

Vectors in a Box*

KEVIN BUCHIN[§]

Department of Mathematics and Computer Science
Technical University of Eindhoven, P.O. Box 513
5600 MB Eindhoven, Netherlands
e-mail: k.a.buchin@tue.nl

JIRÍ MATOUŠEK

Department of Applied Mathematics and
Institute of Theoretical Computer Science (ITI)
Charles University, Malostranské nám. 25
118 00 Praha 1, Czech Republic, and
Institute of Theoretical Computer Science
ETH Zurich, 8092 Zurich, Switzerland
e-mail: matousek@kam.mff.cuni.cz

ROBIN A. MOSER[¶]

Institute of Theoretical Computer Science
ETH Zurich, 8092 Zurich, Switzerland
e-mail: robin.moser@inf.ethz.ch

DÖMÖTÖR PÁLVÖLGYI

Ecole Polytechnique Fédérale de Lausanne
Switzerland
e-mail: dom@cs.elte.hu

Rev. 24/X/09

Abstract

For an integer $d \geq 1$, let $\tau(d)$ be the smallest integer with the following property: If $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_t$ is a sequence of $t \geq 2$ vectors in $[-1, 1]^d$ with $\mathbf{v}_1 + \mathbf{v}_2 + \dots + \mathbf{v}_t \in [-1, 1]^d$, then there is a set $S \subseteq \{1, 2, \dots, t\}$ of indices, $2 \leq |S| \leq \tau(d)$, such that $\sum_{i \in S} \mathbf{v}_i \in [-1, 1]^d$. The quantity $\tau(d)$ was introduced by Dash, Fukasawa, and Günlük, who showed that $\tau(2) = 2$, $\tau(3) = 4$, and $\tau(d) = \Omega(2^d)$, and asked whether $\tau(d)$ is finite for all d .

Using the Steinitz lemma, in a quantitative version due to Grinberg and Sevastyanov, we prove an upper bound of $\tau(d) \leq d^{d+o(d)}$, and based on a construction of Alon and Vũ, whose main idea goes back to Håstad, we obtain a lower bound of $\tau(d) \geq d^{d/2-o(d)}$.

These results contribute to understanding the *master equality polyhedron with multiple rows* defined by Dash et al., which is a “universal” polyhedron encoding valid cutting planes for integer programs (this line of research was started by Gomory in the late 1960s). In particular, the upper bound on $\tau(d)$ implies a pseudo-polynomial running time for an algorithm of Dash et al. for integer programming with a fixed number of constraints. The algorithm consists in solving a linear program, and it provides an alternative to a 1981 dynamic programming algorithm of Papadimitriou.

1 Introduction

Let $d \geq 1$ and let us consider the unit cube $[-1, 1]^d$; we will call it *the box* in this paper. We want to construct a large number t of vectors $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_t$, each of them lying in the box, such that

*This research was partially done at the *Gremo Workshop on Open Problems* 2009, and the support of the ETH Zürich is gratefully acknowledged.

[§]Supported by the Netherlands Organisation for Scientific Research (NWO) under project no. 639.022.707

[¶]This research was partially done during an internship with Microsoft Research, Redmond, Washington, USA.

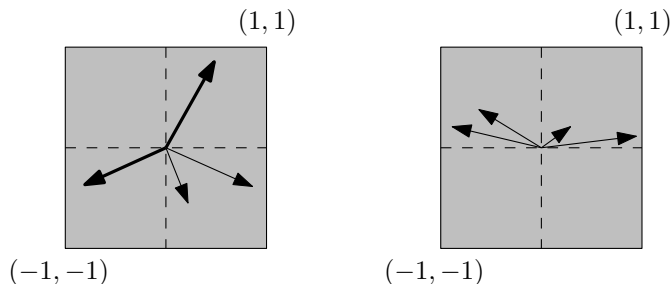


Figure 1: Illustration to the proof of $\tau(2) = 2$: Either we find two vectors in opposite quadrants, or one of the coordinates has the same sign for all the vectors and can be ignored.

- (i) the sum $\mathbf{s} = \mathbf{v}_1 + \mathbf{v}_2 + \dots + \mathbf{v}_t$ also lies in the box, but
- (ii) for every *proper* subset $S \subset [t]$ of indices¹ with $2 \leq |S| < t$, the sum $\sum_{i \in S} \mathbf{v}_i$ lies outside the box (we have to exclude $|S| = 1$, since every \mathbf{v}_i itself does lie in the box).

So we are interested in long *minimal* sequences² with sum in the box. Let $\tau(d)$ denote the largest t such that a minimal sequence as above exists (it is easy to see that the definition in the abstract, although phrased differently, is actually equivalent).

In order to illustrate this definition, let us check that $\tau(2) = 2$. We have $\tau(d) \geq 2$ for all d by definition. For proving $\tau(d) \leq 2$, we need to show that in every sequence $\mathbf{v}_1, \dots, \mathbf{v}_t \in [-1, 1]^2$ with sum in the box there are two vectors with sum in the box.

If two of the vectors lie in opposite quadrants, as in Fig. 1 left, then their sum is in the box and we are done. Otherwise, some two neighboring quadrants have to be empty, which means that one of the two coordinates has the same sign for all the \mathbf{v}_i ; w.l.o.g. we may assume that all the \mathbf{v}_i have a positive y -coordinate. Then the y -coordinate can be ignored (since it lies in $[-1, 1]$ for the sum of any subsequence), and it suffices to show that the sum of some two of the x -coordinates lies in $[-1, 1]$. In other words, it now suffices to check that $\tau(1) = 2$, which we leave to the reader.

An example showing $\tau(3) \geq 4$ is the sequence $(1, 1, \frac{2}{3}), (1, -\frac{2}{3}, -1), (-\frac{2}{3}, 1, -1), (-\frac{2}{3}, -\frac{2}{3}, \frac{2}{3})$.

