

The Support of Integer Optimal Solutions

I. Aliev, J. De Loera, F. Eisenbrand, T. Oertel, and R. Weismantel

December 27, 2017

Abstract

The support of a vector is the number of nonzero-components. We show that given an integral $m \times n$ matrix A , the integer linear optimization problem $\max \{ \mathbf{c}^T \mathbf{x} : A\mathbf{x} = \mathbf{b}, \mathbf{x} \geq \mathbf{0}, \mathbf{x} \in \mathbb{Z}^n \}$ has an optimal solution whose support is bounded by $2m \log(2\sqrt{m}\|A\|_\infty)$, where $\|A\|_\infty$ is the largest absolute value of an entry of A . Compared to previous bounds, the one presented here is independent on the objective function. We furthermore provide a nearly matching asymptotic lower bound on the support of optimal solutions.

Introduction

We consider the integer optimization problem in standard form

$$\max \{ \mathbf{c}^T \mathbf{x} : A\mathbf{x} = \mathbf{b}, \mathbf{x} \geq \mathbf{0}, \mathbf{x} \in \mathbb{Z}^n \}, \quad (1)$$

where $A \in \mathbb{Z}^{m \times n}$, $\mathbf{b} \in \mathbb{Z}^m$ and $\mathbf{c} \in \mathbb{Z}^n$. For convenience, we will assume throughout this paper that Problem (1) is feasible. We will also assume without loss of generality that the matrix A has full row rank, i.e., $\text{rank}(A) = m$.

For a vector $\mathbf{x} \in \mathbb{R}^n$, let $\text{supp}(\mathbf{x}) := \{i \in \{1, \dots, n\} : x_i \neq 0\}$ denote the *support* of \mathbf{x} . The main purpose of this paper is to establish lower and upper bounds on the minimal size of support of an optimal solution to Problem (1) which are polynomial in m and the largest binary encoding length of an entry of A . Polynomial support bounds for integer programming [5, 1] have been successfully used in many areas such as in logic and complexity, see [14, 12] in the design of efficient polynomial-time approximation schemes [10, 11], in fixed parameter tractability [13, 16] and they were an ingredient in the solution of cutting stock with a fixed number of item types [8]. These previous bounds however were tailored for the integer feasibility problem only and thus depend on the largest encoding length of a component of the objective function vector if applied to the optimization problem (1). We believe that the observation that we lay out in this paper, namely that these bounds are independent of the objective function, will find further applications in algorithms and complexity.

Note that the support of an optimal solution of the linear relaxation of (1) is well-understood: if we denote by \mathbf{x}^* a vertex of the polyhedron $P(A, \mathbf{b}) := \{\mathbf{x} \in \mathbb{R} : A\mathbf{x} = \mathbf{b}, \mathbf{x} \geq 0\}$ that corresponds to the linear optimum, then from the theory of linear programming we know that \mathbf{x}^* is determined by a basis B with $\mathbf{x}_B^* = A_B^{-1}\mathbf{b}$ and $x_i^* = 0$ for all $i \in N := \{1, \dots, n\} \setminus B$. In particular, $\text{supp}(\mathbf{x}^*)$ is bounded by m alone. As we will see in this paper (cf. [1]), the story is much more complicated for integer linear programs.

Throughout this paper $\log(\cdot)$ will denote the logarithm with base two and $\|A\|_\infty$ will denote the maximum absolute entry of the matrix A . The first result of this paper shows that Problem 1 has an optimal solution with support of size not exceeding a bound that only depends on m and $\|A\|_\infty$ and independent of n .

Theorem 1 (Upper bound on the discrete support function). *There exists an optimal solution \mathbf{z}^* for Problem (1) such that*

$$|\text{supp}(\mathbf{z}^*)| \leq m + \log \left(g^{-1} \sqrt{\det(AA^T)} \right) \leq 2m \log(2\sqrt{m}\|A\|_\infty), \quad (2)$$

where g denotes the greatest common divisor of all $m \times m$ minors of A .

This theorem cannot be directly derived from the statements in [5, Theorem 1] and [1, Theorem 1.1] for the following reason. To guarantee optimality of \mathbf{y}^* , the objective function vector \mathbf{c} would have to become part of the constraint matrix (see [1, Corollary 1.3]). This, however, does not allow us to bound the support solely in terms of A . The resulting bound would have to depend also on \mathbf{c} .

