

a journal of mathematics

The multidimensional Frobenius problem

Jeffrey Amos, Iuliana Pascu, Vadim Ponomarenko, Enrique Treviño and Yan Zhang

mathematical sciences publishers

2011 vol. 4, no. 2



The multidimensional Frobenius problem

Jeffrey Amos, Iuliana Pascu, Vadim Ponomarenko, Enrique Treviño and Yan Zhang

(Communicated by Scott Chapman)

We provide a variety of results concerning the problem of determining maximal vectors g such that the Diophantine system Mx = g has no solution: 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

Let m, x be column vectors from the nonnegative 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 [Ramírez Alfonsín 2006]. 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 [Novikov 1992] 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 half-space 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 $u - v \in A_{\mathbb{R}^{\geq 0}}$, then we write u > v. Note that u > v implies $u \geq v$, and $u > v \geq w$ implies u > w; however, $u \geq v$ does

MSC2010: 11B75, 11D04, 11D72.

Keywords: Frobenius, coin-exchange, linear Diophantine system.

Research supported in part by NSF grant 0097366.

not imply that u > v. For $v \in \mathbb{R}^n$, we write $(v)_i$ for the *i*-th coordinate of v, and $[>v] = \{u \in \mathbb{Z}^n : u > v\}$. We say that v is *complete* if $[>v] \subseteq M_{\mathbb{N}_0}$. 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 1.1. Let $v \in \mathbb{R}^n$. There exists $v^* \in Q^n$ with $[\succ v] = [\succ Av^*]$ and $v > Av^*$.

Proof. We choose $v^* \in Q^n$ such that $A^{-1}v - v^* = \epsilon = (\epsilon_1, \epsilon_2, \dots, \epsilon_n)$ with $0 \le \epsilon_i < 1/|A|$. Multiplying by A we get $v - Av^* = A\epsilon$; hence $v \ge Av^*$. We will now show that for $u \in \mathbb{Z}^n$, u > v if and only if $u > Av^*$. If u > v, then $u > Av^*$ because $u > v \ge Av^*$. On the other hand, suppose that $u > Av^*$ and $u \not > v$. 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 $(A^{-1}u - A^{-1}v)_i \le 0$. Because $u \in \mathbb{Z}^n$ and A is an integer matrix, we have $A^{-1}u \in Q^n$; hence in fact $(A^{-1}u - v^*)_i \ge 1/|A|$. Now, $0 \ge (A^{-1}u - A^{-1}v)_i = (A^{-1}u - v^* - (A^{-1}v - v^*))_i = (A^{-1}u - v^*)_i - \epsilon_i \ge 1/|A| - \epsilon_i$. 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 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 [1877] 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 [Frumkin 1981; Ivanov and Shevchenko 1975; Novikov 1992; Rycerz 2000; Vizvári 1987]. 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 $(1 \le i \le n)$, $e_i \in M_{\mathbb{Z}}$.
- (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 $(1) \iff (4) \iff (3) \iff (2) \iff (6) \iff (5)$.

- (1) \iff (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 [Novikov 1992, Proposition 5].
- (4) \iff (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) \iff (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) \iff (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) \iff $N = [I|0] \iff$ (6).
- (6) \iff (5): The product of the elementary divisors is known (see, for example, [van der Waerden 1967, Remark 3 in Section 12.2]) 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.

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 [Brauer and Shockley 1962] 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 1.3. 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. 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 2.1. 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) $C^i(x) \neq \emptyset$ for all $i \in [1, n]$.

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) \Longrightarrow (2) If $S_i \subseteq M_{\mathbb{N}_0}$, then x^i is complete, which violates $x \in G$.
- (2) \Longrightarrow (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) \Longrightarrow (1) If $x^* < x$, then $x^* \le x^i$ for some *i*. But no x^i is complete; hence x^* is not complete. Thus *x* is ≥-minimal and complete and thus $x \in G$.

