Bounded integer polytopes with few vertices and many interior lattice points

Noga Alon, nalon@math.princeton.edu

Abstract: What is the maximum possible number of lattice points in a lattice polytope with at most t vertices in the set $\{-d, -d+1, \ldots, 0, 1, \ldots, d\}^n$? We show that if for some fixed $\varepsilon > 0$ $d^2 \log(et/n) \leq n^{1-\varepsilon}$ and $t \geq n^{1+\varepsilon}$ then this maximum is $t^{\Theta(d^2 \log n)}$.

1 Introduction

A lattice polytope is a polytope whose vertices have integer coordinates. Let $f(n, t, d)$ denote the maximum possible number of lattice points in a lattice polytope with at most t vertices in the set $\{-d, -d+1, \ldots, 0, 1, \ldots, d\}^n$. Motivated by the study of factors of sparse multivariate polynomials which arises in the investigation of deterministic factorization algorithms for such polynomials, Bhargava, Saraf and Volkovich [3] proved that

$$f(n, t, d) \leq t^{O(d^2 \log n)} = e^{O(d^2 \log n \log t)} \tag{1}$$

All logarithms here and in what follows are in the natural base e unless otherwise specified. The inequality above is proved by using an approximate Carathédory result that the authors attribute to [4], but the result used is for the ℓ_∞-norm, which is proved earlier in [1]. It is mentioned in [1] that this also follows as a special case of Maurey's Lemma.

An example, due to Saptharishi, described in [3] shows that the above inequality is tight up to the hidden constant in the O-notation at the exponent for $d = 1$. Ilya Volkovich communicated a question first raised by Shubhangi Saraf and Avi Wigderson in 2019 [7]. This question is whether or not the estimate (1) can be improved for t much larger than n. Specifically, it is the following question.

Problem 1.1. *Does the following inequality hold ?*

$$f(n, t, d) \leq t^{poly(d)} n^{O(\log n)}$$

In a more recent paper [8] Saraf and Varadarajan obtain lower bounds for $f(n, n, d)$ for larger values of d. They show that for every fixed $\varepsilon > 0$

- $f(n, n, d) \geq n^{\Omega(d \log n)}$ for $d \leq \frac{\log n}{4}$
- $f(n, n, d) \geq n^{\Omega((\log n)^2)}$ for $\frac{\log n}{4} \leq d \leq (\log n)^{1.5}$
- $f(n, n, d) \geq n^{\varepsilon d^2/(2 \log n)}$ for $(\log n)^{1.5} \leq d \leq (n \log n)^{1/2-\varepsilon}$
- $f(n, n, d) \geq (d^{2\varepsilon}/4)^n$ for $(n \log n)^{1/2+\varepsilon} \leq d < n \log n$

Here we first describe a short self-contained proof showing that the answer to problem 1.1 is negative.

Theorem 1.2. *For any integer $k < n/100$ there is a collection of $t = 10n \cdot 2^k$ vectors in $\{-1, 1\}^n$ so that their convex hull contains all vectors in $\{-1, 0, 1\}^n$ with support of size at most k. In particular, for any t satisfying $n^2 \leq t \leq 2^{\sqrt{n}}$*

$$f(n, t, 1) \geq \sum_{i=0}^{\log_2(t/10n)} \binom{n}{i} 2^i \geq n^{0.25 \log_2 t} = e^{\Omega(\log n \log t)}.$$

This shows that the estimate (1) is tight up to the hidden constant in the exponent for $d = 1$ and all the values of t in the range above, showing that the answer to problem 1.1 is negative.

We next improve the lower bounds of [8], and determine the behaviour of $\log f(n, n, d)$ up to a constant factor in nearly all the admissible range of the parameters.

Theorem 1.3. *The following estimates hold for all positive integers d, n.*

1. *For $d \leq \sqrt{n}$, $f(n, n, d) \geq e^{\Omega(d^2(\log(2n/d^2))^2)}$*
2. *For $d \geq \sqrt{n}$, $f(n, n, d) \geq e^{\Omega(n \log(e^2 d^2/n))}$*

In particular, for any fixed $\varepsilon > 0$, if $d \leq n^{0.5-\varepsilon}$ then $f(n, n, d) = n^{\Theta(d^2 \log n)}$ and if $d \geq n^{0.5+\varepsilon}$ then $f(n, n, d) = d^{\Theta(n)}$

More generally, we consider the function $f(n, t, d)$ for all $n \leq t \leq 2^n$. Note that for $t = 2^n$, $f(n, t, d) = (2d + 1)^n$.