The quantity $\tau(d)$ was introduced by Dash, Fukasawa, and Günlük [5] in the context of integer programming (we will discuss the motivation later). They found the values $\tau(2) = 2$ and $\tau(3) = 4$, and they asked whether $\tau(d)$ is finite for all d . We provide a positive answer, with the following upper bound:

Theorem 1.1 *For all $d \geq 1$ we have $\tau(d) < 4(2d)^d$.*

Our proof, presented in Section 2 below, is based on the so-called Steinitz lemma, in a quantitative version due to Grinberg and Sevastyanov [7].

We also show that the upper bound is not far from the truth.

¹We use the notation $[t] = \{1, 2, \dots, t\}$.

²Strictly speaking, the order of the vectors is irrelevant for the considered property, and so one should perhaps rather speak of sets or multisets of vectors. However, we find sequences easier to work with for notational reasons.

Theorem 1.2 *There is a constant $c > 0$ such that*

$$\tau(d) \geq (cd)^{d/2}$$

for all d that are powers of 2.

The proof, given in Section 2 is based on a construction of very ill-conditioned square matrices with ± 1 entries, due to Alon and Vũ [2] (the basic idea going back to Håstad [8]). It seems likely that the lower bound could be extended to all d , instead of just powers of 2, but this might need a careful analysis of another construction from [2].

There is a natural and, in our opinion, interesting variant of the quantity $\tau(d)$, where one again considers sequences $\mathbf{v}_1, \dots, \mathbf{v}_t \in [-1, 1]^d$ satisfying (i) and (ii) above, but the \mathbf{v}_i are restricted to only ± 1 vectors. Let $\tau_{\pm 1}(d)$ denote the corresponding maximum length of such a sequence; we have $\tau_{\pm 1}(d) \leq \tau(d)$ by definition. We obtain the following slightly weaker lower bound:

Theorem 1.3 *There is a constant $c > 0$ such that $\tau_{\pm 1}(d) \geq (cd)^{d/4}$ for all d that are powers of 2.*

The IP connection. The quantity $\tau(d)$ has been motivated by a connection to an algorithm for integer programming.

Let us consider an integer program in the form

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

where A is an $m \times \ell$ integer matrix, $\mathbf{c} \in \mathbb{Z}^\ell$, and $\mathbf{b} \in \mathbb{Z}^m$. This optimization problem is well-known to be NP-hard even for $m = 1$, i.e., for a single equality constraint (this follows, e.g., from the hardness of the knapsack problem). On the other hand, Papadimitriou [9] proved that if m is fixed and the entries of A and \mathbf{b} are small integers, bounded in absolute value by a parameter N , then the integer program can be solved in *pseudo-polynomial* time. That is, the running time can be bounded by a polynomial in ℓ and N (and the input size of \mathbf{c}); the polynomial depends on m .

Papadimitriou’s algorithm is based on dynamic programming (also see Schrijver [10] for a description); it searches for a shortest path in an auxiliary graph. Dash et al. [5] provided a completely different algorithm for the same problem, which consists in solving a linear program over an auxiliary polyhedron (the so-called *polaroid*).³ They obtained a pseudo-polynomial bound for the number of inequalities in the linear program, and thus also for the running time, but only for input integer programs with $m \leq 3$ constraints (actually, they handled the case of $m = 1$ constraint earlier in [4]). To get pseudo-polynomiality for larger m , they needed the finiteness of $\tau(m)$. Thus, combined with our Theorem 1.1, their algorithm provides an alternative to Papadimitriou’s method.

We won’t review the algorithm here; we only recall some of the key concepts, and then we indicate how $\tau(m)$ is related to the linear program.

The approach of Dash et al. goes back to a paper of Gomory [6]. In that remarkable work, which introduced several important ideas of modern polyhedral combinatorics, Gomory

³More precisely, two linear programs are needed. Moreover, the basic algorithm discussed in [5] solves the *separation problem* for the set $Q := \text{conv}\{\mathbf{x} \in \mathbb{Z}^\ell, A\mathbf{x} = \mathbf{b}, \mathbf{x} \geq \mathbf{0}\}$, but a dual version of it can also be used for the optimization variant. But here we don’t want to go into details.

defined a certain “universal” polyhedron, the *master cyclic group polyhedron*, whose faces encode all instances of integer programs in a certain class (see, e.g., [1] for an introduction). Dash et al. [5] use the somewhat related concept of the *master equality polyhedron* $K^m(N, \mathbf{b})$, which we recall below. For $m = 1$, it was introduced in an earlier paper by Dash et al. [4], who attribute its origin to a 2005 talk of Uocha, and it contains as a face Gomory’s master cyclic group polyhedron, as well as the *master knapsack polyhedron* of Araóz.

Let

$$I := \{-N, -N + 1, \dots, N\}^m,$$

and let $\mathbf{b} \in I$ be a vector corresponding to the right-hand side in (1). Then the master equality polyhedron resides in \mathbb{R}^I and it is defined as

$$K^m(N, \mathbf{b}) := \text{conv}\{\mathbf{x} \in \mathbb{Z}^I : \sum_{\mathbf{v} \in I} x_{\mathbf{v}} \mathbf{v} = \mathbf{b}, \mathbf{x} \geq \mathbf{0}\}.$$

It turns out that the separation problem for the integer program (1) can be reduced to the separation problem for $K^m(N, \mathbf{b})$.

For $m = 1$, Dash et al. [4] obtained a description of a *nontrivial polar* T of $K^1(N, b)$, i.e. a polyhedron whose vertices correspond to the nontrivial facets of $K^1(N, b)$, and thus reduced the separation problem for $K^1(N, b)$ to optimizing a linear function over T . It is important that T is described by polynomially many linear constraints.

