RC25609 (WAT1605-070) May 31, 2016
Mathematics

IBM Research Report

Sublinear Bounds for a Quantitative Doignon-Bell-Scarf Theorem

Stephen R. Chestnut[1], Robert Hildebrand[2], Rico Zenklusen[1]

[1]ETH Zürich

[2]IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598 USA

Sublinear Bounds for a Quantitative Doignon-Bell-Scarf Theorem

Stephen R. Chestnut* Robert Hildebrand† Rico Zenklusen‡

January 29, 2016

Abstract

The recent paper "A quantitative Doignon-Bell-Scarf Theorem" by Aliev et al. generalizes the famous Doignon-Bell-Scarf Theorem on the existence of integer solutions to systems of linear inequalities. Their generalization examines the number of facets of a polyhedron that contains exactly k integer points in $\mathbb{R}^n$. They show that there exists a number $c(n,k)$ such that any polyhedron in $\mathbb{R}^n$ that contains exactly k integer points has a relaxation to at most $c(n,k)$ of its inequalities that will define a new polyhedron with the same integer points. They prove that $c(n,k) = O(k2^n)$. In this paper, we improve the bound asymptotically to be sublinear in k. We also provide lower bounds on $c(n,k)$, along with other structural results. For dimension $n = 2$, our bounds are asymptotically tight to within a constant.

1 Introduction

The classical theorem of Helly states that for any finite collection of convex subsets of $X = \mathbb{R}^n$, if the intersection of every $n+1$ subsets is nonempty, then the intersection of the entire collection is nonempty. In 1973, Doignon was curious as to how such a theorem could hold over the discrete set of integers $X = \mathbb{Z}^n$. What resulted is a famous theorem that can be phrased as follows: any system of linear inequalities in $\mathbb{R}^n$ without integer solutions has a subsystem of at most 2^n inequalities that also has no integer solutions [16]. This result was also independently reproved shortly thereafter by both Bell and Scarf [11, 24]. In its Helly formulation, the Doignon-Bell-Scarf Theorem states that for any finite collection of convex subsets of $\mathbb{R}^n$, if the intersection of every 2^n subsets contains at least one integer point, then the intersection of the entire collection contains at least one integer point.

Since Doignon's result, many versions of Helly's theorem have been studied based on the underlying set of feasible points. For instance, the Helly number with $X = \mathbb{Z}^n \times \mathbb{R}^d$

*Institute for Operations Research, Department of Mathematics, ETH Zürich, stephenc@ethz.ch
†Mathematical Sciences Department, IBM T. J. Watson Research Center, rhildeb@us.ibm.com
‡Institute for Operations Research, Department of Mathematics, ETH Zürich, ricoz@math.ethz.ch

was shown to be $(d+1)2^n$ [5]. See [3] for a recent survey of variations and applications of Helly's theorem. We focus on a quantitative generalization of Doignon's result guided by the following definition.

Definition 1.1. Given n, k two non-negative integers, $c(n,k)$ is the least integer such that for any m, matrix $A \in \mathbb{R}^{m\times n}$, and $b \in \mathbb{R}^m$, if the polyhedron $\{x \in \mathbb{R}^n : Ax \leq b\}$ has exactly k integer solutions, then there exits a subset S of the rows of A with $|S| \leq c(n,k)$ such that $\{x \in \mathbb{R}^n : A_S x \leq b_S\}$ has exactly the same k integer solutions.

It turns out $c(n,k)$ is always finite, so, phrased as a Helly-type theorem, this implies that if a finite collection of convex subsets of $\mathbb{R}^n$ has the property that the intersection of any $c(n,k)$ subsets contains at least $k+1$ integer points, then the intersection of all of them contains at least $k+1$ integer points [1]. Following this notation, the Doignon-Bell-Scarf Theorem asserts that, for all $n \geq 1$, $c(n,0) = 2^n$. The quantity $c(n,k)$ was formally defined by Aliev, De Loera, and Louveaux [2], although a much older result of Bell [11] implies that $c(n,k) \leq (k+2)^n$. Aliev et al. [2] improve the upper bound to $c(n,k) \leq 2^k 2^n$ and have since, together with Bassett [1], improved the bound to

$$c(n,k) \leq \lceil 2(k+1)/3 \rceil 2^n - 2\lceil 2(k+1)/3 \rceil + 2. \tag{1}$$

Our Theorem 3.6 sharpens the upper bound to $o(k) \cdot 2^n$ and simplifies the reasoning behind the bound. To illustrate it, let us quickly describe how one can achieve an upper bound of $k2^n$, which is of the same order as (1). It begins with a trick that was known already by Bell [11], and which is formalized in Lemma 2.2. Recall that a set of points is in convex position if it contains no point that can be expressed as a convex combination of the others. If $P = \{x \in \mathbb{R}^n : Ax \leq b\}$ contains exactly k integer points and is defined by $c(n,k)$ constraints, none of which can be removed without affecting the integer hull, then there exists a collection $S \subseteq \mathbb{Z}^n$ of $c(n,k)$ points in convex position such that[1] $\mathrm{ic}(S) \setminus S \subseteq P$.

To prove the upper bound, take P and S as above, and consider the parities of the points in S. Let $A \subseteq S$ be the set of points with a given parity, that is, with exactly the same coordinates even and odd. The midpoint of any pair of points in A is an integer point in P, so the number integer points in P is bounded like $k \geq |A+A| - |A| \geq |A|$, where $A+A$ is the Minkowski sum and the second inequality holds because the points are in convex position. There are 2^n parity classes and every parity class has at most k points, so $c(n,k) = |S| \leq k2^n$.

For dimension $n = 2$, Erdös, Fishburn, and Füredi [17] have proved that $|A+A| - |A| \geq \frac{1}{4}|A|^2$, when $A \subseteq \mathbb{R}^2$ is in convex position. Applying the reasoning above to this case yields $c(2,k) \leq 8\sqrt{k}$. It is, however, suboptimal. Bell [11] mentions that, due to Andrews [4], any polygon with at least c facets, the removal of any one of which affects the integer hull, has $\Omega(c^3)$ interior lattice points. This argument, implies that there exists a constant C such that

$$c(2,k) \leq Ck^{\frac{1}{3}}. \tag{2}$$

[1] We use the notation $\mathrm{ic}(S) \coloneqq \mathrm{conv}(S) \cap \mathbb{Z}^n$ where $\mathrm{conv}(S)$ is the convex hull of S.

Our Theorem 3.7 sharpens this bound by providing an explicit constant.

The Doignon-Bell-Scarf Theorem has had many applications in the theory of integer programming and the geometry of numbers. Aliev et al. use $c(n, k)$ to extend a randomized algorithm of Clarkson [13] to then find the k best solutions to an integer linear program [1]. A recent focus in the integer programming community relates to cutting planes known as intersection cuts that are derived from maximal lattice-free polyhedra. See, for instance, [14]. It follows from the Doignon-Bell-Scarf Theorem that any maximal lattice free polyhedron has at most 2^n facets. This result has been central in classifying the different types of maximal lattice free convex sets. In a similar way, $c(n, k)$ bounds the facet complexity of a maximal polyhedron containing k integer points.

Baes, Oertel, and Weismantel used the Doignon-Bell-Scarf theorem as a basis for describing a dual for mixed-integer convex minimization [6]. Likewise, $c(n, k)$ could be used to describe a dual for the problem of finding the k best solutions to an integer convex minimization problem.

Finally, the techniques used for studying $c(n, k)$ in [1] and in this paper involve analyzing lattice-polytopes, and hence, bear a close connection to the theory of toric varieties [20].

Our Contributions

This paper improves the asymptotic upper bound on $c(n, k)$ to sublinear in k using the midpoints methodology outlined above and stronger bounds on the cardinality of sumsets from the field of additive combinatorics.

We complement the sublinear (in k) upper bound on $c(n, k)$ with a $\Omega(k^{\frac{n-1}{n+1}})$ lower bound, where the hidden constant depends on the dimension n. The lower bound is proved by relating $c(n, k)$ to the maximum vertex complexity of a lattice polytope containing k lattice points and then applying a theorem of Bárány and Larman [9] that the integer hull of the n-dimensional hyperball with radius r is $\Theta(r^{n(n-1)/(n+1)})$, where the neglected constants depend on n.

