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 [9], 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 [8] 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 *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 $\epsilon_i < 1/|A|$.

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 $\text{lub}(x, y) = Az'$, 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 [4] 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. Portions of the following have been repeatedly rediscovered [5,6,8,12,15]. 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 $(1 \le i \le n)$, $e_i \in M_{\mathbb{Z}}$.

(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 [8]. (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 $1 \le i \le n$. 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, [14]) 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 [3] 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 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 $u \in [\succ v + M_1]$ 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 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 4 *Let x be complete. $x \in G$ if and only if $C^i(x) \neq \emptyset,\ \forall i \in [1,n]$.*

PROOF. We write $x = Ax'$. Let $i \in [1,n]$, and consider $x^\star = x - (1/|A|)Ae_i$. Set $S = [\succ x^\star] \setminus [\succ x]$. Observe that $S = \{Au \in \mathbb{Z}^n : (u)_j > (x')_j \text{ (for } j \neq i), (u)_i = (x')_i\}$. If $v \in C^i(x)$, then $v \in S$ and hence $x^\star \notin G$. If this holds for each $i \in [1,n]$ then in fact x must be minimal, and hence $x \in G$. On the other hand, suppose $C^i(x) = \emptyset$. We will show that $S \subseteq M_{\mathbb{N}_0}$. Suppose otherwise; pick any minimal $y \in S \setminus M_{\mathbb{N}_0}$. Suppose that $(A^{-1}(y-x))_j \notin (0,1]$ for $j \neq i$; in this case, $y - Ae_j$ would also be in $S \setminus M_{\mathbb{N}_0}$, violating the minimality of y. But now $y \in C^i(x)$, which is violative of $C^i(x) = \emptyset$.

Critical elements can also test for uniqueness of Frobenius vectors.

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 $c^i + k(A_1 - Ae_i) \notin M_{\mathbb{N}_0}$ for all $k \in \mathbb{N}_0$.*

PROOF. Set $v_{i,k}(c^i) = v_{i,k} = c^i + k(A_1 - Ae_i)$. Note that as $k \to \infty$, $(A^{-1}v_{i,k})_i = (g)_i$, whereas $(A^{-1}v_{i,k})_j \to \infty$ (for $j \neq i$). Let $g' \in Q^n$; if $(g')_i < (g)_i$, then for some k we have $v_{i,k} \succ g'$; hence $g' \notin G$. Thus if $g' \in G$ then $g' \geq g$ and therefore $|G| = 1$. Now, let $g \in G$ be unique, and suppose that the desired conclusion does not hold. If $v_{i,k}(c^i) \in M_{\mathbb{N}_0}$, then $v_{i,k'}(c^i) \in M_{\mathbb{N}_0}$ for any $k' \geq k$; hence there is some $K \in \mathbb{N}_0$ with $v_{i,k}(c^i) \in M_{\mathbb{N}_0}$ for all $k \geq K$

and for all $c^i \in C^i(g)$. Now, set $g^\star = g + K(A_1 - Ae_i) - (1/|A|)Ae_i$ and set $S = [\succ g^\star] \setminus [\succ g]$. We now show that $S \setminus M_{\mathbb{N}_0}$ is empty; assuming otherwise, we choose u minimal therein. Suppose that $(A^{-1}(u - g^\star))_j \notin (0, 1]$ for $j \neq i$; in this case $u - Ae_j$ would also be in $S \setminus M_{\mathbb{N}_0}$, violating the minimality of u. We now set $c^i = u - K(A_1 - Ae_i)$; we have $c^i \in C^i(g)$ and thus $u = v_{i,K}(c^i) \notin M_{\mathbb{N}_0}$, which is violative of assumption. Hence $S \subseteq M_{\mathbb{N}_0}$ and $g^\star$ is complete. Now take $g' \in G$ with $g' \leq g^\star$. We have $(g')_i \leq (g^\star)_i < (g)_i$ 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 [7] 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 $\gcd(|A|, d) = 1$. We can therefore pick $d^\star \in \mathbb{N}$ with $d^\star d \in 1 + |A|\mathbb{N}_0$; observe that $d^\star dv \equiv v$, for any vector 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 $\theta(x) \in N_{\mathbb{N}_0}$. 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, $d^\star d(x + A1^n) = Ad^\star(y + 1^n) + d^\star dBz$; 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, $x = A(w - 1^n) + Bz \in M_{\mathbb{N}_0}$.