In [5] Dash et al. describe an example showing that for $m \geq 2$, a sufficiently compact description of a nontrivial polar of $K^m(N, \mathbf{b})$ may be very hard to find, if it exists at all. However, they defined the new notion of a *polaroid* of $K^m(N, \mathbf{b})$, and proved that the separation problem for $K^m(N, \mathbf{b})$ can be reduced to a suitable linear program over the polaroid. Again, one needs a polynomial bound on the number of constraints in this linear program, and here $\tau(m)$ enters the game.

The variables of the linear program are $\pi_{\mathbf{v}}$ for all integer vectors $\mathbf{v} \in I$, and the main kind of constraints in it are *subadditivity constraints* of the form

$$\pi_{\mathbf{v}_1} + \dots + \pi_{\mathbf{v}_t} \geq \pi_{\mathbf{v}_1 + \dots + \mathbf{v}_t}, \quad (2)$$

where $\mathbf{v}_1, \dots, \mathbf{v}_t \in I$ are vectors whose sum also lies in I . Now suppose, for example, that $\mathbf{v}_1 + \mathbf{v}_2 + \dots + \mathbf{v}_k$ also lies in I , for some k with $2 \leq k < t$. Then (2) is a consequence of the subadditivity constraints

$$\pi_{\mathbf{v}_1} + \dots + \pi_{\mathbf{v}_k} \geq \pi_{\mathbf{v}_1 + \dots + \mathbf{v}_k} \quad \text{and} \quad \pi_{\mathbf{v}_1 + \dots + \mathbf{v}_k} + \pi_{\mathbf{v}_{k+1}} + \dots + \pi_{\mathbf{v}_t} \geq \pi_{\mathbf{v}_1 + \dots + \mathbf{v}_t}.$$

Similarly, whenever there is an $S \subset [t]$ with $2 \leq |S| < t$ and $\sum_{i \in S} \mathbf{v}_i \in I$, the constraint (2) is implied by subadditivity constraints with a smaller number of terms. Thus, it is sufficient to consider only subadditivity constraints with $t \leq \tau(m)$.

The quantity $\tau(m)$ gives only an upper bound on the number of non-redundant subadditivity constraints. Dash et al. [5] define another quantity $k^*(m) \leq \tau(m)$, which is related to the number of non-redundant constraints more directly. In Corollary 3.3 we will give a lower bound of $(cm)^{m/4}$ for $k^*(m)$, which shows that it is not much smaller than $\tau(m)$.

2 The Upper Bound

Let $B \subset \mathbb{R}^d$ be a d -dimensional closed convex body symmetric about $\mathbf{0}$ (in other words, the unit ball of a norm on \mathbb{R}^d). Riemann and Lévy in the 19th century raised the question of

whether there exists a number $m = m(B)$, depending only on B , such that the vectors of an arbitrary finite set (or multiset) $V \subset B$ with $\sum_{\mathbf{v} \in V} \mathbf{v} = \mathbf{0}$ can be ordered into a sequence $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ so that each of the partial sums $\mathbf{v}_1 + \mathbf{v}_2 + \dots + \mathbf{v}_k$, $1 \leq k \leq n$, belongs to the expanded body $mB = \{m\mathbf{x} : \mathbf{x} \in B\}$. The first complete proof of a positive answer was given by Steinitz [11]. The strongest known quantitative version, with $m(B) = d$ for all bodies in \mathbb{R}^d , is due to Grinberg and Sevastyanov [7] (their beautiful proof can also be found in Bárány’s survey [3, Theorem 2.1]).

Theorem 2.1 (Steinitz lemma) *Let B be a symmetric convex body in \mathbb{R}^d , and let $V \subset B$ be a finite set (or multiset) of vectors satisfying $\sum_{\mathbf{v} \in V} \mathbf{v} = \mathbf{0}$. Then there is an ordering $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ of the elements of V such that for all $k = 1, 2, \dots, n$, we have $\sum_{i=1}^k \mathbf{v}_i \in dB$.*

Proof of Theorem 1.1. Given a collection of t vectors in the box whose sum also lies in the box, and assuming $t \geq t_0 := 4(2d)^d$, we want to find a proper subcollection with sum in the box.

Here it will be more convenient to regard the given collection of t vectors as a multiset W (rather than as a sequence)—later we will obtain suitable ordering of the vectors in W from the Steinitz lemma.

Thus, W is a multiset of t vectors; we let $\mathbf{s} := \sum_{\mathbf{v} \in W} \mathbf{v} \in [-1, 1]^d$ be their sum. We apply the Steinitz lemma as above with $B = [-1, 1]^d$ and $V := W \cup \{-\mathbf{s}\}$ (this is again a multiset, with $t + 1$ vectors). This yields an ordering

$$\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_i, -\mathbf{s}, \mathbf{v}_{i+1}, \dots, \mathbf{v}_t$$

such that the sum of the first k terms lies in dB for every $k = 1, 2, \dots, t + 1$.

First, let us assume that the “artificial” element $-\mathbf{s}$ falls in the second half of the above sequence; that is, $i \geq t/2 \geq t_0/2$. Let us subdivide the blown-up cube dB , whose side length is $2d$, into $(2d)^d$ cubes of side 1, of the form $[0, 1]^d + \mathbf{z}$, $\mathbf{z} \in \{-d, -d + 1, \dots, d - 1\}^d$.

Let $\mathbf{s}_k := \mathbf{v}_1 + \dots + \mathbf{v}_k$ be the k th partial sum, $k = 0, 1, \dots, t_0/2$, and let us consider every second of these, i.e., the points $\mathbf{s}_0, \mathbf{s}_2, \mathbf{s}_4, \dots, \mathbf{s}_{t_0/2}$. These are more than $t_0/4 = (2d)^d$ points in dB , and so some two of them, \mathbf{s}_{2i} and \mathbf{s}_{2j} , $0 \leq i < j \leq t_0/4$, fall in the same cube $[0, 1]^d + \mathbf{z}$.

