A Short Proof of Tight Bounds on the Smallest Support Size of Integer Solutions to Linear Equations

Yatharth Dubey*and Siyue Liu†

Tepper School of Business, Carnegie Mellon University

July 17, 2023

Abstract

In this note, we study the size of the support of solutions to linear Diophantine equations $Ax = b,\ x \in \mathbb{Z}^n$ where $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^n$. We give an asymptotically tight upper bound on the smallest support size, parameterized by $\|A\|_\infty$ and m, and taken as a worst case over all b such that the above system has a solution. This bound is asymptotically tight, and in fact matches the bound given in Aliev, Averkov, De Leora, Oertel [AADLO22], while the proof presented here is simpler, relying only on linear algebra. It removes a factor of order $\log\log(\sqrt{m}\,\|A\|_\infty)$ to the current best bound given in Aliev, De Loera, Eisenbrand, Oertel, Weismantel [ADLE+18].

1 Introduction

The main goal of this work is to establish upper and lower bounds on the smallest support size of solutions to linear Diophantine equations. Let $A \in \mathbb{Z}^{m\times n}$ be a matrix and denote by $\mathcal{L}(A) := \{Ax \mid x \in \mathbb{Z}^n\}$ the lattice generated by the columns of A. For any $b \in \mathcal{L}(A)$, we want to find an integer solution to $Ax = b$ with smallest support size, i.e.

$$\min\ \{\|x\|_0 \mid Ax = b, x \in \mathbb{Z}^n\}, \tag{1}$$

where $\|x\|_0 := |\{j\ :\ x_j \neq 0\}|$. We will assume without loss of generality that A has full row rank, i.e. $\operatorname{rank}(A) = m$, because the system is trivially satisfied if and only if the independent rows of A are satisfied. According to [Nat95], determining the exact solution to (1) is NP-hard. In this note, we study the largest value of (1) taken over all points b in the lattice $\mathcal{L}(A)$. To be precise,

*yathartd@andrew.cmu.edu
†siyueliu@andrew.cmu.edu

for matrix $A \in \mathbb{Z}^{m\times n}$, define $f(A)$ to be the maximum, taken over all $b \in \mathcal{L}(A)$, of the smallest support size of an integer solution to $Ax = b$, i.e.

$$f(A) := \max_{b\in\mathcal{L}(A)} \min \{\|x\|_0 \mid Ax = b, x \in \mathbb{Z}^n\}. \tag{2}$$

Note that this notion has been studied in the literature. For example, in [AADLO22], $f(A)$ is called the *integer linear rank* of A, denoted by $ILR(A)$. Nontrivial bounds on problem (2) have been leveraged in many areas of discrete optimization; see, for example, references in Section 1 of [AADLO22] and in the introduction of [ADLE+18].

As a result, there have been several studies focused on achieving increasingly strong upper bounds on Problem (2). Currently, the best available upper bound of $f(A)$ is achieved in [AADLO22], which we will elaborate on in Section 2.

We parameterize our bound on $f(A)$ by m and $\|A\|_\infty$. In particular, denote by $h(m,t)$ the maximum, taken over all integer matrices A with m rows with entries with absolute value no larger than t, and vectors $b \in \mathcal{L}(A)$, of the smallest support size of an integer solution to $Ax = b$, i.e.

$$\begin{aligned} h(m,t) &:= \max_{A\in\mathbb{Z}^{m\times n}, \|A\|_\infty\le t, b\in\mathcal{L}(A)} \min \{\|x\|_0 \mid Ax = b, x \in \mathbb{Z}^n\} \\ &= \max_{A\in\mathbb{Z}^{m\times n}, \|A\|_\infty\le t} f(A). \end{aligned} \tag{3}$$

There have been several efforts in obtaining good bounds for $h(m,t)$. As far as we know, the current explicitly stated best bound appears in [ADLE+18] as $h(m,t) \le 2m\log(2\sqrt{mt})$. We give the following bound in this paper.

Theorem 1.

$$h(m,t) \le O\left(\frac{m\log(\sqrt{m}\,t)}{\log\log(\sqrt{m}\,t)}\right). \tag{4}$$

The bound in (4) improves the bound in [ADLE+18] by a factor of order $\log\log(\sqrt{mt})$. To obtain this theorem, we prove the following result, which may be of independent interest.

Let A be an integer matrix with m rows and at least m columns. We will denote by $\Gamma(A)$ the largest absolute value of an $m\times m$ subdeterminant, i.e. determinant of an $m\times m$ submatrix of A. We denote by $\gcd(A)$ the greatest common divisor of all $\binom{n}{m}$ such subdeterminants of A, i.e.

$$\begin{aligned} \Gamma(A) &:= \max_B \{|\det(B)| \mid B \text{ is an } m\times m \text{ submatrix of } A\}; \\ \gcd(A) &:= \gcd\{|\det(B)| \mid B \text{ is an } m\times m \text{ submatrix of } A\}. \end{aligned}$$

Theorem 2. *Let A be an integer matrix with m rows and full row rank. Let p_i be the i-th prime. Then, the following relation between $\Gamma(A)$, $\gcd(A)$ and $f(A)$ holds.*

$$\frac{\Gamma(A)}{\gcd(A)} \ge p_2^m p_3^m \cdots p_{\left\lfloor\frac{f(A)}{m}\right\rfloor}^m p_{\left\lceil\frac{f(A)}{m}\right\rceil}^{f(A)-m\left\lfloor\frac{f(A)}{m}\right\rfloor}. \tag{5}$$

Furthermore, the bound is asymptotically tight in the sense that for arbitrarily large integers m and t, there exist an integer matrix A with m rows, full row rank, $\|A\|_\infty > t$, and a vector $b \in \mathcal{L}(A)$ such that equality holds in (5).