Let $g \in G(M)$; we will show that $\theta(g) \in G(N)$. Let $i \in [1, n]$; by Theorem 4, there is $u \in [0,1]^n$ 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 $g(a, a + c, a + 2c, \ldots, a + kc) = a\lceil(a-1)/k\rceil + ac - a - c$, as proved in [10]. 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 $M = [A|A+C|A+2C|\cdots|A+kC]$. 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. Set $S = \{Ax+c\gamma : x \in \mathbb{N}_0^n, \gamma \in \mathbb{N}_0, \gamma \leq k\|x\|_1\}$; we claim that $S = M_{\mathbb{N}_0}$. First, let $Ax+c\gamma \in S$. Without loss we take m and reindex so that $x_i > 0$ for $i \in [1, m]$, and $x_i = 0$ for $i \in [m + 1, n]$. Choose $\gamma_i \leq kx_i$ (for $i \in [1, m]$) so that $\gamma = \sum_i \gamma_i$. We have $a_i x_i + c\gamma_i \in M_{\mathbb{N}_0}$ and hence $Ax + c\gamma \in M_{\mathbb{N}_0}$. Now, choose $z \in M_{\mathbb{N}_0}$. We write $z = \sum_{i,j} \alpha_{i,j}(a_i + jc) = \sum_i(\sum_j \alpha_{i,j})a_i + c\sum_{i,j} \alpha_{i,j}j$ (for $i \in [1, n], j \in [0, k]$). Let $x \in \mathbb{N}_0^n$ via $(x)_i = \sum_j \alpha_{i,j}$, and set $\gamma = \sum_{i,j} \alpha_{i,j}j$; we have $z = Ax + c\gamma$, and $\gamma \leq k\|x\|_1$, so $z \in S$.

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 choice of x, we have $T \subseteq M_{\mathbb{N}_0}$. Further, the elements of T must be inequivalent mod A, since M is dense. 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 $i \in [1,n]$, we have $A(x - e_i) + (|A|-1)c \in C^i(h)$, so $h \in G(M)$. Now, let $g \in G(M)$. By Theorem 9, 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 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 [3]; the following result shows that it characterizes G.

Theorem 8 *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 $V(g) \subseteq [\succ g]$; 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 $(v_{\text{MIN}})_i \geq (v)_i + 1 = (g)_i + 1$ 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 $\text{lub}(N') \geq \text{lub}(C') = g + A_1$. 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 lub(N') = 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 $v \in \text{MIN} \subseteq M_{\mathbb{N}_0}$. 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 $v \in \text{MIN}$. Hence $\text{MIN} \subseteq B_{\mathbb{N}_0}$. Let $z = Bx \in \text{MIN}$. Suppose $||x||_1 \geq |A|$; then we 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 $v_i \in \mathbb{N}_0^m$. Because there are at least $|A| + 1$ terms, two (say $Bv_a \lneq Bv_b$) 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 $y \lneq z$ and $y \equiv z$; this violates $z \in \text{MIN}$.

Corollary 10 $|G|$ *is finite.*

The following result, proved first 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 $\text{MIN} = \{0, B, 2B, \ldots, (|A|-1)B\}$. By Theorem 8, any $g \in G$ must have some $M(g) \subseteq \text{MIN}$ with $g + A_1 = \text{lub}(M(g)) = kB$ for $k \in \mathbb{N}_0 \cap [0, |A| - 1]$. However, if $k < |A| - 1$, g is not complete, since $(|A| - 1)B \notin M_{\mathbb{N}_0}$, which is violative of $g \in G$.