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

Theorem 2.2. 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 $k \to \infty$, $(A^{-1}c^i + k\bar{e}_i)_j \to \infty$ (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 $c^i + kA\bar{e}_i > g'$. 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 $c^i + k(i)A\bar{e}_i \in M_{\mathbb{N}_0}$. 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

$$g^* = g + (K+1)A\bar{e}_i - (1/|A|)Ae_i,$$

$$S = [\succ g^*] \setminus [\succ g] \subseteq \{u \in \mathbb{Z}^n : (A^{-1}(u-g))_i = 0, (A^{-1}(u-g))_j \ge K+1 \ (j \ne i)\}.$$

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, for $j \neq i$,

$$(a)_{j} = \begin{cases} \left\lfloor (A^{-1}(u-g))_{j} \right\rfloor & \text{if } (A^{-1}(u-g))_{j} \notin \mathbb{Z}, \\ (A^{-1}(u-g))_{j} - 1 & \text{if } (A^{-1}(u-g))_{j} \in \mathbb{Z}, \end{cases}$$

Then $u' \in \mathbb{Z}^n \setminus M_{\mathbb{N}_0}$, since otherwise $u \in M_{\mathbb{N}_0}$. We also have $(A^{-1}(u'-g))_i = 0$ and $(A^{-1}(u'-g))_j \in (0, 1]$ 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 our hypothesis.

Our next result generalizes a one-dimensional reduction result in [Johnson 1960] 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 2.3. 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 $d^* \in \mathbb{N}$ with $d^*d \in 1 + |A|^2 \mathbb{N}_0$. For any $v \in Q^n$, we observe that $d^*dv - v \in \mathbb{N}_0 |A|^2 Q^n = \mathbb{N}_0 |A| \mathbb{Z}^n \subseteq A_{\mathbb{Z}}$; 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 $y \in \mathbb{N}_0^n$, 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, $d^*d(x+A1^n) = Ad^*(y+1^n) + d^*dBz$, 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 2.1, 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 2.1 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 $\theta^{-1}(g) \in G(M)$.

3. The MIN method

Let 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 [Brauer and Shockley 1962]; the following result shows that it characterizes the set G.

Theorem 3.1. 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 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 lub(N') ≥ $g + A_1$, 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 3.2. MIN
$$\subseteq \{Bx : x \in \mathbb{N}_0^m, \|x\|_1 \le |A| - 1\}.$$

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 $1 \le i \le n$. Set $w' = v' - e_i$, and w = Mw'. We see that $w \equiv v$, $w \le v$, and $w \in M_{\mathbb{N}_0}$; this contradicts that $v \in \text{MIN}$. Hence $\text{MIN} \subseteq B_{\mathbb{N}_0}$. Let $z = Bx \in \text{MIN}$. Suppose that $\|x\|_1 \ge |A|$. Start with 0 and increment one coordinate at a time, building a sequence $B0 = Bv_0 \le Bv_1 \le Bv_2 \le \cdots \le Bv_{\|x\|_1} = z$ 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 $Bv_a \le Bv_b$) 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 $y \le z$ and $y \equiv z$. This violates that $z \in \text{MIN}$. □

The following result, proved first in [Knight 1980] and rediscovered in [Simpson and Tijdeman 2003], generalizes the classical one-dimensional result on two generators that $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$. 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 3.4. *If* m = 1 *then* $G = \{|A|B - A_1 - B\}$.

Corollary 3.3. |G| is finite.

Proof. By Theorem 3.2, we have MIN = $\{0, B, 2B, \dots, (|A|-1)B\}$, a complete set of coset representatives. By Theorem 3.1, any $g \in G$ must have $g + A_1 = \text{lub}(MIN) = (|A|-1)B$.