We will see how the bound (5) is comparable to the bound of [AADLO22]; in particular, the proof of Theorem 2 can easily be adapted to obtain the bound of [AADLO22].

We intend for this paper to stand out for the strength of its result, but also for its simplicity and readability.

Overview. In Section 2, we discuss related work and how the results of this paper compare with recent developments in bounding the support size of integer solutions to systems of equations/inequalities. In Section 3.1 we introduce the notion of integral independence, which will be useful throughout the proofs of Theorems 1 and 2. In particular, in Section 3.2, we achieve a nontrivial lower bound on the largest $m \times m$ subdeterminant of a matrix A with integrally independent columns, given by Theorem 1—furthermore, this bound increases with the number of columns. In Section 3.3, we use the relationship between the largest subdeterminant and largest entry given by the Hardamard bound, we achieve the upper bound on the number of columns, i.e. $h(m,t)$, given by Theorem 1. Finally, in Section 3.4 we exhibit the matrix A referred to in the latter statement of Theorem 2.

Notation. Throughout this paper we use p_i to denote the i-th prime number. In particular, $p_1 = 2$. For any $p, q \in \mathbb{Z}$, we use $p \mid q$ to denote that p divides q, i.e. $q/p \in \mathbb{Z}$; similarly, $p \nmid q$ to denote that p does not divide q; we may use this interchangeably with the language q is (respectively, is not) divisible by p. We use the convention that $\gcd(a,0) = |a|$ for any $a \in \mathbb{Z}$, including 0. We use the notation $[n] := \{1, 2, ..., n\}$, and, for positive integers $i \leq j$, $[i : j] := \{i, i+1, ..., j\}$. For any matrix $A \in \mathbb{R}^{m \times n}$, and $I \subseteq [m]$, $J \subseteq [n]$, we denote by $A_{I \times J}$ the submatrix of A consisting of rows indexed by I and columns indexed by J. For $x \in \mathbb{R}$, denote by $\lfloor x \rfloor$ the largest integer less than or equal to x; $\lceil x \rceil$ the smallest integer greater than or equal to x. We use $\mathbb{Z}^n_{\geq 0} := \{x \in \mathbb{Z}^n \mid x_j \geq 0 \text{ for all } j \in [n]\}$, and $\mathbb{R}^n_{\geq 0}$ analogously.

2 Related work

Problem (2) has garnered interest from multiple research disciplines. For example, an interesting problem is to find nonnegative integer solutions to $Ax = b$. Define the *integer conic hull* generated by the columns of A to be the vectors that can be represented as nonnegative integer combinations of the columns of A, i.e. $\text{int\_cone}(A) := \{Ax \mid x \in \mathbb{Z}^n_{\geq 0}\}$. Let

$$g(m,t) := \max_{A \in \mathbb{Z}^{m \times n},\ \|A\|_\infty \leq t,\ b \in \text{int\_cone}(A)} \min \{\|x\|_0 \mid Ax = b, x \in \mathbb{Z}^n_{\geq 0}\}. \tag{6}$$

It is easy to see that $h(m,t) \leq g(m,t)$, since any solution to $Ax = b,\ x \in \mathbb{Z}^n_{\geq 0}$ is also a solution to $Ax = b,\ x \in \mathbb{Z}^n$. Thus an upper bound on $g(m,t)$ can serve as an upper bound for $h(m,t)$. [ES06] establishes the first upper bound on $g(m,t)$ using the pigeonhole principle. They show $g(m,t) \leq 2m \log(4mt)$. The bound has been improved by [ADLE+18] to $g(m,t) \leq 2m \log(2\sqrt{mt})$ using Siegel's lemma [BV83]. These upper bounds on $g(m,t)$ have often been used as the best

available upper bound on $h(m,t)$. Note that the bound of Theorem 1 improves these bounds on $h(m,t)$ by a factor of $O(\log\log(\sqrt{mt}))$. [ADLE+18] also establishes an asymptotic lower bound for $g(m,t)$: for any $\epsilon > 0$, there exist a matrix $A \in \mathbb{Z}^{m\times n}$ with n/m large enough and a vector $b \in \text{int\_cone}(A)$, such that $\min\{\|x\|_0 \mid Ax = b, x \in \mathbb{Z}^n_{\geq 0}\} \geq m\log(\|A\|_\infty)^{\frac{1}{1+\epsilon}}$.