Then the difference $\mathbf{s}_{2j} - \mathbf{s}_{2i}$ lies in the box. At the same time, it equals

$$\mathbf{v}_{2i+1} + \mathbf{v}_{2i+2} + \dots + \mathbf{v}_{2j},$$

and so we have found the desired proper submultiset of W with sum in the box (and with at least two elements).

It remains to deal with the case when the artificial element $-\mathbf{s}$ lies in the first half of the sequence—then we use the same kind of argument as above for the second half. Theorem 1.1 is proved. \square

3 Lower bounds

All of our lower bounds are based on results of Alon and Vü [2]. The main theme of that paper are ill-conditioned matrices with ± 1 entries (or $0/1$ entries; these two settings are not very different).

Let us consider a nonsingular $d \times d$ matrix A whose entries are $+1$'s and -1 's, and let $\chi(A)$ be the maximum of the absolute values of the entries of A^{-1} ; the larger $\chi(A)$, the more ill-conditioned the matrix A is. Let $\chi(d) := \max_A \chi(A)$, where the maximum is over all $d \times d$ nonsingular ± 1 matrices.

Alon and Vñ showed that $\chi(d) = d^{d/2+o(d)}$ and gave several interesting applications. The main achievement was the (surprisingly large) lower bound, which was obtained by an explicit construction. For that purpose, Alon and Vñ modified and extended a construction of Håstad [8], which was formulated in a different setting, namely, in the language of threshold gates.

In this section we will provide three lower bound constructions for vectors in the box. The first construction is the simplest: It follows rather directly from a result explicitly stated in [2], but it loses a factor of two in the dimension, leading only to the lower bound of $\tau(d) \geq d^{d/4-o(d)}$. Then we give another, different and more complicated construction, which gives $\tau(d) \geq d^{d/2-o(d)}$ and proves Theorem 1.2, and finally, we modify the latter construction so that only ± 1 vectors are used, obtaining Theorem 1.3.

Large quantities. In order to avoid boring formulas or repetitive phrases, we introduce the following piece of terminology. If $Q = Q(d)$ is some quantity in the forthcoming constructions, depending on d , we say that Q is *large* if there is a constant $c > 0$ such that $|Q| \geq (cd)^{d/2}$ holds for all of the considered values of d (in the first construction we will consider all d , while in the second and third only powers of two). In particular, we note that a large quantity can be either positive or negative.

We note that being large is immune to division by exponential factors; e.g., if some Q is large, then $Q/2^d$ is large as well.

3.1 The First Construction

Here we use the following result of Alon and Vñ:

Proposition 3.1 ([2, Proposition 3.4.3]) *For every $d \geq 1$, there exists a $d \times (d+1)$ matrix C of rank d with entries $+1$ and -1 such that any nonzero integral solution \mathbf{z} of the system $C\mathbf{x} = \mathbf{0}$ has at least one large component.*

The construction. The following construction will show that $\tau(2d)$ is large (for all d), or in other words, that $\tau(d) \geq (cd)^{d/4}$.

Let C be the $d \times (d+1)$ matrix as in Proposition 3.1. Since the system $C\mathbf{x} = \mathbf{0}$ is homogeneous, with rational coefficients, and has fewer equations than unknowns, there exist nonzero integral solutions.

Let $\mathbf{z} \in \mathbb{Z}^{d+1}$ be a nonzero integral solution of $C\mathbf{x} = \mathbf{0}$ with the smallest possible L_1 norm, i.e., minimizing $\|\mathbf{z}\|_1 = \sum_{j=1}^{d+1} |z_j|$. Let us set $t := \|\mathbf{z}\|_1$; by the above, $t = t(d)$ is large.

After possibly flipping the signs of some of the columns of C , we may assume that all components of \mathbf{z} are nonnegative. Let \mathbf{c}_j denote the j th column of C , and let $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_t$ be an (auxiliary) sequence of vectors containing z_j copies of each \mathbf{c}_j , $j = 1, 2, \dots, d+1$.

The \mathbf{w}_i are vectors in the box (even ± 1 vectors), and we have $\sum_{i=1}^t \mathbf{w}_i = \sum_{j=1}^{d+1} z_j \mathbf{c}_j = C\mathbf{z} = \mathbf{0}$.

It is also easy to see that no proper subsequence of the \mathbf{w}_i has sum in the *interior* of the box. Indeed, the sum of any subsequence is an integral vector, so if it lies in $(-1, 1)^d$, it has to be $\mathbf{0}$. But choosing a proper subsequence of the \mathbf{w}_i corresponds to choosing multiplicities z'_1, \dots, z'_{d+1} , with $z'_j \leq z_j$ for all j and with at least one of the inequalities strict. So a

proper subsequence with zero sum corresponds to a nontrivial solution \mathbf{z}' of $C\mathbf{z}' = \mathbf{0}$ with $\|\mathbf{z}'\|_1 < t = \|\mathbf{z}\|_1$, contradicting the assumed minimality of $\|\mathbf{z}\|_1$.

Thus, the \mathbf{w}_i almost achieve what we want, but only almost, since there may be some sums of proper subsequences on the boundary of the box. We get around this by a simple dimension-doubling trick.