Corollary 3.4 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 3.5. Consider a dense M = [A|B] with B a column $(n \times 1)$ vector, i.e., the special case m = 1. Let $C = [c_1, c_2, ..., c_m] \in \mathbb{N}^m$. 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 3.2, we have $MIN(M) = \{0, B, ..., (|A| - 1)B\}$. 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

$$\gcd(|A|, \{c_i s : 1 \le i \le m, s \in S\}) = \gcd(|A|, \gcd(c_1, c_2, \dots, c_m) \gcd(S))$$
$$= \gcd(|A|, \gcd(S)) = 1;$$

hence N is dense. Again by Theorem 3.2, we have $MIN(N) \subseteq B_{\mathbb{N}_0}$. 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 $qB \equiv 0 \mod A$ 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 $B\alpha = k|A|B + BCy = BCy$

 $A\left(k|A|A^{-1}B\right)+BCy\in M_{\mathbb{N}_0}$ (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 $\mathrm{lub}(T)=G(P)B+|A|B=\beta$. Let $g\in G(N)$, and let M be chosen as in Theorem 3.1 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 $\mathrm{lub}(M)\leq \mathrm{lub}(\mathrm{MIN}(N))\leq \mathrm{lub}(T)=G(P)B+|A|B=\beta$. 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.

Example 3.6. Consider $N = \begin{pmatrix} 5 & 0 & 84 & 105 \\ 0 & 4 & 84 & 105 \end{pmatrix}$. We have N = [A|BC], for $A = \begin{pmatrix} 5 & 0 \\ 0 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 3 \\ 3 \end{pmatrix}$, and C = (28, 35). Following Theorem 3.5, 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 $G(N) = \left\{ \begin{pmatrix} 646 \\ 647 \end{pmatrix} \right\}$.

We give three more results using this method. First, we present a \leq -bound for G. This generalizes a one dimensional bound, attributed to Schur in [Brauer 1942]: $g(a_1, a_2, \ldots, a_k) \leq a_1 a_k - a_1 - a_k$ (where $a_1 < a_2 < \cdots < a_k$). Note that Corollary 3.4 shows that equality is sometimes achieved.

Theorem 3.7. *For all* $g \in G$, $g \le \text{lub} (\{|A|b - A_1 - b : b \text{ a column of } B\}).$

Proof. Let $x \in MIN$, 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^* to be a column of B with $(A^{-1}b^*)_i$ maximal. By Theorem 3.2, we have that $(A^{-1}x)_i \leq (A^{-1}b^*)_i \|x'\|_1 \leq (A^{-1}b^*)_i (|A|-1)$. 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 3.1 and have $g + A_1 \leq \text{lub}(\text{MIN}) \leq \text{lub}(\{(|A|-1)b\})$.

Next, we characterize possible G in our context for the special case m=1. This generalizes a one-dimensional construction found in [Rosales et al. 2004]. If we allow m=2, then it is an open problem to determine whether all G are possible.

Theorem 3.8. Let $g \in \mathbb{Z}^n$. There exists a simplicial, dense, M with m = 1 and $G = \{g\}$ if and only if $\frac{1}{2}g \notin \mathbb{Z}^n$.

Proof. Suppose $\frac{1}{2}g \notin \mathbb{Z}^n$. By applying an invertible change of basis, if necessary, we assume without loss that $g \in \mathbb{N}^n$ and that $\frac{1}{2}(g)_1 \notin \mathbb{Z}$. 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 3.4 to get $G = \{g\}$, as desired. Suppose now that we have a simplicial dense M, with $G = \{g\}$ and $\frac{1}{2}g \in \mathbb{Z}^n$. Applying Corollary 3.4 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.

Our last result combines the two methods presented. It generalizes the onedimensional theorem $g(a, a+c, a+2c, ..., a+kc) = a \lceil (a-1)/k \rceil + ac - a - c$, as proved in [Roberts 1956]. The following determines G, for M of a similarly special type.