Another interesting direction is when the columns of matrix A form a *Hilbert basis*, i.e. $\{b : Ax, x \in \mathbb{Z}^n_{\geq 0}\} = \{b : Ax, x \in \mathbb{R}^n_{\geq 0}\} \cap \mathbb{Z}^n$; in other words, for any b in $\text{cone}(A) \cap \mathbb{Z}^n$, b is also in $\text{int\_cone}(A)$, where $\text{cone}(A) := \{Ax \mid x \in \mathbb{R}^n_{\geq 0}\}$. [CFS86] shows that when $\text{cone}(A)$ is pointed and the columns of A form an integral Hilbert basis, $g(m,t) \leq 2m-1$. [Seb90] improves this bound to $2m-2$. Note that the bound is independent of $\|A\|_\infty$.

As far as we know, the most relevant paper in the literature is [AADLO22], where they establish an upper bound for $f(A)$ and show that it is optimal. For any $z \in \mathbb{Z}_{>0}$, consider the prime factorization $z = q_1^{s_1}\cdots q_k^{s_k}$ such that $q_1, ..., q_k$ are pairwise distinct. [AADLO22] introduces $\Omega_m(z) := \sum_{i=1}^k \min\{s_i, m\}$, called *truncated prime* Ω*-funciton*. Let $\binom{[n]}{m}$ be all the subsets of $[n]$ of cardinality m and for $\tau \in \binom{[n]}{m}$, let A_τ be the $m\times m$ submatrix of A with columns indexed by τ. They show

$$f(A) \leq m + \min_{\tau\in\binom{[n]}{m},\det(A_\tau)\neq 0} \Omega_m\left(\frac{|\det(A_\tau)|}{\gcd(A)}\right). \tag{7}$$

They also show this bound is optimal in the sense that neither m can be replaced by any smaller constant nor the function Ω_m can be replaced by any smaller function.

The proof of bound (7) relies on the connection between the theory of finite Abelian groups and lattice theory. In particular, they use the *primary decomposition* theorem of finite Abelian groups (see e.g. Chapter 5.2 in [DF04]) and group representation of lattices (see e.g. Section 4.4 of [Sch98]). In contrast, the approach in this paper is significantly simpler, only using linear algebra. The proof is self-contained and does not require knowledge of group theory or lattice theory. Moreover, we will show how the bound (7) can be obtained as a byproduct of our proof of Theorem 2.

3 Proof of Theorems 1 and 2

3.1 Integral independence

We introduce the notion of integral independence in this section.

Definition 3. *A set of vectors $\{a_1, ..., a_n\}$ is called* integrally dependent *if there is some $k \in [n]$ such that $a_k = \sum_{i\neq k}\mu_i a_i$, where every μ_i is an integer, and* integrally independent *otherwise. Furthermore, if A is a matrix with integrally independent columns, we call the matrix itself integrally independent.*

The integral independence is closely related to the smallest support of integral solutions to equation $Ax = b$, which we will elaborate on in the following proposition.

Proposition 4. *Let A be a matrix with columns $a_1, ..., a_n \in \mathbb{Z}^m$. Then, the following are equivalent:*

1. *the vectors $\{a_1, ..., a_n\}$ are integrally independent;*
2. *there exists a vector $b \in \mathcal{L}(A)$ such that $\|x\|_0 = n$ for any integer solution x to $Ax = b$;*
3. *there is no integer vector in the null space of A with an entry equal to 1, i.e. $\{x \in \mathbb{Z}^n : Ax = 0,\ \exists j \in [n] \text{ such that } x_j = 1\} = \emptyset$.*

Proof. We start by proving (1) $\implies$ (2). Let $b = \sum_{i\in[n]} a_i$. Consider an integral vector $x \in \mathbb{Z}^n$ such that $\sum_{i\in[n]} a_i x_i = \sum_{i\in[n]} a_i$. For sake of contradiction, assume some component of x is zero; without loss of generality, assume $x_n = 0$. Then, $\sum_{i\in[n-1]} a_i x_i = \sum_{i\in[n]} a_i$. It follows that $a_n = -\sum_{i\in[n-1]}(1 - x_i)a_i$, where a_n is an integral combination of $\{a_1, ..., a_{n-1}\}$, a contradiction.

We now prove (2) $\implies$ (1). Let $b \in \mathcal{L}(A)$ be such that every integral x with $Ax = b$ has $\|x\|_0 = n$. Further let x' be one such choice of x and write $b = \sum_{i\in[n]} a_i x'_i$. Suppose for sake of contradiction that $\{a_1, ..., a_n\}$ is integrally dependent. Then, by definition, there is some $k \in [n]$ and $\mu \in \mathbb{Z}^{n-1}$ such that $a_k = \sum_{i\neq k} \mu_i a_i$. So, we can write

$$b = \sum_{i\neq k} a_i x'_i + \sum_{i\neq k} x'_k \mu_i a_i = \sum_{i\neq k} (x'_i + \mu_i x'_k) a_i.$$

It follows from x' and μ are both integral that each $(x'_i + \mu_i x'_k)$ is integral. Then, b can be written as an integral combination of $\{a_1, ..., a_n\} \setminus \{a_k\}$, contradicting the fact that $\|x\|_0 = n$ for every integral x such that $Ax = b$.