Our strategy to prove Theorem 1 is based on a refinement of the proofs for results established in [5, Theorem 1] and [1, Theorem 1.1]. Specifically, in [5, Theorem 1] it was shown that there exists an integer point $\mathbf{y}^* \in P(A, \mathbf{b})$ with support bounded by $2m \log(4m\|A\|_\infty)$. This bound was recently improved in [1, Theorem 1.1] to

$$|\text{supp}(\mathbf{y}^*)| \leq m + \log \left(g^{-1} \sqrt{\det(AA^T)} \right). \quad (3)$$

Notice that an upper bound on the support of an optimal solution in the form of a function in m cannot be expected. This would imply that, for fixed m , one can optimize in polynomial time by first guessing the support of an optimal solution and then finding a solution using Lenstra's algorithm for integer programming in fixed dimension [15]. However, also for fixed m , the optimization problem (1) is *NP*-hard [7].

The next result of this paper implies that the upper bound established in Theorem 1 is nearly optimal. In fact, we consider a more general setting, where we drop the nonnegativity constraints and estimate from below the

size of support of all integer solutions to a suitable underdetermined system $A\mathbf{x} = \mathbf{b}$. The obtained bound depends only on m and $\|A\|_\infty$ and is independent of n and \mathbf{b} . Under the nonnegativity constraints and provided that $m \geq 2$, a lower bound can be derived from an example given in [5].

Theorem 2 (Lower bound on the discrete support function). *For any $\varepsilon > 0$ there exists a natural number N_ε such that the following holds. Let $m, n \in \mathbb{N}$, where $\frac{n}{m} > N_\varepsilon$. Then, there exists a matrix $A \in \mathbb{Z}^{m \times n}$, and a vector $\mathbf{b} \in \mathbb{Z}^m$, such that Problem (1) is feasible and*

$$|\text{supp}(\mathbf{z})| \geq m \log(\|A\|_\infty)^{\frac{1}{1+\varepsilon}},$$

for all $\mathbf{z} \in \mathbb{Z}^n$ with $A\mathbf{z} = \mathbf{b}$.

Our main results have three implications that we outline next:

First we consider the *integer hull* P_I of the polyhedron $P = P(A, \mathbf{b})$, i.e., $P_I = \text{conv}(P \cap \mathbb{Z}^n)$. It was proved by Cook et al. [4, Theorem 2.1] that for a generic rational polyhedron P the number of vertices of P_I is bounded by $2m^n(n^2 \log(\|A\|_\infty))^{n-1}$. For polyhedra in standard form Theorem 1 leads to an upper bound on the number of vertices of the integer hull of P that is polynomial in n , provided that m is a constant.

To see this, let \mathbf{z}^* be a vertex of P_I . There exists $\mathbf{c} \in \mathbb{Z}^n$, such that \mathbf{z}^* is the unique optimum with respect to Problem (1). Taking a vertex \mathbf{x}^* of P that gives an optimal solution of the corresponding continuous relaxation, we can associate every vertex of P_I to at least one vertex of P . Note, that P itself has no more than n^m vertices. By [6, Theorem 6], we can assume that $\|\mathbf{x}^* - \mathbf{z}^*\|_1 \leq m(2m\|A\|_\infty + 1)^m$, where $\|\cdot\|_1$ denotes the ℓ_1 -norm.

From Theorem 1 it follows that every vertex \mathbf{z}^* of P_I has support of size at most $2m \log(2\sqrt{m}\|A\|_\infty)$. Thus, P_I has no more than

$$n^m \cdot n^{2m \log(2\sqrt{m}\|A\|_\infty)} \cdot (m(2m\|A\|_\infty + 1)^m)^{2m \log(2\sqrt{m}\|A\|_\infty)}$$

vertices. Summarizing, we obtain

Corollary 3. *The number of vertices of the integer hull P_I is bounded by*

$$(mn\|A\|_\infty)^{O(m^2 \log(\sqrt{m}\|A\|_\infty))}.$$

A second consequence of Theorem 1 is the following extension to mixed integer optimization problems.