Theorem 3.9. Fix A and a vector $c \ge 0$. 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

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

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

Choose any $x \in \mathbb{N}_0^n$ satisfying $||x||_1 = \lceil (|A|-1)/k \rceil$. Set $T = \{Ax + c\gamma \in M_{\mathbb{N}_0} : 0 \le \gamma \le |A|-1\}$. 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 $h = \text{lub}(T) - A_1 = Ax + (|A|-1)c - A_1$. Note that each $t \in T$ either has $t \in V(h)$ or $t \le t'$ (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 3.1, 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.

Example 3.10. Consider $M = \begin{pmatrix} 5 & 0 & 7 & 2 & 9 & 4 & 11 & 6 & 13 & 8 & 15 & 10 & 17 & 12 & 19 & 14 \\ 0 & 4 & 1 & 5 & 2 & 6 & 3 & 7 & 4 & 8 & 5 & 9 & 6 & 10 & 7 & 11 \end{pmatrix}$. We see that M = [A|A+C|A+2C|A+3C|A+4C|A+5C|A+6C|A+7C] for $A = \begin{pmatrix} 5 & 0 \\ 0 & 4 \end{pmatrix}$ and

 $C = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$. M is dense since |A| = 20, |A + C| = 33 and gcd(20, 33) = 1. Applying Theorem 3.9, we get $G(M) = \left\{Ax + \begin{pmatrix} 33 \\ 15 \end{pmatrix} : x, \|x\|_1 = 3\right\} = \left\{\begin{pmatrix} 48 \\ 15 \end{pmatrix}, \begin{pmatrix} 43 \\ 19 \end{pmatrix}, \begin{pmatrix} 38 \\ 23 \end{pmatrix}, \begin{pmatrix} 33 \\ 27 \end{pmatrix}\right\}$.

Acknowledgements

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

References

[Brauer 1942] A. Brauer, "On a problem of partitions", *Amer. J. Math.* **64** (1942), 299–312. MR 3,270d Zbl 0061.06801

[Brauer and Shockley 1962] A. Brauer and J. E. Shockley, "On a problem of Frobenius", *J. Reine Angew. Math.* **211** (1962), 215–220. MR 26 #6113 Zbl 0108.04604

[Dedekind 1877] R. Dedekind, "Sur la théorie des nombres entiers algébriques", *Darboux Bull.* **9** (1877), 278. Translated as *Theory of algebraic integers*, Cambridge University Press, 1996.

[Frumkin 1981] M. A. Frumkin, "On the number of nonnegative integer solutions of a system of linear Diophantine equations", pp. 95–108 in *Studies on graphs and discrete programming* (Brussels, 1979), edited by P. Hansen, Ann. Discrete Math. 11, North-Holland, Amsterdam, 1981. MR 83k:10028 Zbl 0477,90048

[Ivanov and Shevchenko 1975] N. N. Ivanov and V. N. Shevchenko, "The structure of a finitely generated semilattice", *Dokl. Akad. Nauk BSSR* **19**:9 (1975), 773–774. In Russian. MR 52 #8075 Zbl 0312.10009

[Johnson 1960] S. M. Johnson, "A linear diophantine problem", *Canad. J. Math.* **12** (1960), 390–398. MR 22 #12074 Zbl 0096.02803

[Knight 1980] M. J. Knight, "A generalization of a result of Sylvester's", *J. Number Theory* **12**:3 (1980), 364–366. MR 81j:10019 Zbl 0441.10010

[Novikov 1992] B. V. Novikov, "On the structure of subsets of a vector lattice that are closed with respect to addition", *Ukrain. Geom. Sb.* 35 (1992), 99–103. In Russian; translated in *J. Math. Sci.* 72:4 (1994), 3223–3225. MR 95b:52027 Zbl 0850.06010

[Ramírez Alfonsín 2006] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and its Applications **30**, Oxford University Press, Oxford, 2006. MR 2007i:11052 Zbl 1134.11012