We now prove (1) $\implies$ (3). Suppose there is some $x \in \mathbb{Z}^n \setminus \{0\}$ such that $\sum_{i\in n} a_i x_i = 0$; and without loss of generality, assume $x_n = 1$. Then, we can rewrite this as $a_n = \sum_{i\in[n-1]} \frac{x_i}{x_n} a_i = \sum_{i\in[n-1]} x_i a_i$. Therefore, $\{a_1, ..., a_n\}$ is integrally dependent.

We now prove (3) $\implies$ (1). Suppose that $\{a_1, ..., a_n\}$ is integrally dependent. Then, by definition, there exists a $k \in [n]$ such that $a_k = \sum_{i\neq k} \mu_i a_i$, where every μ_i integer. Therefore, vector $\begin{pmatrix} -\mu_1 & -\mu_2 & \dots & -\mu_{k-1} & 1 & -\mu_{k+1} & \dots & \mu_n \end{pmatrix}$ is in the null space of A. □

3.2 Upper bound on $f(A)$

Applying unimodular column operations, we can bring A into Hermite normal form $H = \begin{pmatrix} D & 0 \end{pmatrix}$, where $D \in \mathbb{Z}^{m\times m}$ is a lower triangular matrix. We have the relation $AU = \begin{pmatrix} D & 0 \end{pmatrix}$, where $U \in \mathbb{Z}^{n\times n}$ is a unimodular matrix corresponding to the unimodular operations (see e.g. Section 1.5.2 in [CCZ+14]). To proceed, we remind readers of some basic facts about unimodular operations.

Fact 1. *Let C be any $m \times n$ integer matrix where $m \leq n$, and V be an $n \times n$ unimodular matrix. Then, the greatest common divisor (GCD) of all $m \times m$ subdeterminants of CV is equal to the GCD of all $m \times m$ subdeterminants of C.*

Fact 2. *The GCD of all $m \times m$ subdeterminants of C is zero (i.e. all $m \times m$ subdeterminants of C are 0) if and only if the rows of C are linearly dependent.*

The first fact follows from the GCD of all $m \times m$ subdeterminants of C being invariant under unimodular column operations (see, e.g., Section 4.4 of [Sch98]). To see the second fact, we can bring C into its Hermite normal form $\begin{pmatrix} C' & 0 \end{pmatrix}$ by applying unimodular column operations V, i.e. $CV = \begin{pmatrix} C' & 0 \end{pmatrix}$. By the first fact, the GCD of all $m \times m$ subdeterminants of C equals to that of CV, which is $\det(C')$. Thus, the GCD is 0 if and only if $\det(C') = 0$, which means the rows of C' are linearly dependent. Since V is unimodular and thus nonsingular, the rows of C' are linearly dependent if and only if the rows of C are linearly dependent. Furthermore, it may be useful to recall that the Hermite normal form of a matrix is unique. Due to these facts and the properties of unimodular matrices, we have the following lemma.

Lemma 5. *Let $A \in \mathbb{Z}^{m \times n}$ be a matrix with integrally independent columns. Let $H = AU$ be the Hermite normal form of A, where U is a unimodular matrix. Suppose $U = \begin{pmatrix} U_1 & U_2 \end{pmatrix}$, where $U_1 \in \mathbb{Z}^{n \times m}, U_2 \in \mathbb{Z}^{n \times (n-m)}$. Then U_2 must satisfy the following properties:*

(P1). U_2 has at least one nonsingular $(n-m) \times (n-m)$ submatrix.

(P2). The GCD of all $(n-m) \times (n-m)$ subdeterminants of U_2 is 1.

(P3). For each row i of U_2, there exists some prime $q_i \geq 2$ such that $q_i \mid (U_2)_{ij}$ for all $j \in [n-m]$.

Proof. It follows from $U^{-1}U = I$ that $U_2^\top (U^{-1})^\top = \begin{pmatrix} I_{n-m} & 0 \end{pmatrix}$. Together with the fact that $(U^{-1})^\top$ is unimodular we obtain that the Hermite normal form of $U_2^\top$ is the $(n-m) \times (n-m)$ identity martix I_{n-m}. According to Fact 1, the GCD of all $(n-m) \times (n-m)$ subdeterminants of U_2 equals to 1, proving (P2). In particular, it is nonzero and thus by Fact 2, U_2 has rank $n-m$ and therefore has a nonsingular $(n-m) \times (n-m)$ submatrix, proving (P1).