Increasing the lower bounds on $|A + A|$ might be one way to decrease our upper bound. In dimension greater than two, surprisingly little is known about the minimum possible cardinality of $|A + A|$ for A in convex position. In Proposition 3.4, we show that the integer points inside a sphere give an upper bound for the minimum number of $|A + A|$. However, we are aware of no lower bounds on sumset cardinalities that specifically make use of convexity of the points, and, therefore, we make virtually no use of convexity when proving the sublinear upper bound.

As the paper progresses towards proving the bounds, we establish some structural properties of $c(n, k)$ and related sequences that may be of independent interest. One of the difficulties, in particular, that we encounter while proving the lower bound is that $c(n, k)$ is not monotonic in k, which we demonstrate by proving that $c(2, 5) = 7 < 8 = c(2, 4)$.

The formula given by Aliev et al. [1] implies $c(n, 2) \leq 2(2^n - 1)$ and they left as an open problem whether equality holds. Gonzalez Merino and Henze [3] have proved it to be true, and we also prove it (Proposition 4.5) as well as give an alternative proof that $c(n, 2) \le 2(2^n - 1)$ (Theorem 3.9). Corollary 3.10 and Proposition 4.5, with the discussion immediately following it, show that this is the correct asymptotic behavior in n for every (fixed) k, specifically, for all k, $c(n, k)$ is asymptotic to 2^{n+1}.

Section 2 describes Bell's technique in more detail. The midpoints technique is applied in Section 3 to prove the sublinear upper bound and in Section 4 we prove the lower bound. Finally, Section 5 proves that $c(n, k)$ is not a monotonic function of k.

2 Bell's Expanding Polyhedron

The main lemma of this section, Lemma 2.2, is an important tool for understanding the behavior of $c(n, k)$. It relates a general system of linear inequalities with a collection of integer points in convex position. Each integer point serves as a witness to one inequality in a system where every inequality is necessary to maintain the integer hull, as described in Lemma 2.1 which we prove first. The basic idea of the proof is described by [11], and it uses several ideas from [1]. Let $\text{int}(X)$ denote the interior of a set X.

Lemma 2.1. *Let $S \subseteq \mathbb{Z}^n$. For any polytope $P = \{x \in \mathbb{R}^n : Ax \le b\}$ with $P \cap \mathbb{Z}^n = S$ there exists a polytope $P' = \{x \in \mathbb{R}^n : A'x \le b'\}$ with $\text{int}(P') \cap \mathbb{Z}^n = S$ that has most as many facets as the number of inequalities in the description of P and exactly one integral point in the interior of each facet.*

Proof. Let $a_i \in \mathbb{R}^n$, for $i = 1, \ldots, m$ denote the rows of A. We would like to enlarge P until each facet of contains a unique integer point. To make these points unique, we will perturb the facets slightly. For this process, we first establish a bounded region to work on. That is, let $Q = \{x : a_i \cdot x \le a_i \cdot x_i + 1\} \supset P$. Notice that Q is bounded since P and Q share the same recession cone. Since Q is bounded, $Q \cap \mathbb{Z}^n$ is finite and there exists an integer $u > 0$ such that $\|x\|_\infty \le u$ for all $x \in Q$.

Next, we establish a region P_ϵ such that $P \subset P_\epsilon \subset Q$. Let $P_\epsilon = \{x : a_i \cdot x \le b_i + \epsilon, i = 1, \ldots, m\}$ where we chose $\epsilon > 0$ such that $P_\epsilon \cap \mathbb{Z}^n = P \cap \mathbb{Z}^n$ and such that, for all integers x and y, $|a_i \cdot (x - y)| > \epsilon$ whenever $a_i \cdot (x - y) \ne 0$ and $\|x\|_\infty, \|y\|_\infty$ are less than u.

We will use the perturbation vector $\bar{a} = \frac{\epsilon}{2nu^{2n}} \sum_{i=1}^n u^i e_i$, where e_i denotes the standard unit vector. By this choice, notice that for all $z \in Q \cap \mathbb{Z}^n$, $\bar{a} \cdot z$ is distinct and that $|\bar{a} \cdot z| \le \frac{\epsilon}{2}$.

Therefore, by choosing $a'_i = a_i + \bar{a}$, we see that $\bar{a}_i \cdot z$ is distinct for all $z \in Q \cap \mathbb{Z}^n$. Therefore the set $\{x : a'_i \cdot x = a'_i \cdot z\} \cap Q \cap \mathbb{Z}^n = \{z\}$ for any $z \in Q \cap \mathbb{Z}^n$. Furthermore, by the size of $\bar{a}$ chosen, it follows that $P'_0 = \{x : a'_i \cdot x \le b_i + \frac{\epsilon}{2}, i = 1, \ldots, m\}$ satisfies $P \cap \mathbb{Z}^n = \text{int}(P'_0) \cap \mathbb{Z}^n$, and that x_i is valid for all inequalities of P'_0 except for $a'_i \cdot x \le b_i + \frac{\epsilon}{2}$.

In order, for $i = 1, \ldots, m$, set $b'_i = \min_{x \in P'_i \cap \mathbb{Z}^n} a'_i \cdot x$ where $\bar{P}_i$ is the polyhedron given by the inequalities

$$\begin{cases} a'_j \cdot x \le b'_j & j = 1, \dots, i-1, \\ a'_j \cdot x \ge b_j + \epsilon & j = i, \\ a'_j \cdot x \le b_j + \frac{\epsilon}{2} & j = i+1, \dots, m. \end{cases}$$

Note that we let $b'_i = +\infty$ if the minimization problem is infeasible.

Finally, setting $P' = \{x : a'_i \cdot x \le b'_i,\ i = 1, \dots, m\}$ satisfies the hypotheses since every facet contains a unique integer point, and therefore it must be in the relative interior. Inequalities $a'_i \cdot x \le b'_i$ with $b'_i = +\infty$ are irrelevant, and hence P' has at most m facets. Furthermore, no new integer points were introduced to the interior of P'. ■

If $Ax \le b$ is a system of inequalities such that removing any one inequality strictly increases the number of integer solutions we say that $Ax \le b$ is *stable*.

Lemma 2.2. *If $P = \{x \in \mathbb{R}^n : Ax \le b\}$ is stable with s inequalities, then there exists a set $S \subseteq \mathbb{Z}^n$ in convex position, $|S| = s$, such that* $\mathrm{ic}(S) \setminus S \subseteq P \cap \mathbb{Z}^n$.

Proof. Let $P' = \{x \in \mathbb{R}^n : A'x \le b'\}$ be the polyhedron obtained from P by Lemma 2.1, and let S be the integer points on the facets of P'. By construction, $\mathrm{ic}(S) \setminus S \subseteq P \cap \mathbb{Z}^n$. Since P is stable, no inequality can be removed during the expansion step in the proof of Lemma 2.1, i.e., $b'_i < +\infty$ for all $i = 1, \dots, m$. Therefore, $A'x \le b'$ has s inequalities and this is the same as the number of points in S. ■

3 Asymptotic Upper Bounds

We obtain asymptotically sublinear (in k) upper bounds on $c(n,k)$ by focusing on a question based on the discrete geometry of lattice points. The bounds are derived from upper bounds on $\ell(n,k)$.

Definition 3.1. Given n, k two non-negative integers, $\ell(n,k)$ is the smallest integer such that for any set $S \subseteq \mathbb{Z}^n$ in convex position with $|S| = \ell(n,k)$, we have that $|\mathrm{ic}(S) \setminus S| \ge k$.

Although not stated explicitly, [1] proves the following lemma. They go on to show that $\ell(n,k) \le \lceil 2k/3 \rceil 2^n - 2\lceil 2k/3 \rceil + 2$ by inductively using the fact that $\ell(n,1) = 2^n + 1$. We provide a proof here for completeness.

Lemma 3.2. $c(n,k) < \ell(n,k+1)$.