Corollary 4. *There exists an optimal solution \mathbf{z}^* for the mixed-integer optimization problem*

$$\max \left\{ \mathbf{c}^T \mathbf{x} : A\mathbf{x} = \mathbf{b}, \mathbf{x} \geq \mathbf{0}, \mathbf{x} \in \mathbb{Z}^n \times \mathbb{R}^d \right\},$$

such that

$$|\text{supp}(\mathbf{z}^*)| \leq 2m + \log \left(g^{-1} \sqrt{\det(AA^T)} \right) \leq m + 2m \log(2\sqrt{m}\|A\|_\infty).$$

Given a positive integer k , an integer matrix A is called k -modular if all its absolute subdeterminants are bounded by k . Theorem 1 immediately implies the following result.

Corollary 5. *Fix a positive integer k . For a k -modular matrix A , Problem (1) has an optimal solution with the size of support bounded by a polynomial in m .*

Proofs of Theorem 1 and Theorem 2

We will describe the refinement of the proofs established in [5] and [1]. In the proofs of both of these results the key idea is to show that if the support of a feasible solution is large, specifically if the bound (3) is violated, then there exists a certain nonzero integer vector $\mathbf{y} \in \{-1, 0, 1\}^n$ in $\ker(A) := \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} = \mathbf{0}\}$. This vector can then be used to perturb the feasible solution and decrease its support. We show that if (2) is violated, then there exists such a vector \mathbf{y} that satisfies additionally $\mathbf{c}^T \mathbf{y} = 0$. This allows us to perturb an optimal solution and decrease its support while remaining optimal. As in [1], we will utilize the following result by Bombieri and Vaaler.

Theorem 6 ([2, Theorem 2]). *There exist $n-m$ linearly independent integral vectors $\mathbf{y}_1, \dots, \mathbf{y}_{n-m} \in \ker(A) \cap \mathbb{Z}^n$ satisfying*

$$\prod_{i=1}^{n-m} \|\mathbf{y}_i\|_\infty \leq g^{-1} \sqrt{\det(AA^T)},$$

where g is the greatest common divisor of all $m \times m$ subdeterminants of A .

Proof of Theorem 1. In [1, Theorem 1.1 (ii)] it was verified that the second inequality in (2) always holds. Therefore we only need to prove that the first inequality in (2) holds. For that, let \mathbf{z}^* be an optimal solution for Problem (1) with minimal support.

First, we argue that it suffices to consider the case $|\text{supp}(\mathbf{z}^*)| = n$. Suppose that $|\text{supp}(\mathbf{z}^*)| < n$. For $S = \text{supp}(\mathbf{z}^*)$ define $\bar{A} = A_S$, the submatrix of A whose columns are labeled by the indices of S . Let $\bar{\mathbf{b}} = \mathbf{b}$, $\bar{\mathbf{c}} = \mathbf{c}_S$, and $\bar{\mathbf{z}}^* = \mathbf{z}_S^*$. By removing linearly dependent rows from $\bar{A}\bar{\mathbf{x}} = \bar{\mathbf{b}}$, we may assume that \bar{A} has full row rank. Let $\bar{m} = \text{rank}(\bar{A}) \leq m$. Observe that $\bar{\mathbf{z}}^*$ is an optimal solution for the corresponding Problem (1) with minimal support. Furthermore, note that $\bar{\mathbf{z}}^*$ has full support. Now, if (2) holds true for $\bar{\mathbf{z}}^*$, then by [1, Lemma 2.3] we have

$$|\text{supp}(\mathbf{z}^*)| = |\text{supp}(\bar{\mathbf{z}}^*)| \leq \bar{m} + \bar{g}^{-1} \sqrt{\det(\bar{A}\bar{A}^T)} \leq m + g^{-1} \sqrt{\det(AA^T)},$$

where \bar{g} denotes the greatest common divisor of all $\bar{m} \times \bar{m}$ minors of \bar{A} .