It remains to prove property (P3). Since $A \begin{pmatrix} U_1 & U_2 \end{pmatrix} = \begin{pmatrix} D & 0 \end{pmatrix}$, for $D \in \mathbb{Z}^{m \times m}$ some lower triangular matrix, we notice that columns of U_2 are in the null space of A. Since the columns of A are integrally independent, by Proposition 4, any integral x in the null space of A has no entry equal to 1. Suppose for the sake of contradiction, the entries in row i of U_2 have GCD 1. Then, by Bézout's theorem there exists an integral $\mu \in \mathbb{Z}^{n-m}$ such that $\sum_{j=1}^{n-m} \mu_j (U_2)_{ij} = 1$. Then $x = U_2 \mu$ is an integral vector in the null space of A with $x_i = 1$, which contradicts the integral independence of A. Therefore, for any row of U_2, its entries must have a common divisor strictly greater than 1, and therefore a prime that is at least 2. □

The following is key to derive Theorem 2 of this paper. It establishes a lower bound for the largest $m \times m$ subdeterminant of a matrix with integrally independent columns.

Theorem 6. *Let matrix $A \in \mathbb{Z}^{m \times n}$ be of full row rank with integrally independent columns. Let p_i be the i-th prime. Then,*

$$\frac{\Gamma(A)}{\gcd(A)} \geq p_2^m p_3^m \cdots p_{\lfloor \frac{n}{m} \rfloor}^m p_{\lceil \frac{n}{m} \rceil}^{n - m \lfloor \frac{n}{m} \rfloor}.$$

To prove this theorem, we need to introduce Jacobi's Theorem (see Theorem 2.5.2 of [Pra94]), which uses linear algebra to establish the relation between the subdeterminant of a matrix and its inverse.

Lemma 7. *[Jacobi] Let $A \in \mathbb{R}^{n\times n}$, $A = (a_{ij})_1^n$. For any $I, J \subseteq [n]$, denote $A_{I\times J}$ be the submatrix of A consisting of rows indexed by I and columns indexed by J. Let $A^* = (a^*_{ij})_1^n$ be the classical adjoint of A, where*

$$a^*_{ij} = (-1)^{i+j} \det(A_{[n]\setminus\{j\} \times [n]\setminus\{i\}})$$

is the cofactor of element a_{ji} in A. Let $\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}$ be an arbitrary permutation. Let $1 \le p \le n$. Let $I = \{i_1, ...i_p\}, J = \{j_1, ..., j_p\}, I' = \{i_{p+1}, ..., i_n\}, J' = \{j_{p+1}, ..., j_n\}$. Then,

$$\det(A^*_{I\times J}) = (-1)^\sigma \det(A_{J'\times I'}) \cdot \det(A)^{p-1}.$$

To prove Theorem 6, we will use the following direct corollary of Lemma 7.

Corollary 8. *Let $U \in \mathbb{R}^{n\times n}$ be a unimodular matrix. Then for any $I \subseteq [n], J \subseteq [n]$,*

$$det((U^{-1})_{I\times J}) = \pm det(U_{[n]\setminus J \times [n]\setminus I}), \tag{8}$$

where $U_{I\times J}$ denotes the submatrix of U consisting of rows indexed by I and columns indexed by J.

Proof of Theorem 6. Suppose by applying unimodular column operations, we bring A into Hermite normal form $H = \begin{pmatrix} D & 0 \end{pmatrix}$, where $D \in \mathbb{Z}^{m\times m}$ is a lower triangular matrix. We obtain the relation of $AU = \begin{pmatrix} D & 0 \end{pmatrix}$, where $U \in \mathbb{Z}^{n\times n}$ is a unimodular matrix. Let $U = \begin{pmatrix} U_1 & U_2 \end{pmatrix}$, where $U_1 \in \mathbb{Z}^{n\times m}, U_2 \in \mathbb{Z}^{n\times(n-m)}$.

Recall property (P3) of U_2 in Lemma 5 saying that for each row i of U_2, there exists some prime $q_i \ge 2$ such that $q_i \mid (U_2)_{ij}$ for all $j \in [n-m]$. For any prime q, let $I_q := \{i \in [n] : q \mid (U_2)_{ij}, \forall j \in [n-m]\}$ be the indices of rows of U_2 which are divisible by q. Notice for any prime q, U_2 must have a nonsingular $(n-m)\times(n-m)$ submatrix $(U_2)_{I\times[n-m]}$ with $I \subseteq [n] \setminus I_q$, $|I| = n-m$. Suppose for sake of contradiction that every nonsingular $(n-m)\times(n-m)$ submatrix of U_2 includes at least one row whose index is in I_q. Since such a row is divisible by q, the determinant of such a submatrix must also be divisible by q. Therefore if every nonsingular $(n-m)\times(n-m)$ submatrix of U_2 includes at least one such row, the GCD of the $\binom{n}{n-m}$ such subdeterminants is at least $q \ge 2$, contradicting property (P2) in Lemma 5. Therefore, by the pigeonhole principle, $|I_q| \le n - |I| = m$ for any prime q.