Proof. Suppose, for the sake of contradiction, that $c(n,k) \ge \ell(n,k+1)$. Let $P = \{x : Ax \le b\}$ be a stable system of $c(n,k)$ inequalities with k integer solutions, and let $S \subseteq \mathbb{Z}^n$ in convex position with $|S| = c(n,k)$ be given by Lemma 2.2. Since $\mathrm{ic}(S) \setminus S \subseteq P \cap \mathbb{Z}^n$, we must have $|\mathrm{ic}(S) \setminus S| \le k$. But this contradicts the assumption $c(n,k) \ge \ell(n,k+1)$. ■

Clearly, the points $\{0,1\}^n$ demonstrate that $\ell(n,1) > 2^n$. The proof of $\ell(n,1) \leq 2^n+1$ follows by the parity and pigeonhole principle argument outlined in the introduction. Consider the parities of the 2^n+1 points in S. Since there are only 2^n total parities, there must be two points with the same parity in S. Since these two points share the same parity, the midpoint of these two points is also an integer point, and thus S contains at least one integer point in its convex hull that is not in S.

For any set $S \subseteq \mathbb{R}^n$, let $M(S)$ denote the *set of midpoints* of points in S, that is, $M(S) = \frac{1}{2}(S+S) \setminus S = \{\frac{1}{2}(x_1+x_2) : x_1, x_2 \in S\} \setminus S$. Given n, s two non-negative integers, $\mu(n,s)$ is the minimum integer such that for any set of points $S \subseteq \mathbb{R}^n$, $|S| = s$, with no three points of S collinear, $|M(S)| \geq \mu(n,s)$. In a similar way, $\mu_{\mathrm{c}}(n,s)$ is the minimum integer such that for any set of points $S \subseteq \mathbb{R}^n$, $|S| = s$, in convex position, $|M(S)| \geq \mu_{\mathrm{c}}(n,s)$. Obviously, $\mu(n,s) \leq \mu_{\mathrm{c}}(n,s)$; ℓ and μ_{c} are related in the following way, which follows as well by a parity and pigeonhole principle argument.

Lemma 3.3. *Let $n \geq 1$, $k \geq 0$, and let $s_{n,k} \coloneqq \min\{s : \mu_{\mathrm{c}}(n,s) \geq k\}$. Then $\ell(n,k) \leq (s_{n,k}-1)2^n + 1$.*

It appears that the quantity $\mu_{\mathrm{c}}(n,k)$ has not been studied for $n \geq 3$. The strong quadratic growth that is observed in dimension $n = 2$ does not hold in higher dimensions.

Proposition 3.4. *For every fixed n, $\mu_{\mathrm{c}}(n,s) = O(s^{(n+1)/(n-1)})$. Therefore, $s_{n,k} = \Omega(k^{(n-1)/(n+1)})$.*

Proof. Let n be fixed. By [19], there exists $u \in \mathbb{R}^n$ such that for all $N \in \mathbb{Z}_+$, there exists a radius R_N such that $|B_n(u, R_N) \cap \mathbb{Z}^n| = N$. For every R, let V_R denote the set of vertices of the integer hull of $B_n(u,R)$. Partition the set of vertices V_R into parity sets $V_{R,x} \coloneqq \{v \in V : v \equiv x \pmod 2\}$ for $x \in \{0,1\}^n$. Let $s_R = \max\{|V_{R,x}| : x \in \{0,1\}^n\}$ and $S_R = V_{R,x_R}$ be a parity set that corresponds to s_R, i.e., $s_R = |V_R|$.

By choice of u, $s_{R_{N+1}} \leq s_{R_N}+1$. Hence, for every $s \in \mathbb{Z}_+$, there exists a radius R such that $s = s_R$. Since $S_R \subseteq \mathbb{Z}^n$ has the same parity, all midpoints of this set are integral, that is, $M(S_R) \subseteq B_n(u,R) \cap \mathbb{Z}^n$. Note that $s_R \geq \frac{1}{2^n}|V_R|$. By [7] and [9], $s_R = \Omega(R^{\frac{n(n-1)}{n+1}})$ while $|B_n(u,R) \cap \mathbb{Z}^n| = O(R^n)$. It follows that $\mu_{\mathrm{c}}(n,s) = O(s^{\frac{n+1}{n-1}})$. ■

In this section we are interested lower bounds on $\mu_{\mathrm{c}}(n,s)$. It is trivial to show $\mu_{\mathrm{c}}(n,s) \geq s$. Pach [21] and Stanchescu [25] have both proved superlinear lower bounds for $\mu(2,s)$, and we could take advantage of these by projecting a convex set in n dimensions to a set in the plane that has no three term arithmetic progression. However, we achieve a slightly better bound from the following theorem of Sanders.

Theorem 3.5 (Sanders [23]). *There exists a constant C such for any abelian group G and finite subset $A \subseteq G$ containing no three-term arithmetic progressions*

$$|A+A| \geq C|A| \left(\frac{\log^{\frac{1}{3}} |A|}{\log\log |A|} \right).$$

Sanders's Theorem implies

$$\mu(n,s) \geq Cs\frac{\log^{\frac{1}{3}} s}{\log\log s}. \tag{3}$$

We are in position to prove the sublinear upper bound on $c(n,k)$.

Theorem 3.6. *For all $n, k \geq 1$,*

$$c(n,k) \leq \ell(n,k+1) \leq O\left(k\frac{\log\log k}{\log^{\frac{1}{3}} k}\right) \cdot 2^n.$$

Proof. Let s be the solution, in terms of k, to $k = C's'\frac{\log^{\frac{1}{3}} s'}{\log\log s'}$, where C' is the constant from (3). Then

$$\mu_c(n,\lceil s\rceil) \geq \mu(n,\lceil s\rceil) \geq C'\lceil s\rceil\frac{\log\log\lceil s\rceil}{\log^{\frac{1}{3}}\lceil s\rceil} \geq k.$$

It follows from the parities argument that $c(n,k) \leq 2^n\lceil s\rceil$. One easily checks that s is asymptotic, in k, to $\frac{k\log\log k}{C'\log^{\frac{1}{3}} k}$. Applying Lemma 3.3 completes the proof. ■

As pointed out by Bell [11], in dimension $n = 2$, we can do much better. Here is a proof based on a recent bound for the minimum area of a lattice n-gon that gives an explicit upper bound.

Theorem 3.7.

$$c(2,k) \leq \ell(2,k+1) \leq \lfloor 4.43(k+4)^{\frac{1}{3}}\rfloor.$$

Proof. Let $\ell = 4.43(k+4)^{\frac{1}{3}}$. We want to show that for any set $S \subseteq \mathbb{Z}^2$ in convex position, if $|S| \geq \ell$, then $|\operatorname{ic}(S) \setminus S| \geq k+1$. We instead show the contrapositive: if $|\operatorname{ic}(S) \setminus S| < k+1$ then $|S| < \ell$.

Let $P = \operatorname{conv}(S)$. Let $v = |S|$ be the number of vertices of P, let b be the number of lattice points on the boundary of P that are not vertices, and let i be the number of interior lattice points. Therefore $i + b < k+1$. By Pick's Theorem, the area A of P is given by $A = i + \frac{v+b}{2} - 1$. By [22], $A \geq \frac{v^3}{8\pi^2}$. Hence $\frac{v^3}{8\pi^2} \leq i + \frac{v+b}{2} - 1$. After rearranging, we have $\frac{v^3}{8\pi^2} - \frac{v}{2} \leq i + \frac{b}{2} - 1 < k$. One choice of a lower bound for $v \geq 0$ is $\frac{v^3}{4.43^3} - 4 \leq \frac{v^3}{8\pi^2} - \frac{v}{2} < k$. The result follows now by isolating v and then applying the floor operator since v is an integer. ■

From the calculation above, we could also say that for every $\epsilon > 0$ there exists a constant C_ϵ such that $\ell(n,k+1) \leq (8\pi^2+\epsilon)^{\frac{1}{3}}(k+C_\epsilon)^{\frac{1}{3}}$. It was shown that for A_v, the minimum area of a convex lattice polygon with v vertices, the limit $\lim_{v\to\infty}\frac{A_v}{v^3}$ exists and is very nearly $1/54$ [10]. Using this asymptotic result, the relation to $k^{\frac{1}{3}}$ can be value $(8\pi^2+\epsilon)$ could be improved further.