From now on, suppose that $|\text{supp}(\mathbf{z}^*)| = n > m + \log(g^{-1}\sqrt{\det(AA^T)})$. This inequality implies that $g^{-1}\sqrt{\det(AA^T)} < 2^{n-m}$. By Theorem 6, there exists a vector $\mathbf{y} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ such that

$$A\mathbf{y} = \mathbf{0} \quad \text{and} \quad \|\mathbf{y}\|_\infty \leq \left(g^{-1}\sqrt{\det(AA^T)}\right)^{1/(n-m)} < 2.$$

In particular, this implies that $y_i \in \{-1, 0, 1\}$ for all $i \in \{1, \dots, n\}$. Since $z_i^* > 0$ for all $i \in \{1, \dots, n\}$, it follows that $\mathbf{z}^* + \mathbf{y}$ and $\mathbf{z}^* - \mathbf{y}$ are feasible. As \mathbf{z}^* is optimal, it also follows that $\mathbf{c}^T \mathbf{y} = 0$. Otherwise $\mathbf{c}^T(\mathbf{z}^* + \mathbf{y})$ or $\mathbf{c}^T(\mathbf{z}^* - \mathbf{y})$ would be larger.

We may assume that $y_i < 0$ for at least one i . Otherwise, replace \mathbf{y} by $-\mathbf{y}$. Let $\lambda = \min\{z_i^* : y_i < 0\}$. Now, by construction $\mathbf{z}^* + \lambda\mathbf{y}$ is an optimal solution to (1) with support strictly smaller than n . The obtained contradiction completes the proof. \square

Now we discuss the proof of Theorem 2. Assuming that the columns of A form a Hilbert basis, Cook et al. [3] showed that the support of an optimal solution can be bounded solely in terms of m . In the same article the authors constructed an example showing that such a result cannot hold for more general A . We extend their construction as follows.

Let $p_i \in \mathbb{N}$ denote the i -th prime number. The i -th *primorial* $p_i\#$ is defined as the product of the first i prime numbers, that is

$$p_i\# := \prod_{j=1}^i p_j.$$

Based on the Prime Number Theorem (see e.g., [9, Theorem 6]) the asymptotical growth of primorials is well known to be

$$p_i\# = e^{(1+o(1))i \ln(i)}, \quad (4)$$

where $\ln(\cdot)$ denotes the natural logarithm (see [17, Sequence A002110]).

Proof of Theorem 2. Let $k = \lfloor n/m \rfloor$ and let $p_1, \dots, p_k \in \mathbb{N}$ be the first k prime numbers. We define

$$q_i := \frac{p_k\#}{p_i}.$$

By construction, $\gcd(q_1, \dots, q_k) = 1$. Thus, there exists a $\boldsymbol{\lambda} \in \mathbb{Z}^k$ such that $\sum_{j=1}^k \lambda_j q_j = 1$. Since, $\gcd(q_1, \dots, q_{j-1}, q_{j+1}, \dots, q_k) = p_j$ for any $j \in \{1, \dots, k\}$, it must hold that $\lambda_j \neq 0$ for all $j \in \{1, \dots, k\}$. We set $\bar{q}_j := -q_j$ if $\lambda_j < 0$ and $\bar{q}_j := q_j$ if $\lambda_j > 0$.

Now, let $A \in \mathbb{Z}^{m \times n}$ be a matrix with

$$A_{ij} = \begin{cases} \bar{q}_{j+k-ik} & \text{if } k(i-1) < j \leq ik, \\ 0 & \text{otherwise.} \end{cases}$$

Further, let $\mathbf{1}$ denote the all-one m -dimensional vector. The vector $\mathbf{z}^* \in \mathbb{Z}^n$ with entries $z_i^* = |\lambda_{i-k\lfloor(i-1)/k}\rangle|$ for $i \in \{1, \dots, km\}$ and $z_i^* = 0$ for $i \in \{km+1, \dots, n\}$ is strictly positive in the first km entries and satisfies $A\mathbf{z}^* = \mathbf{1}$. So, Problem (1) with $\mathbf{b} = \mathbf{1}$ is feasible. However, no integer vector $\mathbf{z} \in \mathbb{Z}^n$ exists that satisfies $A\mathbf{z} = \mathbf{1}$ and $|\text{supp}(\mathbf{z})| < km$.