[Roberts 1956] J. B. Roberts, "Note on linear forms", Proc. Amer. Math. Soc. 7 (1956), 465–469.MR 19,1038d Zbl 0071.03902

[Rosales et al. 2004] 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 (2004), 5–12. MR 2004j;20117 Zbl 1077.20071

[Rycerz 2000] A. Rycerz, "The generalized residue classes and integral monoids with minimal sets", *Opuscula Math.* 20 (2000), 65–69. MR 2002k:11035

[Simpson and Tijdeman 2003] 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 (2003), 1661–1671. MR 2004k:11025 Zbl 1013.05087

[Vizvári 1987] B. Vizvári, "An application of Gomory cuts in number theory", *Period. Math. Hungar.* **18**:3 (1987), 213–228. MR 89d:11017 Zbl 0626.10013

[van der Waerden 1967] B. L. van der Waerden, *Algebra*, vol. 2, 5th ed., Heidelberger Taschenbücher **23**, Springer, Berlin, 1967. In German; translated as *Algebra*, vol. 2, Frederick Ungar, New York, 1970. MR 41 #8187b

Received: 2011-03-02 Revised: 2011-05-09 Accepted: 2011-05-09

jmamos1984@gmail.com Department of Mathematics, Kansas State University,

Manhattan, KS 66506, United States

ipascu@wellesley.edu Department of Economics,

Massachusetts Institute of Technology, 50 Memorial Drive,

Cambridge, MA 02142, United States

San Diego State University, 5500 Campanile Drive,

San Diego CA 92182-7720, United States http://www-rohan.sdsu.edu/~vadim/

Hanover, NH 03755, United States

yanzhang@fas.harvard.edu Department of Mathematics, Massachusetts Institute of

Technology, 50 Memorial Drive, 77 Massachusetts Avenue,

Cambridge, MA 02139-4307, United States



pjm.math.berkeley.edu/involve

EDITORS

MANAGING EDITOR

Kenneth S. Berenhaut, Wake Forest University, USA, berenhks@wfu.edu

BOARD OF EDITORS

	John V. Baxley	Wake Forest University, NC, USA baxley@wfu.edu	Chi-Kwong Li	College of William and Mary, USA ckli@math.wm.edu
1	Arthur T. Benjamin	Harvey Mudd College, USA benjamin@hmc.edu	Robert B. Lund	Clemson University, USA lund@clemson.edu
	Martin Bohner	Missouri U of Science and Technology, USbohner@mst.edu	SA Gaven J. Martin	Massey University, New Zealand g.j.martin@massey.ac.nz
	Nigel Boston	University of Wisconsin, USA boston@math.wisc.edu	Mary Meyer	Colorado State University, USA meyer@stat.colostate.edu
A	marjit S. Budhiraja	U of North Carolina, Chapel Hill, USA budhiraj@email.unc.edu	Emil Minchev	Ruse, Bulgaria eminchev@hotmail.com
	Pietro Cerone	Victoria University, Australia pietro.cerone@vu.edu.au	Frank Morgan	Williams College, USA frank.morgan@williams.edu
	Scott Chapman	Sam Houston State University, USA scott.chapman@shsu.edu	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran moslehian@ferdowsi.um.ac.ir
	Jem N. Corcoran	University of Colorado, USA corcoran@colorado.edu	Zuhair Nashed	University of Central Florida, USA znashed@mail.ucf.edu
	Michael Dorff	Brigham Young University, USA mdorff@math.byu.edu	Ken Ono	University of Wisconsin, USA ono@math.wisc.edu
	Sever S. Dragomir	Victoria University, Australia sever@matilda.vu.edu.au	Joseph O'Rourke	Smith College, USA orourke@cs.smith.edu
Bel	hrouz Emamizadeh	The Petroleum Institute, UAE bemamizadeh@pi.ac.ae	Yuval Peres	Microsoft Research, USA peres@microsoft.com