3.1 Tighter bounds for specified arrangements

The dependence on k of the upper bound is tight for $n = 2$, but it is likely not tight for $n \geq 3$. The goal of this section is to achieve a smaller upper bound for specified arrangements of points. For a set $S \subseteq \mathbb{Z}^n$, let $c(S)$ denote the maximum number of number of inequalities in any stable system $P = \{x \in \mathbb{R}^n : Ax \leq b\}$ such that $P \cap \mathbb{Z}^n = S$ or $c(S) = -\infty$ if there is no such system. One can show that $c(S)$ is no larger than the Helly number of $X = \mathbb{Z}^n \setminus S$ [5], but it is unclear if these numbers coincide. The quantities $c(S)$ and $c(n, k)$ are related as follows.

Proposition 3.8.

$$c(n,k) = \max_{\substack{S \subseteq \mathbb{Z}^n \\ |S|=k}} c(S),$$

in particular $c(S)$ is finite.

The two main theorems of this section are Theorem 3.9 and Theorem 3.11. The values for both bounds can be substantially lower than $c(n, k)$. The first theorem says that if S, $|S| = k$, lies in a d-dimensional subspace, then $c(S) \leq c(d, |S|) + 2(2^n - 1)$. This bound upper bound is sharp, and equal to $2(2^n - 1)$, for any set of collinear points, which gives an alternative proof that $c(n, 2) \leq 2(2^n - 1)$ as every two points are collinear. The bound for the case of collinear points is used in our proof that $c(2, 5) \leq 7$.

The second theorem proves the bound $c(S) \leq p(2^n - 1)$, where p is the size of the smallest system of inequalities whose integer solutions are exactly the points in S. We learn that the largest system with solutions S and no unnecessary inequalities is not more than 2^n times larger than the smallest system with solutions S. Therefore, given any system whose integer solutions are S we can derive an upper bound on $c(S)$.

Theorem 3.9. *If $1 \leq d \leq n$ and $S \subseteq \mathbb{Z}^n$, $\mathrm{ic}(S) = S$, is contained d-dimensional affine subspace of $\mathbb{R}^n$, then $c(S) \leq c(d, k) + 2(2^n - 2)$.*

Proof. The Doignon-Bell-Scarf Theorem covers the case $k = 0$ and (1) covers $k = 1$. Henceforth, let $k \geq 2$. Without loss of generality we may assume that $0 \in S$.

Suppose that $P = \{x \in \mathbb{R}^n : Ax \leq b\}$ is a polytope defined by a stable system of $c(S)$ inequalities and has $P \cap \mathbb{Z}^n = S$. Let P' be the polytope from Lemma 2.1 with $c(S)$ facets and let T be the set of $c(S)$ integer points, one on the interior of each facet of P'. Let $L \subseteq \mathbb{R}^n$ be a d-dimensional subspace containing S. There exists a hyperplane H such that $L \subseteq H$ and $H \cap (\mathbb{Z}^n \setminus L) = \emptyset$, since a random hyperplane containing L has this property. Let H_0 and H_1 denote the closed halfspaces with $H_0 \cap H_1 = H$. Notice that no two points in $T \cap \mathrm{int}(H_0)$ can have the same parity nor can a point here have the same parity as a point in S because their midpoint cannot lie in L. The same holds for $T \cap \mathrm{int}(H_1)$. Since $\mathrm{ic}(S) = S$ and $k \geq 2$, the points in S have at least two distinct parities. Therefore $|T \cap \mathrm{int}(H_0)|, |T \cap \mathrm{int}(H_1)| \leq 2^n - 2$.

It remains to bound $|T \cap H|$. Let $B \in \mathbb{Z}^{n \times d}$ be a basis for the lattice $L \cap \mathbb{Z}^n$, and let $B^{-1} \in \mathbb{R}^{d \times n}$ denote the inverse of B when it is viewed as a linear map from $\mathbb{R}^d$ to

L. Now consider $Q = B^{-1}(P' \cap L)$. Q is a polytope in $\mathbb{R}^d$ that has $|S| = k$ integer points in its interior and $|T \cap L|$ integer points on its boundary. Each of the points on the boundary of Q is in the interior of a facet. It follows, by the definition of $c(d,k)$ that we can remove all but $c(d,k)$ facets from Q without changing the set of interior integer points. Obviously, such a relaxation must retain facets containing points in T. Thus $c(d,k) \geq |T \cap L|$, and we have

$$c(S) = |T| = |T \cap L| + |T \cap \mathrm{int}(H_0)| + |T \cap \mathrm{int}(H_1)| \leq c(d,k) + 2(2^n - 2).$$

■

As any k points in $\mathbb{R}^n$ are contained in a $k-1$ dimensional affine subsapce, an immediate consequence of Theorem 3.9 is the following corollary. In particular, for each fixed k, $c(n,k)$ is asymptotic to 2^{n+1}.

Corollary 3.10. *If $k \leq n$, then $c(n,k) \leq c(k-1,k) + 2(2^n - 2)$.*

Theorem 3.11. *Let $S \subseteq \mathbb{Z}^n$ be a set of points such that $S = \mathrm{ic}(S)$ and let $P = \{x \in \mathbb{R}^n : Ax \leq b\}$ be any system of inequalities with $P \cap \mathbb{Z}^n = S$. Let p denote the number of inequalities. Then $c(S) \leq p(2^n - 1)$.*

Proof. The statement is implied by the Doignon-Bell-Scarf Theorem if $S = \emptyset$, so suppose $S \neq \emptyset$. Consider a stable system of inequalities whose integer points are the set S and let $Q = \{x \in \mathbb{R}^n : Ax \leq b\}$ be the system obtained after applying Lemma 2.1. Q also has $c(S)$ facets, and each facet has one integer point in its interior. Let $T = \{t_1, t_2, \ldots, t_{c(S)}\}$ denote these points. Apply Lemma 2.1 to P as well and perturb the result to get a polytope with integral solutions S in its interior and no integer points on its boundary. We denote the new polytope again by P; we may have reduced the size of its inequality description but this will only tighten the lower bound. We have $P \cap \mathbb{Z}^n = \mathrm{int}(Q) \cap \mathbb{Z}^n$, and in particular $T \cap P = \emptyset$.

Consider the relative positions of the facets of Q and the facets of P. The fact that every facet of Q contains an integral point in T implies that no facet of Q is contained in P. For each facet F of P, let $H_F = \{x \in \mathbb{R}^n \mid a_F \cdot x \leq b_F\}$ be the halfspace such that $F = H_F \cap P$. Without loss of generality, we can assume that $a_F \in \mathbb{Q}^n$ and $b_F \in \mathbb{R} \setminus \mathbb{Q}$, so there are no integer points on the hyperplane $a_F \cdot x = b$.

Let $Q_F = Q \cap H_F$, clearly there are at most p such polytopes. For every F, one facet of Q_F shares its supporting hyperplane with a facet of P, and the remaining facets of Q_F are contained in facets of Q. We call these the P-facet and the Q-facets of Q_F, respectively. Notice that each point $t_i \in T$ lies on the interior of some Q-facet.