Recall p_i is the i-th prime and $q_i \ge 2$ is a prime that divides row i of U_2. The above argument implies that U_2 has a nonsingular $(n-m)\times(n-m)$ submatrix, denoted as V, whose row indices are in $[n] \setminus I_{p_1}$. Assume V consists of the first $n-m$ rows of U_2 without loss of generality. Then, we have

$$q_1 q_2 \cdots q_{n-m} \Big| |\det(V)|$$

Notice that each prime p_i appears at most m times among $\{q_1, ..., q_{n-m}\}$, since $|I_q| \leq m$ for any prime q and p_1 never appears in $\{q_1, ..., q_{n-m}\}$. It follows from $\det(V) \neq 0$ that

$$|\det(V)| \geq q_1 q_2 \cdots q_{n-m} \geq p_2^m p_3^m \cdots p_{\lfloor \frac{n}{m} \rfloor}^m p_{\lceil \frac{n}{m} \rceil}^{n-m\lfloor \frac{n}{m} \rfloor}.$$

Moreover, we use the relation between the determinant of the submatrix of A and U to bound above $\det(V)$. Notice $A = \begin{pmatrix} D & 0 \end{pmatrix} U^{-1}$ and thus $A_{[m]\times[n-m+1:n]} = D \cdot (U^{-1})_{[m]\times[n-m+1:n]}$. We have

$$\begin{aligned} |\det(A_{[m]\times[n-m+1:n]})| &= |\det(D)| \cdot |\det((U^{-1})_{[m]\times[n-m+1:n]})| \\ &= \gcd(A) \cdot |\det((U^{-1})_{[m]\times[n-m+1:n]})| \\ &= \gcd(A) \cdot |\det(U_{[n-m]\times[m+1:n]})| \\ &= \gcd(A) \cdot |\det(V)|, \end{aligned}$$

where the second equality follows from Fact 1 and the third equality follows from Corollary 8. Recall $\Gamma(A)$ is the largest absolute value of an $m \times m$ subdeterminant of A. Combining them together we obtain

$$\begin{aligned} \frac{\Gamma(A)}{\gcd(A)} &\geq \frac{|\det(A_{[m]\times[n-m+1:n]})|}{\gcd(A)} \\ &= |\det(V)| \\ &\geq p_2^m p_3^m \cdots p_{\lfloor \frac{n}{m} \rfloor}^m p_{\lceil \frac{n}{m} \rceil}^{n-m\lfloor \frac{n}{m} \rfloor}, \end{aligned}$$

as desired. □

Recall from Proposition 4 that a matrix A has integrally independent columns if and only if there exists some b such that every integer solution to $Ax = b$ has full support. Taking advantage of this observation, Theorem 6 can be naturally adapted to derive an upper bound for $f(A)$, i.e. the maximum, taken over $b \in \mathcal{L}(A)$, of smallest support size of an integer solution to $Ax = b$ (formally defined in (2)). This yields the proof of one of our main results.

Proof of Theorem 2. Take b such that $Ax = b$ has maximum smallest support size of an integer solution to $Ax = b$, i.e. $\min\{\|x\|_0 \mid Ax = b, x \in \mathbb{Z}^n\} = f(A)$. Let x^* be an integral solution to $Ax = b$ with smallest support, i.e. $\|x^*\|_0 = f(A)$. We can assume without loss of generality that $A \in \mathbb{Z}^{m \times f(A)}$ by deleting the columns j of A corresponding to $x_j^* = 0$ for $j \in [n]$. This will not increase $\Gamma(A)$, the largest $m \times m$ subdeterminant of A, and will not decrease $\gcd(A)$, the GCD of all $m \times m$ subdeterminants of A (this is easily seen by the fact that redundant columns can be zeroed out using unimodular column operations). Thus it suffices to prove inequality (5) after deleting redundent columns of A. By the minimality of support size of x^*, any integer solution to $Ax = b$ has full support. By Proposition 4, columns of A are integrally independent. It follows from Theorem 6 that inequality (5) holds. □

Remark 1. *We demonstrate how to modify the proof of Theorem 6 to obtain the bound (7) given in [AADLO22]. We use the same notation as in the proof of Theorem 6. For any $m \times m$ submatrix of A*

whose columns are indexed by J where $|J| = m$, we have

$$\begin{aligned}|\det(A_{[m]\times J})| &= |\det(D)| \cdot |\det((U^{-1})_{[m]\times J})| \\ &= \gcd(A) \cdot |\det((U^{-1})_{[m]\times J})| \\ &= \gcd(A) \cdot |\det(U_{[n]\setminus J \times [m+1:n]})|.\end{aligned}$$

We also know that

$$\prod_{i\in[n]\setminus J} q_i \,\Big|\, |\det(U_{[n]\setminus J \times [m+1:n]})|,$$

and thus

$$\prod_{i\in[n]\setminus J} q_i \,\Big|\, \frac{|\det(A_{[m]\times J})|}{\gcd(A)},$$