Let us set $\varepsilon := 1/(10t)$, say. Let \mathbf{w}'_i be the vector obtained from \mathbf{w}_i by replacing all -1 components by $-(1 - \varepsilon)$ and keeping all $+1$ components. Similarly, \mathbf{w}''_i is obtained by keeping the -1 components of \mathbf{w}_i and replacing $+1$'s by $1 - \varepsilon$. Thus, for example, if we had $\mathbf{w}_i = (+1, +1, -1)$, then $\mathbf{w}'_i = (+1, +1, -(1 - \varepsilon))$ and $\mathbf{w}''_i = (1 - \varepsilon, 1 - \varepsilon, -1)$. Finally, let $\mathbf{v}_i \in \mathbb{R}^{2d}$ be obtained by concatenating \mathbf{w}'_i and \mathbf{w}''_i .

We claim that this sequence $\mathbf{v}_1, \dots, \mathbf{v}_t$ witnesses $\tau(2d) \geq t$. Clearly, the \mathbf{v}_i lie in the box. Moreover, since all the \mathbf{w}_i sum to $\mathbf{0}$ and $\|\mathbf{w}_i - \mathbf{w}'_i\|_\infty \leq \varepsilon$, $\|\mathbf{w}_i - \mathbf{w}''_i\|_\infty \leq \varepsilon$, we have $\sum_{i=1}^t \mathbf{v}_i \in [-t\varepsilon, t\varepsilon]^{2d} \subset [-1, 1]^{2d}$.

Next, let us consider a proper subset $S \subset [t]$, $2 \leq |S| < t$. We already know that $\sum_{i \in S} \mathbf{w}_i \neq \mathbf{0}$; let us fix a coordinate k in which this sum has a nonzero component. Let a be the number of $+1$'s in the k th coordinate of the sum, and let b be the number of -1 's there; that is, $a := |\{i : (\mathbf{w}_i)_k = 1\}|$, $b := |S| - a = |\{i : (\mathbf{w}_i)_k = -1\}|$. We have $a \neq b$.

Then $(\sum_{i \in S} \mathbf{v}_i)_k = (\sum_{i \in S} \mathbf{w}'_i)_k = (a - b) + b\varepsilon$ and $(\sum_{i \in S} \mathbf{v}_i)_{d+k} = (\sum_{i \in S} \mathbf{w}''_i)_k = (a - b) - a\varepsilon$; we claim that at least one of these numbers falls outside $[-1, 1]$. Indeed, this is clear if $|a - b| \geq 2$. If $a - b = 1$, then $b \geq 1$ (since $a + b = |S| \geq 2$), and so $(a - b) + b\varepsilon \geq 1 + \varepsilon > 1$. Similarly, for $a - b = -1$ we find that $a - b - a\varepsilon \leq -1 - \varepsilon < -1$. Thus, $\sum_{i \in S} \mathbf{v}_i$ is not in the box and Theorem 1.2 is proved. \square

A lower bound for the quantity $k^*(m)$. As was mentioned in the last part of the introduction, Dash et al. [5] define an integer function $k^*(m)$, which is bounded above by $\tau(m)$,⁴ but which is more directly related to the number of constraints in their linear program. Here we won't recall the definition of $k^*(m)$, since we won't use it directly. Rather, we will rely on a property of $k^*(m)$, which is expressed in Lemma 6.1 of [5], and which in our notation can be re-phrased as follows.

Lemma 3.2 (Dash et al. [5]) *Let $m \geq 1$, and suppose that there are rational vectors $\mathbf{v}_1, \dots, \mathbf{v}_t \in [-1, 1]^m$, with $\mathbf{s} := \sum_{i=1}^t \mathbf{v}_i \in [-1, 1]^d$, such that $\sum_{i \in S} \mathbf{v}_i$ lies outside the box for every $S \subset [t]$, $2 \leq |S| < t$, and moreover, for every choice of nonnegative integer coefficients q_1, \dots, q_t with $1 \leq q := \sum_{i=1}^t q_i \leq t/2$, the vector $\mathbf{s} - \mathbf{s}'$, where $\mathbf{s}' := \sum_{i=1}^t q_i \mathbf{v}_i$, also lies outside the box. Then $k^*(m) \geq t$.*

It turns out that the vectors $\mathbf{v}_1, \dots, \mathbf{v}_t$ constructed in the previous proof also have the additional property in the above lemma, and so we get $k^*(m) \geq (cm)^{m/4}$ for all even m :

Corollary 3.3 *We have $k^*(m) \geq (cm)^{m/4}$ for all even m , where c is a positive constant.*

Sketch of proof. Let us set $m = 2d$ and use the vectors $\mathbf{v}_1, \dots, \mathbf{v}_t \in [-1, 1]^{2d}$ from the previous proof. The only property which we haven't yet verified for them is the "moreover" part in Lemma 3.2, and we do this now. We need to assume $t \geq 4$ (which we can since the bound is asymptotic and so very small values of m can be ignored).

⁴They don't prove this explicitly, but it can be seen from the proofs of their Theorems 4.4 and 4.7.

It is easily checked that the first d coordinates of \mathbf{s} equal $\frac{1}{2}t\varepsilon$ and the remaining d coordinates are $-\frac{1}{2}t\varepsilon$.

Arguing as in the previous proof, we get that $\sum_{i=1}^t q_i \mathbf{w}_i \neq \mathbf{0}$ (the fact that one \mathbf{w}_i may appear several times in the sum makes no difference), and so there is some coordinate k where the number a of $+1$ contributions differs from the number b of -1 contributions, $a + b = q$. (More formally, $a = \sum_{i: (\mathbf{w}_i)_k = +1} q_i$, $b = \sum_{i: (\mathbf{w}_i)_k = -1} q_i$.) Let us suppose, for example, that $a < b$; then we calculate that the k th coordinate of $\mathbf{s} - \mathbf{s}'$ equals $\frac{1}{2}t\varepsilon - (a - b) - b\varepsilon$, which is surely above $+1$ for $a - b \leq -2$. For $a - b = -1$ it equals $1 + (t/2 - b)\varepsilon$, and we have $b = \frac{q+1}{2} \leq \frac{t/2+1}{2} < t/2$. For $a > b$ we argue similarly using the $(k + d)$ th coordinate. \square

3.2 The Second Construction

The stronger construction used in the proof of Theorem 1.2 is based on the following result of Alon and Vü [2].