Theorem 1.4. *The following holds for $n \leq t \leq 2^n$.*

1. *If $d\sqrt{\log(et/n)} \leq \sqrt{n}$ then*

$$f(n, t, d) \geq e^{\Omega(d^2 \log(et/n) \log \frac{2n}{d^2 \log(et/n)})}.$$

2. *If*

$$d\sqrt{\log(et/n)} \geq \sqrt{n}$$

then

$$f(n, t, d) \geq (\min(d, \frac{d^2 \log(et/n)}{n}))^{\Omega(n)}.$$

In particular, if for some fixed $\varepsilon > 0$

$$d^2 \log(et/n) \leq n^{1-\varepsilon} \quad \text{and} \quad t \geq n^{1+\varepsilon}$$

then

$$f(n, t, d) = e^{\Theta(d^2 \log t \log n)} = t^{\Theta(d^2 \log n)}.$$

If

$$\frac{d^2 \log(et/n)}{n} \geq d^{\varepsilon} \quad \text{then} \quad f(n, t, d) = e^{\Theta(n \log(2d))} = (2d)^{\Theta(n)}.$$

The rest of this note is organized as follows. In the next section we describe a quick self-contained proof of Theorem 1.2. The proofs of Theorem 1.3 and Theorem 1.4 are presented in Section 3. We conclude with a brief description of some open problems in Section 4. To simplify the presentation we omit all floor and ceiling signs whenever these are not crucial, and assume, whenever needed, that the parameter n is sufficiently large.

2 Estimating $f(n, t, 1)$

The proof of Theorem 1.2 is probabilistic, and is based on the next geometric lemma. This lemma is established by following an elegant argument of Wendell [9]. The constant 6 in the statement of this lemma, as well as the constants 10 and 100 in Theorem 1.2 can be easily improved and we make no attempt to optimize them here.

Lemma 2.1. *Let $\mathcal{F}$ be a collection of N random vectors in $\{-1, 1\}^m$ chosen uniformly and independently among all 2^m vectors in this collection. Then the probability that the 0-vector is not in the convex hull of the vectors in $\mathcal{F}$ is at most*

$$2^{-N+1} \sum_{i=0}^{m-1} \binom{N-1}{i}.$$

In particular, if $N \geq 6m$ then this probability is smaller than $2^{-m/4}$.

Proof. Choose the vectors in $\mathcal{F}$ by first choosing randomly N pairs of vector v and $-v$ uniformly and independently in $\{-1, 1\}^m$, and then by choosing randomly exactly one vector of each pair in order to form $\mathcal{F}$. For each fixed choice of the N pairs of vectors, the choices that lead to a collection of vectors in which 0 is not in the convex hull correspond exactly to the choices of a subset of the $2N$ points in all these pairs that can be separated from the other points by a hyperplane through the origin. The result now follows from the known formula for the number of such subsets (that is, the number of ways to partition a set of N pairs of antipodal points in R^n into two subsets by such a hyperplane). This formula can be proved by induction, it is also simple to get its correct asymptotic by observing that we can always shift the hyperplane without changing the partition until it is determined by $m-1$ of the points (and the origin). □

Note that the result of Wendell [9] is formulated for random uniform points on the unit sphere, but the argument works for any symmetric distribution like the one considered here. We can now prove Theorem 1.2.

Proof. Let $\mathcal{T}$ be a random collection of $10n \cdot 2^k$ vectors in $\{-1, 1\}^n$, chosen randomly, independently and uniformly. Fix a set I of at most k coordinates, and fix values $\varepsilon_i \in \{-1, 1\}$ for each $i \in I$. The number of vectors in $\mathcal{T}$ that agree with ε_i for each $i \in I$ is a Binomial random variable with parameters $10n \cdot 2^k$ and probability $2^{-|I|} \geq 2^{-k}$. Therefore, by the standard estimates

for Binomial distributions (see, e.g., [2]) the probability that this number is smaller than $6n$ is (much) smaller than $2^{-n/10}$. Note that in order to identify such $6n$ vectors it suffices to expose only the coordinates of all vectors in $\mathcal{T}$ in the indices I, the other coordinates stay random.