where $q_i, i \in [n]\setminus J$ are primes numbers and with the same prime repeating at most m times in $\{q_i \mid i \in [n]\setminus J\}$. Recall notation $\Omega_m(z) = \sum_{i=1}^{k} \min\{s_i, m\}$ for the prime factorization of $z = r_1^{s_1} \cdots r_k^{s_k}$ with multiplicities $s_1, ..., s_k \in \mathbb{Z}_{>0}$. Clearly, when $x \mid y$, $\Omega_m(x) \le \Omega_m(y)$. Thus, $\Omega_m\left(\prod_{i\in[n]\setminus J} q_i\right) \le \Omega_m\left(\frac{|\det(A_{[m]\times J})|}{\gcd(A)}\right)$. Moreover, since the multiplicity of each q_i in $\prod_{i\in[n]\setminus J} q_i$ is at most m, we have $\Omega_m\left(\prod_{i\in[n]\setminus J} q_i\right) = |[n]\setminus J| = n-m$. Therefore, $n-m \le \Omega_m\left(\frac{|\det(A_{[m]\times J})|}{\gcd(A)}\right)$. Since J is an arbitrary subset of $[n]$ with cardinality m, we obtain $n \le m + \min_{\tau\in\binom{[n]}{m},\det(A_\tau)\neq 0} \Omega_m\left(\frac{|\det(A_\tau)|}{\gcd(A)}\right)$. Applying the same argument as in the proof of Theorem 2 above, we obtain $f(A) \le m + \min_{\tau\in\binom{[n]}{m},\det(A_\tau)\neq 0} \Omega_m\left(\frac{|\det(A_\tau)|}{\gcd(A)}\right)$.

3.3 Upper bound on $h(m,t)$

Recall $h(m,t)$ is the maximum, taken over all integer matrices A with m rows and largest entry t, of the smallest support size of an integer solution to $Ax = b$ for some $b \in \mathcal{L}(A)$ (formally defined in (3)). Using a relation between the size of largest entry of a matrix and the size of its subdeterminant, we want to use results in Section 3.2 to obtain an upper bound for $h(m,t)$. We will use the well-known Hadamard inequality [Had93], which gives us an upper bound on the determinant of a matrix, i.e. for any matrix $B \in \mathbb{R}^{m\times m}$,

$$|\det(B)| \le (\sqrt{m}\,\|B\|_\infty)^m.$$

Applying this to inequality (5), we obtain the following corollary.

Corollary 9. *$h(m,t)$ satisfies*

$$(\sqrt{m}\,t)^m \ge p_2^m p_3^m \cdots p_{\lfloor\frac{h(m,t)}{m}\rfloor}^m p_{\lceil\frac{h(m,t)}{m}\rceil}^{h(m,t)-m\lfloor\frac{h(m,t)}{m}\rfloor}. \tag{9}$$

Proof. Suppose $A \in \mathbb{Z}^{m\times n}$ is a full row rank matrix with $\|A\|_\infty \le t$ and $b \in \mathcal{L}(A)$ such that it has the smallest support of any integer solution to $Ax = b$ is the maximum possible, i.e. $\min\{\|x\|_0 \mid Ax = b, x \in \mathbb{Z}^n\} = h(m,t)$. Then inequality (9) follows directly from Theorem 2 and Hadamard's inequality. □

Furthermore, we can prove the upper bound on $h(m,t)$ of Theorem 1 by applying prime number theorem to approximate the product of the first k primes $\prod_{i=1}^{k} p_i$.

Proof of Theorem 1. According to the prime number theorem, the product of the first k primes $\prod_{i=1}^{k} p_i \sim e^{(1+o(1))k\log k}$, where $\log(\cdot)$ is the natural logarithm (see e.g. [Zag97]). Let $n = h(m,t)$. Relaxing (9), we have

$$(\sqrt{m}\,t)^m \geq p_2^m p_3^m \cdots p_{\lfloor \frac{n}{m} \rfloor}^m p_{\lceil \frac{n}{m} \rceil}^{n-m\lfloor \frac{n}{m} \rfloor} \geq (p_1 p_2 \cdots p_{\lfloor \frac{n}{m} \rfloor})^m / 2^m.$$

Taking logarithm and applying $\prod_{i=1}^{k} p_i \sim e^{(1+o(1))k\log k}$, we have

$$\log(\sqrt{m}\,t) \geq \log(p_1 p_2 \cdots p_{\lfloor \frac{n}{m} \rfloor}) - \log 2 \geq C \left\lfloor \frac{n}{m} \right\rfloor \log \left\lfloor \frac{n}{m} \right\rfloor$$

for some constant C.

We claim that $\lfloor \frac{n}{m} \rfloor = O\left(\frac{\log(\sqrt{m}\,t)}{\log\log(\sqrt{m}\,t)} \right)$. Suppose not, we assume $\lfloor \frac{n}{m} \rfloor > \frac{2\log(\sqrt{m}\,t)}{C\log\log(\sqrt{m}\,t)}$ for some m that is arbitrarily large. Thus,

$$\log(\sqrt{m}\,t) \geq C \left\lfloor \frac{n}{m} \right\rfloor \log \left\lfloor \frac{n}{m} \right\rfloor > \frac{2\log(\sqrt{m}\,t)}{\log\log(\sqrt{m}\,t)} \Big(\log\log(\sqrt{m}\,t) - \log\big(C\log\log(\sqrt{m}\,t)\big) \Big).$$

This will give us

$$2\log\big(C\log\log(\sqrt{m}\,t)\big) > \log\log(\sqrt{m}\,t),$$

which is not going to hold when m is arbitrarily large, a contradiction. Thus, we have $\lfloor \frac{n}{m} \rfloor = O\left(\frac{\log(\sqrt{m}\,t)}{\log\log(\sqrt{m}\,t)} \right)$. It follows that $n = O\left(\frac{m\log(\sqrt{m}\,t)}{\log\log(\sqrt{m}\,t)} \right)$. □

3.4 Lower bound on $f(A)$

Finally, we prove the latter statement of Theorem 2 by giving an example integer matrix A with arbitrarily large number of rows m and $\|A\|_\infty$, showing that the upper bound on $f(A)$ is asymptotically tight. A similar construction has appeared in [ADLE+18, AADLO22] to prove lower bounds on support size of integer solutions.