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 $m = 1$. 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 9, we have $\mathrm{MIN}(M) = \{0, B, \ldots, (|A| - 1)B\}$. 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 $|A|$. We have $\gcd(|A|, \{c_i s : 1 \le i \le m, s \in S\}) = \gcd(|A|, \gcd(c_1, c_2, \ldots, c_m) \gcd(S)) = \gcd(|A|, \gcd(S)) = 1$, where we have used the denseness of M and P. Hence N is dense. By Theorem 9 again, we have $\mathrm{MIN}(N) \subseteq B_{\mathbb{N}_0}$. 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 $q \equiv 0$ and hence $q = k|A|$ for some $k \in \mathbb{N}$ 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 $A^{-1}B \in Q^{\ge 0}$ since M is simplicial). Hence, $T = \{G(P)B + kB : k \in [1, |A|]\} \subseteq M_{\mathbb{N}_0}$, with $\mathrm{lub}(T) = G(P)B + |A|B = \beta$. 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 $\mathrm{MIN}(N)$ lie on $B\mathbb{R}$, we have $\mathrm{lub}(M) \le \mathrm{lub}(\mathrm{MIN}(N)) \le \mathrm{lub}(T) = G(P)B + |A|B = \beta$. 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.

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 [2]: $g(a_1, a_2, \ldots, a_k) \leq a_1 a_k - a_1 - a_k$ (where $a_1 < a_2 < \cdots < a_k$). Note that Corollary 11 shows that equality is sometimes achieved.

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

PROOF. Let $x \in$ 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 $b^\star$ to be a column of B with $(A^{-1}b^\star)_i$ maximal; we have $(A^{-1}x)_i \leq (A^{-1}b^\star)_i ||x'||_1 \leq (A^{-1}b^\star)_i(|A|-1)$, applying Theorem 9. By the choice of $b^\star$, 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 [11]; 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 $A = \text{diag}(2, 1, 1, \ldots, 1)$, 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); 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. Define square matrix R via $(R)_{ii} = 1$, $(R)_{in} = 1$, $(R)_{ij} = 0$ (otherwise). Note that AR has each entry of its last column even; hence $2| \det(AR) = \det(A)\det(R) = \det(A)$, which contradicts the assumption that $|A|$ is odd. Therefore we must have $|A|$ even. But now we consider $\det A^{\underline{i}}$; we expand on the i^{th} column (with cofactors $C_{j,i}$) to get $\det A^{\underline{i}} = \sum_j (B)_j C_{j,i} = 1/(|A| - 1) \sum_j (g + A_1)_j C_{j,i} = 1/(|A| - 1) \left(\sum_j (g)_j C_{j,i} + \sum_j A_1 C_{j,i}\right) = 1/(|A| - 1) \left(\sum_j (g)_j C_{j,i} + \det A\right)$. Now, $\det A$ is even, as is $(g)_j$, and $|A| - 1$ is odd; hence $\det A^{\underline{i}}$ is even. Hence, all $n \times n$ minors of M are even, which is violative of the denseness of M.

References

[1] Matthias Beck and Shelemyahu Zacks. Refined upper bounds for the linear Diophantine problem of Frobenius. *Adv. in Appl. Math.*, 32(3):454–467, 2004.

[2] Alfred Brauer. On a problem of partitions. *Amer. J. Math.*, 64:299–312, 1942.

[3] Alfred Brauer and James E. Shockley. On a problem of Frobenius. *J. Reine Angew. Math.*, 211:215–220, 1962.

[4] Richard 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.

[5] 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)*, volume 11 of *Ann. Discrete Math.*, pages 95–108. North-Holland, Amsterdam, 1981.

[6] N. N. Ivanov and V. N. Ševčenko. The structure of a finitely generated semilattice. *Dokl. Akad. Nauk BSSR*, 19(9):773–774, 857, 1975.

[7] S. M. Johnson. A linear diophantine problem. *Canad. J. Math.*, 12:390–398, 1960.

[8] B. V. Novikov. On the structure of subsets of a vector lattice that are closed with respect to addition. *Ukrain. Geom. Sb.*, (35):99–103, 164, 1992 (translation in J. Math. Sci. 72 (1994), no. 4, 3223–3225).

[9] J.L. Ramirez Alfonsin. *The Diophantine Frobenius Problem.* Oxford Lecture Series in Mathematics and Its Applications. Oxford University Press, New York, 2006.

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

[11] J. C. Rosales, P. A. García-Sánchez, and J. I. García-García. Every positive integer is the Frobenius number of a numerical semigroup with three generators. *Math. Scand.*, 94(1):5–12, 2004.

[12] Anna Rycerz. The generalized residue classes and integral monoids with minimal sets. *Op. Math.*, 20:65–69, 2000.

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

[14] 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.

[15] B. Vizvári. An application of Gomory cuts in number theory. *Period. Math. Hungar.*, 18(3):213–228, 1987.