	Errin W. Fulp	Wake Forest University, USA fulp@wfu.edu	YF. S. Pétermann	Université de Genève, Switzerland petermann@math.unige.ch
	Andrew Granville	Université Montréal, Canada andrew@dms.umontreal.ca	Robert J. Plemmons	Wake Forest University, USA plemmons@wfu.edu
	Jerrold Griggs	University of South Carolina, USA griggs@math.sc.edu	Carl B. Pomerance	Dartmouth College, USA carl.pomerance@dartmouth.edu
	Ron Gould	Emory University, USA rg@mathcs.emory.edu	Bjorn Poonen	UC Berkeley, USA poonen@math.berkeley.edu
	Sat Gupta	U of North Carolina, Greensboro, USA sngupta@uncg.edu	James Propp	U Mass Lowell, USA jpropp@cs.uml.edu
	Jim Haglund	University of Pennsylvania, USA jhaglund@math.upenn.edu	Józeph H. Przytycki	George Washington University, USA przytyck@gwu.edu
	Johnny Henderson	Baylor University, USA johnny_henderson@baylor.edu	Richard Rebarber	University of Nebraska, USA rrebarbe@math.unl.edu
	Natalia Hritonenko	Prairie View A&M University, USA nahritonenko@pvamu.edu	Robert W. Robinson	University of Georgia, USA rwr@cs.uga.edu
(Charles R. Johnson	College of William and Mary, USA crjohnso@math.wm.edu	Filip Saidak	U of North Carolina, Greensboro, USA f_saidak@uncg.edu
	Karen Kafadar	University of Colorado, USA karen.kafadar@cudenver.edu	Andrew J. Sterge	Honorary Editor andy@ajsterge.com
	K. B. Kulasekera	Clemson University, USA kk@ces.clemson.edu	Ann Trenk	Wellesley College, USA atrenk@wellesley.edu
	Gerry Ladas	University of Rhode Island, USA gladas@math.uri.edu	Ravi Vakil	Stanford University, USA vakil@math.stanford.edu
	David Larson	Texas A&M University, USA larson@math.tamu.edu	Ram U. Verma	University of Toledo, USA verma99@msn.com
	Suzanne Lenhart	University of Tennessee, USA lenhart@math.utk.edu	John C. Wierman	Johns Hopkins University, USA wierman@jhu.edu

PRODUCTION Sheila Newbery, Senior Production Editor

See inside back cover or http://pjm.math.berkeley.edu/involve for submission instructions.

Silvio Levy, Scientific Editor

Cover design: ©2008 Alex Scorpan

The subscription price for 2011 is US \$100/year for the electronic version, and \$130/year (+\$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to

Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA. Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of

California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOWTM from Mathematical Sciences Publishers.



A NON-PROFIT CORPORATION

The visual boundary of \mathbb{Z}^2 Kyle Kitzmiller and Matt Rathbun	103
An observation on generating functions with an application to a sum of secant powers JEFFREY MUDROCK	117
Clique-relaxed graph coloring Charles Dunn, Jennifer Firkins Nordstrom, Cassandra Naymie, Erin Pitney, William Sehorn and Charlie Suer	127
Cost-conscious voters in referendum elections Kyle Golenbiewski, Jonathan K. Hodge and Lisa Moats	139
On the size of the resonant set for the products of 2×2 matrices Jeffrey Allen, Benjamin Seeger and Deborah Unger	157
Continuous <i>p</i> -Bessel mappings and continuous <i>p</i> -frames in Banach spaces MOHAMMAD HASAN FAROUGHI AND ELNAZ OSGOOEI	167
The multidimensional Frobenius problem JEFFREY AMOS, IULIANA PASCU, VADIM PONOMARENKO, ENRIQUE TREVIÑO AND YAN ZHANG	187
The Gauss–Bonnet formula on surfaces with densities IVAN CORWIN AND FRANK MORGAN	199