For every F, $\mathrm{int}(Q_F) \cap \mathbb{Z}^n = \emptyset$. Let $Cx \leq d$ be a minimal inequality description of Q_F. By perturbing Q_F slightly so it contains no integer points and applying the Doignon-Bell-Scarf Theorem, there is a subsystem of at most 2^n of these inequalities so that the resulting polytope also contains no integral points in its interior. Let the resulting polytopes be denoted Q'_F. No inequality corresponding to a Q-facet can be removed where a point from T is present, and the P-facet cannot be removed, since removing these clearly introduces S into the interior. Thus, the number of Q-facets in Q'_F is at most $2^n - 1$, and every Q-facet is represented in at least one of the polytopes Q'_F because that facet's integral point is. Thus the total number of facets of Q is at most $p(2^n - 1)$, since there are p polytopes Q_F. Since Q has $c(S)$ facets, this proves that $c(S) \leq p(2^n - 1)$. ∎

4 Asymptotic Lower Bounds

In this section, we prove that $c(n,k)$ is at least as large as the maximum number of vertices of any lattice polytope with k non-vertex integer points. It follows that exhibiting such a polytope with many vertices gives a lower bound for $c(n,k)$. We use the integer hull of the hyperball. The result is a lower bound for $c(n,k)$ whenever there exists $r > 0$ so that k is the number of non-vertex lattice points in the integer hull of the hyperball with radius r. We do not know if every $k \in \mathbb{N}$ can be achieved in this way, for example by a translation of the hyperball, so this leads us to a lower bound on $c(n,k_r)$ only for a sequence of values $k_r \to \infty$. The problem is compounded by the fact that $c(n,k)$ may decrease as k increases, which makes it difficult to extend the bound from the sequence k_r to all $k \geq 0$. Fortunately, as the next lemma shows, the decrease is modest. This is enough to fill in the gaps between consecutive values k_r.

Lemma 4.1. *For all $k, n \geq 1$, $c(n,k) \geq c(n,k-1) - 1$.*

Proof. Let $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$ be stable with $c(n,k-1)$ inequalities and containing $k-1$ lattice points. Let $P' = \{x \in \mathbb{R}^n : A'x \leq b'\}$ as given in Lemma 2.1. Then there exists an $\epsilon > 0$ such that $P'' = \{x \in \mathbb{R}^n : a'_1 \cdot x \leq b'_1, a'_i \cdot x \leq b'_i - \epsilon \text{ for all } i = 2, \ldots, c(n,k-1)\}$ contains exactly k lattice points. By construction, there are $c(n,k-1)-1$ inequalities, those numbered $2, 3, \ldots, c(n,k-1)$, that cannot be removed from P'' without increasing the number of integer points in P''. Hence, $c(n,k) \geq c(n,k-1) - 1$. ∎

As with the upper bound, our lower bound is proved by considering integer points in convex position.

Definition 4.2. Let

$$\alpha(n,k) \coloneqq \max \{|S| : S \subseteq \mathbb{Z}^n \text{ in convex position}, |\operatorname{ic}(S) \setminus S| = k\}. \tag{4}$$

In other words, $\alpha(n,k)$ is the maximum number vertices of a lattice polytope that contains exactly k lattice points. A related quantity has been studied by Averkov [5]. Let X be a discrete subset of $\mathbb{R}^n$ and let $f(X)$ denote the maximum number vertices of a polytope P with vertices in X such that P no other vertices in X. If follows from [5] that $f(X)$ is equivalent to the Helly number of X. See also [3, 18]. Clearly $\alpha(n,k) \leq \max\{f(\mathbb{Z}^n \setminus Y) : Y \subseteq \mathbb{Z}^n, |Y| = k, \operatorname{ic}(Y) = Y\}$, but it is unclear if these are always equal.

Many lower bounds for $\alpha(2,k)$ can be found in [12]. In that paper, Castryck studies the number of interior lattice points for convex lattice n-gons in the plane. They define the genus $g(n)$ as the minimum number of interior lattice points of a lattice n-gon. They compute $g(n)$ for $n = 1, \dots, 30$ and also provide related information such as the number of equivalence classes up to lattice invariant transformations. Although the computations done here are with respect to interior lattice points, many of their examples have no boundary lattice points that are not vertices. Therefore, these examples provide lower bounds on the values of $\alpha(2,k)$ and hence $c(2,k)$. For example, $\alpha(2,17) \geq 11$, $\alpha(2,45) \geq 15$, $\alpha(2,72) \geq 17$, and $\alpha(2,105) \geq 19$.

Our strategy is to prove that $c(n,k) \geq \alpha(n,k)$ and then use known properties of the integer hull of the Euclidean ball to prove a lower bound on $\alpha(n,k)$. The first lemma in this direction is the following.

Lemma 4.3. *Let $k \in \mathbb{Z}_{\geq 0}$ and $S \subseteq \mathbb{Z}^n$ be a maximizer of* (4)*. There exists a polyhedron $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$ with $|S|$ facets such that* (a) *each point of S is contained in the relative interior of a different facet of P and* (b) $P \cap \mathbb{Z}^n = \mathrm{ic}(S)$.

Proof. Because the points in S are in convex position, for each $x_i \in S$ there exists $a_i \in \mathbb{R}^n$ and $b_i \in \{0,1\}$ such that $a_i \cdot x_i = b_i$ and, for all $y \in S \setminus \{x_i\}$, $a_i \cdot y < b_i$. Let A and b represent the combined system of inequalities $a_i \cdot x \leq b_i$, for all $x_i \in S$, and let $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$. By construction P has $|S|$ facets and satisfies (a).

Furthermore, $\mathrm{conv}(S) \subseteq P$, so $\mathrm{ic}(S) \subseteq P \cap \mathbb{Z}^n$, as well. Suppose, for contradiction, that P does not satisfy (b), so that there exists an integral point in P that is not in the convex hull of S. Let $x \in \mathbb{Z}^n$ be such a point that minimizes $d(x, \mathrm{conv}(S)) := \min_{s \in \mathrm{conv}(S)} \|x - s\|_2^2$. Notice that $S \cup \{x\}$ is in convex position because we chose $x \notin \mathrm{conv}(S)$ and each point of S is alone on the interior of some facet of P. It suffices for us to show that $\mathrm{ic}(S) \setminus S = \mathrm{ic}(S \cup \{x\}) \setminus (S \cup \{x\})$, because this contradicts the maximality of S.

Indeed, suppose that there is an integral point $y \in P \setminus \mathrm{conv}(S)$ and some $s \in \mathrm{conv}(S)$ such that $y = \lambda x + (1-\lambda)s$, $0 < \lambda < 1$. The function $d(\cdot, \mathrm{conv}(S))$ is a convex function on $\mathbb{R}^n$, so $d(y, \mathrm{conv}(S)) \leq \lambda d(x, \mathrm{conv}(S)) < d(x, \mathrm{conv}(S))$, which contradicts the choice of x. Thus, $\mathrm{ic}(S \cup \{x\}) \setminus (S \cup \{x\}) = \mathrm{ic}(S) \setminus S$, which completes the proof. ∎

Lemma 4.4. *For all $n \geq 1$ and $k \geq 0$, $c(n,k) \geq \alpha(n,k)$.*

Proof. Let S be a maximizer of (4) and let $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$ be the polyhedron from Lemma 4.3. We have $\mathrm{ic}(S) \setminus S \subseteq \mathrm{int}(P)$. Thus, there exists $\epsilon > 0$ such that, for $b' = b - \epsilon\vec{\mathbf{1}}$, the polyhedron $P' = \{x \in \mathbb{R}^n \mid Ax \leq b'\}$ has $\mathrm{ic}(S) \setminus S = P' \cap \mathbb{Z}^n$ and removing any inequality from $Ax \leq b'$ adds a point from S to the polyhedron. $c(n,k)$ is at least as large as the smallest subsystem of $Ax \leq b'$ that preserves the set of interior integral points. We have just shown that the smallest such subsystem is the entire system of inequalities, which has cardinality $|S| = \alpha(n,k)$. Therefore, $c(n,k) \geq \alpha(n,k)$. ∎

Notice that Lemma 4.4 is already a useful result to quickly obtain some bounds on $c(n,k)$. For example, we can get a much shorter proof of $c(n,1) \geq 2(2^n - 1)$ (and thus

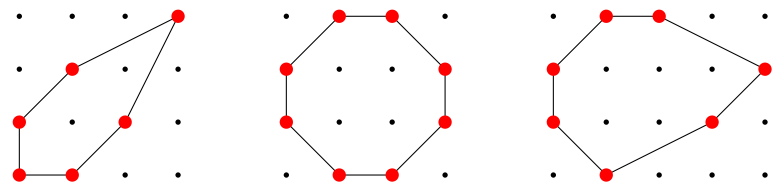

Figure 1: This figure gives three examples of integer point configurations which imply lower bounds for $c(n,k) \geq \alpha(n,k)$. In each example, the set S is the set of integer points colored red that create the vertices of a polygon containing other integer points. From left to right, these examples show that $\alpha(2,2) \geq 6$, $\alpha(2,4) \geq 8$, and $\alpha(2,5) \geq 7$.