It remains to note that by (4) $\|A\|_\infty = q_1 = \frac{p_k\#}{2} = \frac{1}{2}e^{(1+o(1))k \ln(k)}$. Thus, $\log(\|A\|_\infty) = \frac{\log(e)}{2}(1+o(1))k \ln(k)$. Provided we have chosen N_ε sufficiently large, we have $\frac{\log(e)}{2}(1+o(1))k \ln(k) \leq k^{1+\varepsilon}$, and therefore $|\text{supp}(\mathbf{z})| = mk \geq m \log(\|A\|_\infty)^{1/(1+\varepsilon)}$. \square

Acknowledgements: This work was partially supported by NSF grant DMS-1440140, while the second author was in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Fall 2017. The second author was also partially supported by NSF grant DMS-1522158.

The third author is supported by the Swiss National Science Foundation (SNSF) within the project *Convexity, geometry of numbers, and the complexity of integer programming (Nr. 163071)*. This work was done in part while the third author was visiting the Simons Institute for the Theory of Computing, partially supported by the DIMACS/Simons Collaboration on Bridging Continuous and Discrete Optimization through NSF grant #CCF-1740425.

The work of the fifth author was supported by an Alexander von Humboldt research award.

References

- [1] I. Aliev, J. De Loera, T. Oertel, and C. O’Neill. Sparse solutions of linear diophantine equations. *SIAM Journal on Applied Algebra and Geometry*, 1(1):239–253, 2017.
- [2] E. Bombieri and J. Vaaler. On Siegel’s lemma. *Invent. Math.*, 73(1):11–32, 1983.
- [3] W. Cook, J. Fonlupt, and A. Schrijver. An integer analogue of Carathéodory’s theorem. *J. Combin. Theory Ser. B*, 40(1):63–70, 1986.
- [4] W. Cook, M. Hartmann, R. Kannan, and C. McDiarmid. On integer points in polyhedra. *Combinatorica*, 12(1):27–37, 1992.
- [5] F. Eisenbrand and G. Shmonin. Carathéodory bounds for integer cones. *Oper. Res. Lett.*, 34(5):564–568, 2006.
- [6] F. Eisenbrand and R. Weismantel. Proximity results and faster algorithms for integer programming using the Steinitz lemma. Available as ArXiv:1707.00481v2, 2017.
- [7] Michael R. Garey and David S. Johnson. *Computers and intractability*. W. H. Freeman and Co., San Francisco, Calif., 1979. A guide to the theory of NP-completeness, A Series of Books in the Mathematical Sciences.

- [8] M. X. Goemans and T. Rothvoß. Polynomiality for bin packing with a constant number of item types. In *Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*, pages 830–839. SIAM, 2014.
- [9] G.H. Hardy, E.M. Wright, R. Heath-Brown, and J. Silverman. *An Introduction to the Theory of Numbers*. Oxford mathematics. OUP Oxford, 2008.
- [10] K. Jansen. An eptas for scheduling jobs on uniform processors: using an milp relaxation with a constant number of integral variables. *SIAM Journal on Discrete Mathematics*, 24(2):457–485, 2010.
- [11] K. Jansen, K.-M. Klein, and J. Verschae. Closing the gap for makespan scheduling via sparsification techniques. *arXiv preprint arXiv:1604.07153*, 2016.
- [12] E. Kieronski, J. Michaliszyn, I. Pratt-Hartmann, and L. Tendera. Two-variable first-order logic with equivalence closure. *SIAM Journal on Computing*, 43(3):1012–1063, 2014.
- [13] D. Knop, M. Koutecký, and M. Mnich. Combinatorial n-fold integer programming and applications. *arXiv preprint arXiv:1705.08657*, 2017.
- [14] V. Kuncak and M. Rinard. Towards efficient satisfiability checking for boolean algebra with presburger arithmetic. In *CADE*, volume 21, pages 215–230. Springer, 2007.
- [15] H.W. Lenstra. Integer programming with a fixed number of variables. *Mathematics of Operations Research*, 8(4):538–548, 1983.
- [16] S. Onn. Huge tables and multicommodity flows are fixed-parameter tractable via unimodular integer carathéodory. *Journal of Computer and System Sciences*, 83(1):207–214, 2017.
- [17] N.J.A. Sloane. The on-line encyclopedia of integer sequences. <http://oeis.org>, 2017.