Proposition 3.4 *For every d that is a power of 2, there exists a $d \times d$ nonsingular matrix A with entries ± 1 such that the matrix $B := 2^d A^{-1}$ is integral, has nonnegative row sums, and all the entries in the first row of B are nonnegative and large.*

This statement is not explicitly formulated in [2]; rather, it can be combined from several remarks scattered throughout that paper, so we recall a (very easy) proof from more a explicit statement in [2].

Proof. Let d be a power of 2. In the proof of Theorem 2.1.1 in [2], Alon and Vü construct an $d \times d$ nonsingular matrix \tilde{A} with entries ± 1 such that there exists a column of \tilde{A}^{-1} in which all entries are large.

They also show that $\det(\tilde{A}) = 2^{d-1}$. By transposing \tilde{A} and reordering its columns, we can guarantee that the first row of the inverse matrix consists of large entries. Since changing the sign of a column changes the sign of the corresponding row of the inverse matrix, by flipping the signs of suitable rows we can make all entries in the first row of the inverse nonnegative. Finally, by flipping the signs of some columns we can arrange for nonnegativity of the row sums of the inverse. In this way we obtain the desired A .

Since all the operations performed above preserve the determinant, we still have $\det(A) = 2^{d-1}$, and since the adjoint $\text{adj}(A)$ is integral, $B = 2^d A^{-1}$ is integral as well. \square

For a vector $\mathbf{x} \in \mathbb{R}^n$, the notation $\mathbf{x} > \mathbf{0}$ means that all entries of \mathbf{x} are nonnegative and $\mathbf{x} \neq \mathbf{0}$.

Corollary 3.5 *Let A be as in the previous proposition and let $\mathbf{b} > \mathbf{0}$ be an integral vector. Then the (unique) solution \mathbf{z} of $A\mathbf{x} = \mathbf{b}$ has the first component z_1 positive and large.*

Proof. Since $\mathbf{z} = A^{-1}\mathbf{b}$, z_1 is a linear combination of the entries of the first row of A^{-1} with nonnegative integer coefficients (given by \mathbf{b}), at least one of them nonzero. Since the entries in the first row of A^{-1} are all large and positive, the corollary follows. \square

Proof of Theorem 1.2. Using the matrix A provided by Proposition 3.4, we construct a sequence $\mathbf{v}_1, \dots, \mathbf{v}_t$ of vectors in $[-1, 1]^{d+1}$ with $t = t(d)$ large and with sum in the box. This

time we won't show that the sequence is minimal; rather, we will prove that every subsequence with at least 2 terms and with sum in the box has to have a large number of terms.

Let r_j be the sum of all entries in the j th row of $B = 2^d A^{-1}$, which, as Proposition 3.4 asserts, is a nonnegative integer. We can also write $\mathbf{r} = (r_1, \dots, r_d) = B\mathbf{1}$, where $\mathbf{1}$ is the all 1's vector. Let $R := \sum_{j=1}^d r_j$, and let $\alpha := \frac{2^d}{R}$. We note that since R is large, may assume $\alpha \in (0, 1)$.

Let \mathbf{a}_j denote the j th column of A , and let $\bar{\mathbf{a}}_j = (\mathbf{a}_j, 1) \in \mathbb{R}^{d+1}$ be obtained from \mathbf{a}_j by appending the component 1 to the end.

Our sequence $\mathbf{v}_1, \dots, \mathbf{v}_t$ consists of r_i copies of $\bar{\mathbf{a}}_j$, $j = 1, 2, \dots, d$, and of R copies of the vector $\mathbf{c} := (-\alpha\mathbf{1}, -1) \in \mathbb{R}^{d+1}$, making a total number of $t = 2R$ vectors.

The vector \mathbf{c} and its multiplicity were chosen so that the sum of all vectors in the sequence is $\mathbf{0}$, as we now check. For the $(d+1)$ st coordinate this is equivalent to $\sum_{j=1}^d r_j = R$. The vector consisting of the first d entries of $\sum_{i=1}^t \mathbf{v}_i$ equals

$$\left(\sum_{j=1}^d r_j \mathbf{a}_j \right) - R\alpha\mathbf{1} = A\mathbf{r} - 2^d\mathbf{1} = A(B\mathbf{1}) - 2^d\mathbf{1} = 2^d A A^{-1} \mathbf{1} - 2^d\mathbf{1} = \mathbf{0}.$$

It remains to show that if for some $S \subseteq [t]$, $|S| \geq 2$, the sum $\sum_{i \in S} \mathbf{v}_i$ lies in the box, then $|S|$ is large.

Choosing a subsequence corresponds to choosing multiplicities of the vectors $\bar{\mathbf{a}}_1, \dots, \bar{\mathbf{a}}_d$ and \mathbf{c} ; we denote these multiplicities by z_1, \dots, z_d and k , respectively. The number of terms is $\sum_{j=1}^d z_j + k \geq 2$.

Let us suppose that the sum $\mathbf{s}' := \sum_{i \in S} \mathbf{v}_i$ lies in $[-1, 1]^{d+1}$. First we check the z_j can't be all 0. If we had $\mathbf{z} = \mathbf{0}$, then we would get $k \geq 2$, and $s'_{d+1} \leq -2$ —a contradiction. So $\mathbf{z} > \mathbf{0}$.