$c(n,1) = 2(2^n - 1)$ by our upper bound on $c(n,1)$) than the example presented in [1]. It suffices to consider $S = (\{-1,0\}^n \cup \{0,1\}^n) \setminus \{0\}^n$, and observe that S is in convex position and fulfills $|\operatorname{ic}(S) \setminus S| = |\{0\}^n| = 1$. Hence, $\alpha(n,1) \geq |S| = 2(2^n-1)$, and by Lemma 4.4, $c(n,1) \geq \alpha(n,1) \geq 2(2^n-1)$.

The authors of [1] use (1) to prove $c(n,2) \leq 2(2^n-1)$ and leave it as an open question of this bound is tight.

Proposition 4.5. $c(n,2) = 2(2^n-1)$

Proof. From (1), or also Theorem 3.9, we see that $c(n,2) \leq 2(2^n-1)$. We show that $c(n,2) \geq \alpha(n,2) \geq 2(2^n-1)$.

Consider the set $S = (\{-1,0\}^n \cup \{0,1\}^n \cup \{\vec{\mathbf{2}}\}) \setminus \{\vec{\mathbf{0}}, \vec{\mathbf{1}}\}$, there $\vec{\mathbf{t}}$ denotes the vector with all entries t. Notice that $|S| = 2(2^n-1)$, S is in convex position, and $(\operatorname{conv}(S) \cap \mathbb{Z}^n) \setminus S = \{\vec{\mathbf{0}}, \vec{\mathbf{1}}\}$. Hence, $c(n,2) \geq \alpha(n,2) \geq 2(2^n-1)$. ■

Upon replacing $\vec{\mathbf{2}}$ with $\vec{\mathbf{k}}$ in the last proof one can find lower bound of $2(2^n-1)$ on $c(S)$ for any collinear set S of $k \geq 2$ points where $\operatorname{ic}(S) = S$. Thus $c(S) = 2(2^n-1)$ for any set S of $k \geq 2$ collinear points with $\operatorname{ic}(S) = S$, by Theorem 3.9.

We now use the integer points in a ball to give a lower bound on $c(n,k)$. We begin by exhibiting a sequence that lower bounds many values of $\alpha(n,k)$, and therefore $c(n,k)$, for many values of k. We will then use Lemma 4.1 to connect these lower bounds to all other entries k.

Theorem 4.6. *For each $n \geq 2$, there exists a constant C, depending only on n, such that*

$$c(n,k) \geq Ck^{\frac{n-1}{n+1}}.$$

Proof. Throughout, we will assume that the dimension n is fixed. Hence, many of the constants used in the proof will depend on n.

By [19], there exists $u \in \mathbb{R}^n$ such that for all $N \in \mathbb{Z}_+$, there exists a radius R such that $|B_n(u,R) \cap \mathbb{Z}^n| = N$. Fix a $u \in U \cap B_n(0,1)$. Define

$$N_r := |B_n(u,r) \cap \mathbb{Z}^n|, \quad v_r := |\operatorname{vert}(\operatorname{conv}(B_n(u,r) \cap \mathbb{Z}^n))|, \quad k_r := N_r - v_r.$$

The number of integer points contained in a ball of radius r in n-dimensions is known to grow asymptotically as $r^n \operatorname{vol}(B_n(0,1))$, where $\operatorname{vol}(S)$ denotes the n-dimensional volume of S. For $n \geq 4$, it is known that the error term is of order r^{n-2}, and for $n = 2, 3$, the exact orders are still unknown. For our purposes, we can use the weaker error order of $r^{\frac{n(n-1)}{n+1}}$, which holds for all $n \geq 2$ [7]. It is easy to see that these results apply also to any translate of the ball from the origin. Hence, we have

$$N_r = \operatorname{vol}(B_n(0,1))r^n + \mathcal{E}(r), \quad \text{where} \quad \mathcal{E}(r) = O(r^{\frac{n(n-1)}{n+1}}). \tag{5}$$

Bárány and Larman [9] show that the number of vertices of the integer hull of a ball of radius r in n-dimensions grows like $r^{\frac{n(n-1)}{n+1}}$. Since their arguments do not depend on the center of the ball, their work shows that there exist constants C_1, C_2 such that

$$C_1\, r^{\frac{n(n-1)}{n+1}} \leq v_r \leq C_2\, r^{\frac{n(n-1)}{n+1}}. \tag{6}$$

See also [8] for a discussion of this problem and related extremal problems.

From (5) and (6), we see that there exist constants C_3, C_4 such that

$$C_3\, r^n \leq k_r \leq C_4\, r^n. \tag{7}$$

It follows that

$$\alpha(n, k_r) \geq v_r \geq C_1 r^{\frac{n(n-1)}{n+1}} \geq C_1 \left(\frac{k_r}{C_4}\right)^{\frac{n-1}{n+1}} = C_5\, k_r^{\frac{n-1}{n+1}}.$$

By Lemma 4.4, we have that

$$c(n, k_r) \geq C_5\, k_r^{\frac{n-1}{n+1}}. \tag{8}$$

This shows that for all k such that $k = k_r$, for some value r, the theorem holds. We will now show that we can extend the lower bound to all values sufficiently large values of k.

Fix $k \in \mathbb{Z}_+$. Next, fix r, R such that $k_r \leq k \leq k_R$. By the choice of $u \in U$, we can choose r, R such that

$$|N_r - N_R| = 1.$$

For this to hold, we must have $|r - R| \leq 1$. Therefore, it follows from (7) that

$$k \leq k_R \leq C_4 R^n \leq C_4 (r+1)^n \leq C_6\, k_r \tag{9}$$

for some constant C_6. By (8) and (9) we see that

$$c(n, k_r) \geq C_5 k_r^{\frac{n-1}{n+1}} \geq C_5 \left(\frac{k}{C_6}\right)^{\frac{n-1}{n+1}} = \left(\frac{C_5}{C_6^{\frac{n-1}{n+1}}}\right) k^{\frac{n-1}{n+1}}. \tag{10}$$

Next, we derive an upper bound for the difference $|k - k_r|$. First notice that

$$0 \leq k - k_r \leq k_R - k_r \leq N_R - N_r + v_r - v_R = 1 + v_r - v_R.$$

Therefore, it is important that we estimate the difference in the number of vertices v_r and v_R. Let $\bar{x} \in (B_n(u,R) \setminus B_n(u,r)) \cap \mathbb{Z}^n$ be the single integer point that is not in common in both balls. When $\bar{x}$ is included in the ball, some of the vertices of $\mathrm{conv}(B_n(u,r) \cap \mathbb{Z}^n)$ cease to be extreme points. Let $V_R = \mathrm{vert}(\mathrm{conv}(B_n(u,R) \cap \mathbb{Z}^n))$, $V_r = \mathrm{vert}(\mathrm{conv}(B_n(u,r) \cap \mathbb{Z}^n))$. Let $P = \mathrm{conv}(V_R)$ and $Q = \mathrm{conv}(V_R \setminus \{\bar{x}\})$. From these definitions, we have that $|v_r - v_R| = |V_r \cap (P \setminus Q)|$.

The strategy for the rest of the proof to find a spherical cap of $B_n(u,R)$ that contains all of the vertices that are "lost" when $\bar{x}$ is added to the ball. The number of points in the cap can be bounded using its volume. We should expect to be able to find a small cap because all of the vertices of $\mathrm{conv}(B_n(u,r) \cap \mathbb{Z}^n$ are contained in a thin spherical shell near the surface of the ball.

Let $V_{\bar{x}}$ denote the set of vertices z of P such that there exists an edge $[\bar{x}, z]$ of P. Let $T = \mathrm{conv}(V_{\bar{x}} \cup \{\bar{x}\})$.

