \times n$ minors of M are even, which is violative of the denseness of M. $\square$

Our last result combines the two methods presented. It generalizes the one-dimensional theorem $g(a, a+c, a+2c, \ldots, a+kc) = a\lceil (a-1)/k \rceil + ac - a - c$, as proved in [15]. The following determines G, for M of a similarly special type.

Theorem 15 *Fix A and a 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* $G(M) = \{Ax + |A|c - A_1 - c : x \in \mathbb{N}_0^n, \|x\|_1 = \lceil (|A|-1)/k \rceil\}$.

PROOF. We have

$$\begin{aligned} M_{\mathbb{N}_0} &= \{\sum_{i=0}^{k} (A+iC)x^i : x^i \in \mathbb{N}_0^n\} \\ &= \{A\sum_{i=0}^{k} x^i + C\sum_{i=0}^{k} ix^i : x^i \in \mathbb{N}_0^n\} \\ &= \{A\sum_{i=0}^{k} x^i + c\sum_{i=0}^{k} i||x^i||_1 : x^i \in \mathbb{N}_0^n\} \\ &= \{Ax + c\sum_{i=0}^{k} i||x^i||_1 : x^i \in \mathbb{N}_0^n; x = \sum_{i=0}^{k} x^i\}. \end{aligned}$$

Now, for a 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 $M_{\mathbb{N}_0} = \{Ax + c\gamma : x \in \mathbb{N}_0^n, \gamma \in \mathbb{N}_0, \gamma \le k\|x\|_1\}$.

Choose any $x \in \mathbb{N}_0^n$ satisfying $\|x\|_1 = \lceil (|A|-1)/k \rceil$. Set $T = \{Ax + c\gamma \in M_{\mathbb{N}_0} : 0 \le \gamma \le |A| - 1\}$. 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 $\mathbb{Z}^n/A_{\mathbb{Z}}$. Set $h = \mathrm{lub}(T) - A_1 = Ax + (|A|-1)c - A_1$. Note that each $t \in T$ either has $t \in V(h)$ or $t \le t'$ (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 $A(x - e_i) + (|A|-1)c \in C^i(h)$, and thus $h \in G(M)$. Now, let $g \in G(M)$. By Theorem 7, we have $g \ge Ax + (|A|-1)c - A_1$, for some $x \in \mathbb{N}_0^n$ with $|A| - 1 \le k\|x\|_1$. By our earlier observation, $Ax + (|A|-1)c - A_1 \in G(M)$, so we have equality by the minimality of g. $\square$

Example 16 *Consider* $M = \left(\begin{smallmatrix} 5 & 0 & 7 & 2 & 9 & 4 & 11 & 6 & 13 & 8 & 15 & 10 & 17 & 12 & 19 & 14 \\ 0 & 4 & 1 & 5 & 2 & 6 & 3 & 7 & 4 & 8 & 5 & 9 & 6 & 10 & 7 & 11 \end{smallmatrix}\right)$. *We see that* $M = [A|A+C|A+2C|A+3C|A+4C|A+5C|A+6C|A+7C]$ *for* $A = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 4 \end{smallmatrix}\right)$ *and* $C = \left(\begin{smallmatrix} 2 & 2 \\ 1 & 1 \end{smallmatrix}\right)$. *$M$ is dense since* $|A| = 20, |A + C| = 33$ *and* $\gcd(20, 33) =$

1. *Applying Theorem 15, we get* $G(M) = \{Ax + \binom{33}{15} : x, \|x\|_1 = 3\} = \{\binom{48}{15}, \binom{43}{19}, \binom{38}{23}, \binom{33}{27}\}$.

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

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] M. J. Knight, A generalization of a result of Sylvester's, J. Number Theory 12 (3) (1980) 364–366.

[12] 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).

[13] A. Brauer, On a problem of partitions, Amer. J. Math. 64 (1942) 299–312.

[14] 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.

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