Similarly we find, using the last coordinate again, that $k > 0$. Indeed, if we had $k = 0$, then $s'_{d+1} = \sum_{j=1}^d z_j \geq 2$. Thus, $k > 0$ as claimed.

The vector of the first d coordinates of \mathbf{s}' equals $A\mathbf{z} - k\alpha\mathbf{1}$. We consider the vector $\mathbf{b} := A\mathbf{z}$. Clearly, it is integral and nonzero (since the only solution of $A\mathbf{x} = \mathbf{0}$ is $\mathbf{0}$, while $\mathbf{z} \neq \mathbf{0}$). We claim that $\mathbf{b} \geq \mathbf{0}$. Indeed, if $b_j < 0$, then $b_j \leq -1$ by integrality, and so we would get $s'_j = b_j - k\alpha \leq -1 - \alpha < -1$ (using $k \geq 1$)—a contradiction.

We have shown that $A\mathbf{z} = \mathbf{b}$ with $\mathbf{b} > \mathbf{0}$ integral, and we can apply Corollary 3.5 to conclude that z_1 is large. This also means that $|S|$ is large. \square

3.3 The Third Construction: ± 1 Vectors

Here we will prove Theorem 1.3, the lower bound for $\tau_{\pm 1}(d)$. To this end, we will exhibit a sequence $\mathbf{v}_1, \dots, \mathbf{v}_t$, t large, of ± 1 vectors in \mathbb{R}^{2d+1} , with sum $\mathbf{0}$ and such that every subsequence of length at least 2 with sum in the box has a large number of terms.

As in the previous subsection, we use the matrix A provided by Proposition 3.4, we set $r_j := (2^d A^{-1} \mathbf{1})_j$, $R := \sum_{j=1}^d r_j$, and $t = 2R$. By Corollary 3.5, t is large. Moreover, we note that R is divisible by two because, as we demonstrated in the previous section, $\sum_{j=1}^d r_j \mathbf{a}_j = 2^d \mathbf{1}$, and since all the \mathbf{a}_j are vectors with ± 1 entries, we need an even number of them to reach a point with even coordinates. Therefore, t is divisible by 4.

Now let $\mathbf{u}_1, \dots, \mathbf{u}_t \in \{+1, -1\}^d$ be a sequence of vectors that consists of r_i copies of the i th column of A . We build the vectors $\mathbf{v}_1, \dots, \mathbf{v}_t \in \{+1, -1\}^{2d+1}$ as follows. For $i = 1, 2, \dots, t/2$

and $i \in [2d + 1]$, we let

$$(\mathbf{v}_i)_j := \begin{cases} (\mathbf{u}_j)_i & \text{if } 1 \leq j \leq d \\ +1 & \text{if } d + 1 \leq j \leq 2d \text{ and } 1 \leq i \leq t/4 - 2^{d-1} \\ -1 & \text{if } d + 1 \leq j \leq 2d \text{ and } t/4 - 2^{d-1} < i \leq t/2 \\ +1 & \text{if } j = 2d + 1. \end{cases}$$

Then for $i = t/2 + 1, \dots, t$ and $j \in [2d + 1]$, we let

$$(\mathbf{v}_i)_j := \begin{cases} (\mathbf{v}_{i-t/2})_{j+d} & \text{if } 1 \leq j \leq d \\ (\mathbf{v}_{i-t/2})_{j-d} & \text{if } d + 1 \leq j \leq 2d \\ -1 & \text{if } j = 2d + 1. \end{cases}$$

We first claim that the sequence sums to $\mathbf{0}$. Just as in the last section, $\sum_{i=1}^{t/2} \mathbf{u}_i = 2^d \mathbf{1}$. Therefore, by the definition of the \mathbf{v}_i ,

$$\sum_{i=1}^{t/2} \mathbf{v}_i = \underbrace{(2^d, 2^d, \dots, 2^d)}_{d \text{ times}}, \underbrace{(-2^d, -2^d, \dots, -2^d)}_{d \text{ times}}, t/2,$$

and

$$\sum_{i=t/2+1}^t \mathbf{v}_i = \underbrace{(-2^d, -2^d, \dots, -2^d)}_{d \text{ times}}, \underbrace{(2^d, 2^d, \dots, 2^d)}_{d \text{ times}}, -t/2.$$

In conclusion, the total sum is zero.

Now let us consider an index set $S \subseteq [t]$, $|S| \geq 2$, and let us suppose that $\mathbf{s} := \sum_{i \in S} \mathbf{v}_i \in \{-1, 0, 1\}^d$, and that $|S|$ is not large. By analyzing several cases, we will show that this leads to a contradiction.

Let $S_1 := S \cap [t/2]$ and $S_2 := S \setminus S_1$. Let $\mathbf{s}_1 := \sum_{i \in S_1} \mathbf{v}_i$ and $\mathbf{s}_2 := \sum_{i \in S_2} \mathbf{v}_i = \mathbf{s} - \mathbf{s}_1$. Moreover, let $\mathbf{s}_1^{(1)} \in \{-1, 1\}^d$ and $\mathbf{s}_1^{(2)} \in \{-1, 1\}^d$ be the projections of \mathbf{s}_1 onto the coordinates 1 through d and the coordinates $d + 1$ through $2d$, respectively, and similarly for $\mathbf{s}_2^{(1)}, \mathbf{s}_2^{(1)}$.

First let us suppose that $(\mathbf{s}_1)_{2d+1} = 0$. Then $|S_1| = 0$, and since $|S| \geq 2$, we have $|S_2| \geq 2$. But then $(\mathbf{s})_{2d+1} = (+1)|S_1| + (-1)|S_2| < -1$ —a contradiction. Therefore, $(\mathbf{s}_1)_{2d+1} > 0$. Symmetrically, $(\mathbf{s}_2)_{2d+1} < 0$.