We claim that $T \supseteq P \setminus Q$. To see this let $\mathrm{cone}_{\bar{x}}(P) = \{g \in \mathbb{R}^n :$ there exits $\lambda \geq 0$ such that $\bar{x} + \lambda g \in P\}$. It follows that $\mathrm{cone}_{\bar{x}}(P) = \mathrm{cone}(\{z - \bar{x} : z \in V_{\bar{x}}\})$ where $\mathrm{cone}(X) = \{\sum_{x \in X} \mu_x x : \mu_x \geq 0\}$. Let $y \in P \setminus Q$. Since P is convex, there exists $g \in \mathrm{cone}_{\bar{x}}(P)$ such that $y = x + g$. Then $g = \sum_{z \in V_{\bar{x}}} \mu_z (z - \bar{x})$ for some $\mu \geq 0$. Let $\bar{\mu} = \sum_{z \in V_{\bar{x}}} \mu_z$. Define $\bar{y} = \bar{x} + \frac{1}{\bar{\mu}} g = \sum_{z \in V_{\bar{x}}} \frac{\mu_z}{\bar{\mu}} z \in \mathrm{conv}(V_{\bar{x}}) \subseteq Q$. Next, define $\tilde{y} = \bar{x} + \lambda g$ where $\lambda = \max\{\lambda : \bar{x} + \lambda g \in P\}$. By definition, $\lambda \geq 1$ and $\tilde{y}$ lies in a face of P that does not contain $\bar{x}$. Therefore $\tilde{y} \in Q$. Finally, if $\bar{\mu} \leq 1$, then $y = \bar{x} + g = (1 - \bar{\mu})\bar{x} + \sum_{z \in V_{\bar{x}}} \mu_z z \in T$. Otherwise, $\bar{\mu} > 1$. But then $\frac{1}{\bar{\mu}} < 1 \leq \lambda$. Therefore $y \in \mathrm{conv}(\{\bar{y}, \tilde{y}\}) \in Q$, which is a contradiction. Therefore, $T \supseteq P \setminus Q$.

We may assume, without loss of generality, that $r \geq 2\sqrt{n}$, as this may be accounted for by adjusting the final constant C. Since $R \geq r \geq 2\sqrt{n}$, it holds that $P \supseteq B_n(u, R - 2\sqrt{n})$. If this is not the case, then, since these are convex sets, there exists an inequality $a \cdot x \leq b$ valid for $\mathrm{ic}(B_n(u,r))$, but is not valid for $B_n(u, R - \sqrt{n})$. Let $y = \arg\max\{a \cdot x : x \in B_n(R, -2\sqrt{n}\}$ by the unique maximizer of the linear functional $a \cdot x$. Next, let $z = \frac{R - \sqrt{n}}{\|y\|_2} y$. It follows that $B_n(z, \frac{1}{2}\sqrt{n}) \cap \mathrm{ic}(B_n(u,R)) = \emptyset$ while $B_n(z, \frac{1}{2}\sqrt{n}) \subseteq B_n(u,R)$. But since any ball of radius $\frac{1}{2}\sqrt{n}$ must contain an integer point, we have that $B_n(z, \sqrt{n}) \cap \mathbb{Z}^n \neq \emptyset$, which is a contradiction.

Next we claim that any edge e of P has Euclidean length at most $4\Delta^{\frac{1}{2}} R^{\frac{1}{2}}$ where $\Delta = 2\sqrt{n}$. Since $P \supseteq B_n(u, R - 2\sqrt{n})$, every edge of P must not intersect the interior of $B_n(R - 2\sqrt{n})$. Clearly the Euclidean length of any edge of P is at most the length of the longest chord in $B_n(u,r) \setminus \mathrm{int}(B_n(u, r - \Delta))$. By the Pythagorean Theorem, it is easy to see that the length of the longest chord in $B_n(u,R) \setminus \mathrm{int}(B_n(u, R - \Delta))$ is

$$2\sqrt{R^2 - (R - \Delta)^2} = 2\sqrt{2R\Delta + \Delta^2} \leq 4\Delta^{\frac{1}{2}} R^{\frac{1}{2}}.$$

By convexity of T and the function $\|\cdot\|_2$, since $\|z - \bar{x}\|_2 \leq 4\Delta^{\frac{1}{2}} R^{\frac{1}{2}}$ for all $z \in V_{\bar{x}}$, we have that

$$T \subseteq B_n(\bar{x}, 4\Delta^{\frac{1}{2}} R^{\frac{1}{2}}).$$

Therefore the volume $\mathrm{vol}(T) \le C_7 R^{\frac{n}{2}}$. By [4] (see also [8]), the number of vertices of any full dimensional lattice polytope $K \subseteq \mathbb{R}^n$ is at most $C_8 \,\mathrm{vol}(K)^{\frac{n-1}{n+1}}$ for some constant C_8. Note that T has positive volume by its definition and the fact that $\mathrm{conv}(B_n(u,R) \cap \mathbb{Z}^n)$ has positive volume. Further, if $\mathrm{conv}((T \setminus \{\bar{x}\}) \cap \mathbb{Z}^n)$ does not have positive volume, then $\mathrm{vert}(\mathrm{conv}((T \setminus \{\bar{x}\}) \cap \mathbb{Z}^n)) = \mathrm{vert}(\mathrm{conv}(T)) \setminus \{\bar{x}\}$. Since

$$\mathrm{vert}(\mathrm{conv}((T \setminus \{\bar{x}\}) \cap \mathbb{Z}^n)) \supseteq (V_r \setminus V_R),$$

it follows that $|V_r \setminus V_R| \le C_8 (C_7 R^{\frac{n}{2}})^{\frac{n-1}{n+1}} \le C_8 (C_7 C_6^{\frac{1}{2}} k_r^{\frac{1}{2}})^{\frac{n-1}{n+1}}$. Since $v_r - v_R = |V_r \setminus V_R|$ and that $|R - r| \le 1$, we see that there exists a constant C_9 such that

$$|k_r - k_R| = |v_r - v_R| \le C_9 k_r^{\frac{n-1}{2(n+1)}}. \tag{11}$$

Finally, by applying induction to Lemma 4.1, we see that

$$c(n,k) \ge c(n,k_r) - |k - k_r|. \tag{12}$$

Combining equations (10), (11), and (12), we have that

$$c(n,k) \ge c(n,k_r) - |k - k_r| \ge \left(\frac{C_5}{C_6^{\frac{n-1}{n+1}}} \right) k^{\frac{n-1}{n+1}} - C_9 k_r^{\frac{n-1}{2(n+1)}} \ge C k^{\frac{n-1}{n+1}},$$

where, C is a constant. This completes the proof. ■

We remark that the bound we give above on $v_r - v_R$ is likely quite loose. This is because we use the fact that $\mathrm{conv}(B_n(u,R) \cap \mathbb{Z}^n) \supseteq B_n(u, R - \Delta)$ for $\Delta = 2\sqrt{n}$ and because we bound the volume of the cap by the volume of a ball with the same radius. The value Δ can likely decrease with the size of R. For comparison, $\mathrm{vert}(\mathrm{conv}(B_n(0,r) \cap \mathbb{Z}^n)) \subseteq B_n(0,r) \setminus B_n(0, r - \delta)$ where $\delta \le C r^{-\frac{n-1}{n+1}}$ [7] .

5 Non-monotonicity of $c(n,k)$ in k

It is easy to see that $c(n,k)$ is nondecreasing in n. So, it is natural to ask whether $c(n,k)$ is nondecreasing in k. It is not. Lemmas 5.2 and 5.3 show that $c(2,5) \le 7$ and $c(2,4) \le 8$. The reverse inequalities are established by the examples in Figure 1. The next proposition will help with some case analysis in the proof of Lemma 5.2

Proposition 5.1. *Let $S \subseteq \mathbb{R}^2$. If the points in S are all collinear then $|M(S)| \ge |S| - 1$. If the points in S are not all collinear then $|M(S)| \ge 2|S| - 3$.*

Proof. The first claim is trivial. If the points are not collinear, then any triangulation of S has at least $2|S| - 3$ edges [15], and each edge contains a distinct midpoint. ■

Lemma 5.2. $c(2,5) \le 7$.