Proposition 10. *For arbitrarily large (m,t), there exists A with m rows, full row rank, and $\|A\|_\infty > t$, and $b \in \mathcal{L}(A)$ such that equality holds in (5). In other words, the bound in Theorem 2 is asymptotically tight.*

Proof. Let p_i be the i-th prime. There exists k such that $p_2 p_3 \cdots p_k > t$. Let $n = km$. Define $A \in \mathbb{Z}^{m\times n}$ as

$$A_{ij} = \begin{cases} p_1 p_2 \cdots p_k / p_r & j = (i-1)k + r,\ 1 \leq r \leq k \\ 0 & o.w. \end{cases}$$

and $b = A\mathbf{1}$. Then, $\|A\|_\infty = p_2 p_3 \cdots p_k > t$. For any $i \in [m]$, $b_i = \sum_{r=1}^{k} p_1 p_2 \cdots p_k / p_r$. Observe that $p_j \nmid b_i, \forall i = 1, ..., m, j = 1, ..., k$. Any $x \in \mathbb{Z}^n$ with $\|x\|_0 < n$ would have $x_j = 0$ for some $j = (i-1)k+r$ with $1 \leq r \leq k$. Thus, $(Ax)_i = \sum_{s=1, s\neq r}^{k} (p_1 p_2 \cdots p_k / p_s) x_{(i-1)k+s}$. Since $p_r \mid (p_1 p_2 \cdots p_k / p_s)$, $\forall s \neq r$, we have $p_r \mid (Ax)_i$. Thus, $Ax \neq b$, which means any integer x with $\|x\|_0 < n$ is not a solution to $Ax = b$. Therefore, any integer solution of $Ax = b$ has smallest support size $n = km$. Moreover, $\Gamma(A) = \max_B \{|\det(B)| \mid B \text{ is an } m \times m \text{ submatrix of } A\} = p_2^m p_3^m \cdots p_k^m$, matching the right hand side in (5). □

Acknowledgements

This work was supported by ONR grant N00014-22-1-2528 and a Balas PhD Fellowship. We acknowledge the invaluable discussions with Ahmad Abdi, Gérard Cornuéjols, and Levent Tunçel, without whom this project would not have been possible. We also thank Ahmad Abdi and Timm Oertel for feedback that very much improved the presentation of these results.

Declarations

The authors have no conflicts of interest or competing interests.

References

[AADLO22] Iskander Aliev, Gennadiy Averkov, Jesús A De Loera, and Timm Oertel. Sparse representation of vectors in lattices and semigroups. *Mathematical Programming*, 192(1-2):519–546, 2022.

[ADLE+18] I Aliev, JA De Loera, F Eisenbrand, T Oertel, and R Weismantel. The support of integer optimal solutions. *SIAM Journal on Optimization*, 28(3):2152–2157, 2018.

[BV83] Enrico Bombieri and Jeffrey Vaaler. On siegel's lemma. *Inventiones mathematicae*, 73(1):11–32, 1983.

[CCZ+14] Michele Conforti, Gérard Cornuéjols, Giacomo Zambelli, et al. *Integer programming*, volume 271. Springer, 2014.

[CFS86] William Cook, Jean Fonlupt, and Alexander Schrijver. An integer analogue of caratheodory's theorem. *Journal of Combinatorial Theory, Series B*, 40(1):63–70, 1986.

[DF04] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[ES06] Friedrich Eisenbrand and Gennady Shmonin. Carathéodory bounds for integer cones. *Operations Research Letters*, 34(5):564–568, 2006.

[Had93] Jacques Hadamard. Resolution d'une question relative aux determinants. *Bull. des sciences math.*, 2:240–246, 1893.

[Nat95] Balas Kausik Natarajan. Sparse approximate solutions to linear systems. *SIAM journal on computing*, 24(2):227–234, 1995.

[Pra94] Viktor Vasil_evich Prasolov. *Problems and theorems in linear algebra*, volume 134. American Mathematical Soc., 1994.

[Sch98] Alexander Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1998.

[Seb90] András Sebö. Hilbert bases, caratheodory's theorem and combinatorial optimization. In *Proceedings of the 1st Integer Programming and Combinatorial Optimization Conference*, pages 431–455, 1990.

[Zag97] Don Zagier. Newman's short proof of the prime number theorem. *The American mathematical monthly*, 104(8):705–708, 1997.