Next, let us suppose that $\mathbf{s}_1^{(1)} = \mathbf{0}$. Since $|S_1| > 0$ and $\mathbf{s}_1^{(1)}$ is a linear combination of the columns of A , we would get that $A\mathbf{x} = \mathbf{0}$ has a nonzero integral solution, which is not the case, and so we can conclude $\mathbf{s}_1^{(1)} \neq \mathbf{0}$. Symmetrically, $\mathbf{s}_2^{(2)} \neq \mathbf{0}$.

Now we suppose that $\mathbf{s}_1^{(2)} \neq \mathbf{0}$. By the way that vector is composed, we then have $\mathbf{s}_1^{(2)} = k\mathbf{1}$ for some nonzero integer k . First let us assume $k < 1$. Then, since \mathbf{s} lies in the box, $\mathbf{s}_2^{(2)} \geq \mathbf{0}$, and since we have shown $\mathbf{s}_2^{(2)} \neq \mathbf{0}$, we even have $\mathbf{s}_2^{(2)} > \mathbf{0}$. According to Corollary 3.5, that implies that $\mathbf{s}_2^{(2)}$ is a sum of a large number copies of the columns of A , and in this case $|S|$ is large, contrary to the assumption.

So we may suppose $k > 1$. For analogous reasons, this implies that $\mathbf{s}_2^{(2)} < \mathbf{0}$. But then, again by Corollary 3.5, it is impossible to express $\mathbf{s}_2^{(2)} < \mathbf{0}$ as a nonnegative integer linear combination of the columns of A (since the corollary implies that for $\mathbf{b} < \mathbf{0}$, an integral solution of $A\mathbf{x} = \mathbf{b}$ has a negative component)—a contradiction.

Having dealt with the case $\mathbf{s}_1^{(2)} \neq \mathbf{0}$, we now assume $\mathbf{s}_1^{(2)} = \mathbf{0}$; symmetrically, we may assume $\mathbf{s}_2^{(1)} = \mathbf{0}$ as well.

Now the total sum \mathbf{s} has $\mathbf{s}_1^{(1)} \neq \mathbf{0}$ in the first d coordinates and $\mathbf{s}_2^{(2)} \neq \mathbf{0}$ in the coordinates $d + 1$ through $2d$. For parity reasons we get $\mathbf{s}_1^{(1)}, \mathbf{s}_2^{(2)} \in \{-1, 1\}^d$. This implies that $|S_1| \equiv |S_2| \equiv 1 \pmod{2}$. On the other hand, we have shown $\mathbf{s}_1^{(2)} = \mathbf{s}_2^{(1)} = \mathbf{0}$, and this gives $|S_1| \equiv |S_2| \equiv 0 \pmod{2}$ —a contradiction. Theorem 1.3 is proved. \square

4 Conclusion

It would be interesting to determine the asymptotics of $\tau(d)$ more precisely. We conjecture that the truth should be close to the lower bound, i.e., of order roughly $d^{d/2}$.

One way of improving on the upper bound might be to get a factor better than d in the Steinitz lemma (Theorem 2.1) for the case $B = [-1, 1]^d$. It is known, and not hard to see, that if B is the unit ball of the ℓ_1 norm, then the factor cannot be smaller than $\frac{d}{2}$. However, it is possible that the factor of $O(\sqrt{d})$ suffices for $B = [-1, 1]^d$ (from which the bound $d^{d/2+o(d)}$ for $\tau(d)$ would follow).

However, apparently there is no improvement over d for any B known, and the problem may be hard. As Bárány [3] puts it, for the case where B is the Euclidean ball, “even the much weaker $o(d)$ estimate seems to be out of reach though quite a few mathematicians have tried,” and for $B = [-1, 1]^d$ “there is no proof in sight even for the weaker $o(d)$ estimate.”

Acknowledgment

We would like to thank Tibor Szabó for raising the problem at the GWOP’09 workshop, Sanjeeb Dash for prompt answers to our questions, and Patrick Traxler for useful discussions.

References

- [1] K. Aardal, R. Weismantel, and L. A. Wolsey. Non-standard approaches to integer programming. *Discrete Appl. Math.*, 123(1-3):5–74, 2002.
- [2] N. Alon and V. H. Vū. Anti-Hadamard matrices, coin weighing, threshold gates, and indecomposable hypergraphs. *J. Comb. Theory Ser. A*, 79(1):133–160, 1997.
- [3] I. Bárány. On the power of linear dependencies. In Gy. O. H. Katona and M. Grötschel, editors, *Building bridges*, pages 31–46. Springer, Berlin, 2008.
- [4] S. Dash, R. Fukasawa, and O. Günlük. On a generalization of the master cyclic group polyhedron. *Mathematical Programming*. To appear.
- [5] S. Dash, R. Fukasawa, and O. Günlük. The master equality polyhedron with multiple rows. Technical Report RC24746, IBM Research, 2009.
- [6] R. E. Gomory. Some polyhedra related to combinatorial problems. *Linear Algebra and Its Applications*, 2:451–558, 1969.
- [7] V. S. Grinberg and S. V. Sevastyanov. The value of the Steinitz constant (in Russian). *Funk. Anal. Prilozh.*, 14:56–57, 1980.

- [8] J. Håstad. On the size of weights for threshold gates. *SIAM J. Discr. Math.*, 7:484–492, 1994.
- [9] C. H. Papadimitriou. On the complexity of integer programming. *J. ACM*, 28(4):765–768, 1981.
- [10] A. Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, Inc., New York, NY, USA, 1986.
- [11] E. Steinitz. Bedingt konvergente Reihen und konvexe Systeme. *J. Reine Ang. Mathematik*, 143:128–175, 1913. Ibid., 144(1914), 1–40. Ibid., 146(1916), 1–52.