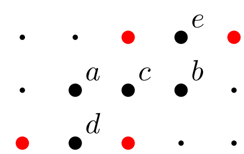

Figure 2: The five interior (black) and facet (red) points for the final case in the proof of Lemma 5.2.

Proof. Let $P \subseteq \mathbb{R}^2$ be a stable polytope with $c(2,5)$ facets and containing five integer points. Applying Lemma 2.2 yields a set $T \subseteq \mathbb{Z}^2$ of cardinality $c(2,5)$ in convex position such that $\mathrm{ic}(T) \setminus T \subseteq P \cap \mathbb{Z}^2$.

Partition the points in $T \cup (P \cap \mathbb{Z}^2)$ according to their parities. If every parity class has three or fewer points, then $c(2,5)+5 \leq 12$, hence $c(2,5) \leq 7$. If any parity class contains five or more points, then Proposition 5.1 implies that $|P \cap \mathbb{Z}^2| \geq 7$, a contradiction. We will now show that it is possible for one parity class to have four points, but in this case the remaining parity classes have no more than eight points combined. This implies $c(n,k) \leq 7$.

First, if any parity class contains four collinear points, then all five of the integer points in P are collinear. It follows from Theorem 3.9 that $|T| \leq 6$.

Suppose that no parity class contains four collinear points, but some parity class contains four points which are not collinear. By Proposition 5.1 there are at least five (integral) midpoints among them. As all of the midpoints are integral points in P, there can be no more then five, and the four points of the parity class lie on the boundary of P'. Since the four points have only five (rather than six) distinct midpoints they must form the vertices of a parallelogram.

Consider the parity classes of the five interior integer points. The above arguments show that no four or five of them can be in one parity class. It is impossible for any three to be in the same parity class since this implies that the five interior points are collinear, which cannot happen because we have already shown that they are the midpoints of a set of four points in convex position.

One parity class is taken entirely by the four vertices of the parallelogram, so we are left with the five interior points in three parity classes, with two classes containing two of the points and the third class containing one point. We claim that no point in T can lie in a parity class with two interior points. If we label the points as in Figure 5, then the interior points are grouped into parity classes as $\{\{a,b\},\{c\},\{d,e\}\}$.

We will prove that no point in T lies in the parity classes with a,b or d,e. All together, this implies that the size of the classes are at most $4,3,2,2$ hence there are 11 total points so $|T| \leq 11-5=6$.

Suppose, for contradiction, that a point $z \in \mathbb{Z}^2$ lies on a facet of P' and is in the same parity class as a and b. We have $m_1 = \frac{1}{2}(z+a)$ and $m_2 = \frac{1}{2}(z+b)$ are in $\mathrm{int}(P')$. If we show that $\{m_1, m_2\} \not\subseteq \{a,b,c,d,e\}$, then we have the desired contradiction. We have already shown that z cannot be a vertex of the parallelogram. If z is collinear with a and b, then at least one of $\{m_1, m_2\}$ is not among $\{a, b, c, d, e\}$ which is a contradiction. If b is not collinear with a and b, then it lies in an open half-space to one side of the line through a and b. The midpoints m_1 and m_2 lie in the same open half space, but none of $\{a, b, c\}$ are there and at most one of $\{d, e\}$. Therefore, $\{m_1, m_2\} \not\subseteq \{a, b, c, d, e\}$. ■

Lemma 5.3. *$c(2, 4) \leq 8$.*

Proof. By Lemmas 4.1 and 5.2 we have

$$c(2, 4) \leq c(2, 5) + 1 \leq 8.$$

■

References

[1] Iskander Aliev, Robert Bassett, Jesús A. De Loera, and Quentin Louveaux. A quantitative Doignon-Bell-Scarf theorem. eprint arXiv:1405.2480 [math.CO], to appear in *Combinatorica*, 2015.

[2] Iskander Aliev, Jesús A. De Loera, and Quentin Louveaux. Integer programs with prescribed number of solutions and a weighted version of Doignon-Bell-Scarf's Theorem. In Jon Lee and Jens Vygen, editors, *Integer Programming and Combinatorial Optimization*, volume 8494 of *Lecture Notes in Computer Science*, pages 37–51. Springer International Publishing, 2014.

[3] Nina Amenta, Jesús A. De Loera, and Pablo Soberón. Helly's Theorem: New variations and applications. *arXiv preprint arXiv:1508.07606*, 2015.

[4] George E. Andrews. A lower bound for the volume of strictly convex bodies with many boundary lattice points. *Transactions of the American Mathematical Society*, 106(2):270–279, 1963.

[5] Gennadiy Averkov and Robert Weismantel. Transversal numbers over subsets of linear spaces. *Advances in Geometry*, 12:19–28, 2012.

[6] Michel Baes, Timm Oertel, and Robert Weismantel. Duality for mixed-integer convex minimization. *Mathematical Programming*, pages 1–18, 2015.

[7] Antal Balog and Imre Bárány. On the convex hull of the integer points in a disc. In *Proceedings of the Seventh Annual Symposium on Computational Geometry*, SCG '91, pages 162–165, New York, NY, USA, 1991. ACM.

[8] Imre Bárány. Extremal problems for convex lattice polytopes: a survey. In Jacob E. Goodman, János Pach, and Richard Pollack, editors, *Surveys on discrete and computational geometry: Twenty years later*, Contemporary mathematics, pages 87–103. American Mathematical Society, 2008.

[9] Imre Bárány and David G. Larman. The convex hull of the integer points in a large ball. *Mathematische Annalen*, 312(1):167–181, 1998.

[10] Imre Bárány and Norihide Tokushige. The minimum area of convex lattice n-gons. *Combinatorica*, 24(2):171–185, 2004.

[11] David E. Bell. A theorem concerning the integer lattice. *Studies in Applied Mathematics*, 56(2):187–188, 1977.

[12] Wouter Castryck. Moving out the edges of a lattice polygon. *Discrete & Computational Geometry*, 47(3):496–518, 2012.

[13] Kenneth L. Clarkson. Las Vegas algorithms for linear and integer programming when the dimension is small. *Journal of the ACM*, 42(2):488–499, March 1995.

[14] M. Conforti, G. Cornuéjols, and G. Zambelli. Corner polyhedra and intersection cuts. *Surveys in Operations Research and Management Science*, 16:105–120, 2011.

[15] Mark De Berg, Marc Van Kreveld, Mark Overmars, and Otfried Cheong Schwarzkopf. *Computational geometry.* Springer, 2000.

[16] Jean-Paul Doignon. Convexity in cristallographical lattices. *Journal of Geometry*, 3(1):71–85, 1973.

[17] Paul Erdös, Peter C. Fishburn, and Zoltán Füredi. Midpoints of diagonals of convex n-gons. *SIAM Journal on Discrete Mathematics*, 4(3):329–341, 1991.

[18] A. J. Hoffman. Binding constraints and helly numbers. *Annals of the New York Academy of Sciences*, 319(1):284–288, 1979.

[19] Tomasz Kochanek. Steinhaus' lattice-point problem for Banach spaces. May 2013.

[20] Ezra Miller and Bernd Sturmfels. *Combinatorial commutative algebra*, volume 227. Springer Science & Business Media, 2005.

[21] János Pach. Midpoints of segments induced by a point set. *Geombinatorics*, 13(2):98–105, 2003.

[22] Stanley Rabinowitz. $O(n^3)$ bounds for the area of a convex lattice n-gon. *Geombinatorics*, 2:85–88, 1993.

[23] Tom Sanders. Three-term arithmetic progressions and sumsets. *Proceedings of the Edinburgh Mathematical Society (Series 2)*, 52:211–233, 2009.

[24] Herbert E. Scarf. An observation on the structure of production sets with indivisibilities. *Proceedings of the National Academy of Sciences*, 74(9):3637–3641, 1977.

[25] Yonutz V. Stanchescu. Planar sets containing no three collinear points and non-averaging sets of integers. *Discrete Mathematics*, 256(1-2):387 – 395, 2002.