Now choose $6n$ vectors with the required projection on I and expose their other coordinates. By Lemma 2.1 the probability that the 0-vector of length $n - |I|$ on all the coordinates not in I is not in the convex hull of these is less than $2^{-(n-|I|)/4}$. This together with the union bound over all $\sum_{i=0}^{k} \binom{n}{i} 2^i$ choices of I and ε_i for $i \in I$ complete the proof. □

3 The general case

In this section we describe the proofs of Theorem 1.3 and Theorem 1.4. The main ingredient in these proofs is a known result of Guédon, Litvak and Tatarko [5] (see also [6] for a short proof) about the geometry of random polytopes. We start with the statement of this result. Let B_∞^n denote the unit ℓ_∞ ball in R^n, and let B_2^n denote the unit ℓ_2 ball in R^n. Let ξ be a symmetric random variable with variance 1 which satisfies a small-ball condition, that is, there are constants $\alpha, \beta > 0$ so that the probability that $|\xi| \geq \alpha$ is at least β. Let $\mathcal{F}$ be a collection of N independent identically distributed random vectors $v_i \in R^n$ where each v_i has independent, identically distributed coordinates, each being a copy of ξ. The following result is proved in [6], Theorem 1.5, following a similar result proved in [5].

Theorem 3.1 ([5], [6]). *Let ξ, α, β, N, n and v_i be as above. Then there are two positive constants c_1, c_2 so that for $N \geq c_1 n$ the convex hull of the $2N$ vectors $\pm v_i$ contains, with high probability, the intersection*

$$c_2(B_\infty^n \cap \sqrt{\log(eN/n)} B_2^n).$$

The random variable ξ which attains the values $\{-1, 1\}$ with equal probability clearly satisfies the small-ball inequality (with $\alpha = \beta = 1$) and therefore the conclusion above holds when each v_i is a random vector in $\{-1, 1\}^n$.

Before proceeding with the proofs of the two theorems we observe that the function $f(n, t, d)$ is monotone non-decreasing in all the three variables. This is obvious for the variables t, d by the definition. For the variable n we note that for $n' < n$, $f(n, t, d) \geq f(n', t, d)$ by considering t vectors in which all the last $(n - n')$ coordinates are 0. Throughout the proofs we denote absolute positive constants by $c_1, c_2, c_3, \ldots$ (where the first two are from the conclusion Theorem 3.1) without specifying the precise relations among them.

Proof of Theorem 1.3, part 1. For constant d the required lower bound is already known, so we may and will assume that d is at least some large constant. By monotonicity $f(n, n, d) \geq f(n, n/2, c_3 d)$ for any $c_3 \leq 1$. By choosing an appropriate small c_3 we may assume that $n/2 \geq c_1(\sqrt{c_3} n)$, where c_1 is the constant from Theorem 3.1 (and $c_3 d$ is still at least 1). Moreover, since

the lower bound we have to prove has the same shape when replacing d by $\Theta(d)$ we rename the quantity $c_3 d$ and denote it by d for simplicity. Thus we may now assume that d is much smaller than $\sqrt{n}$ to ensure that the parameter m that we now define by $m = \sqrt{n}d$ satisfies $m < n/2c_1$. Taking now $N = n/2$ random vectors in $\{-d, d\}^m$ and appending $(n-m)$ 0-coordinates to each of them we conclude, by Theorem 3.1, that with high probability the convex hull of these vectors and their inverses fully contains the set

$$c_2 d(B_\infty^m \cap \sqrt{\log(en/(2\sqrt{n}d))} B_2^m),$$

where, with some abuse of notation, the two balls here are considered as balls on the first m coordinates, where the last $n-m$ coordinates are all 0. Fix n vectors (the random ones and their inverses) for which this is the case.

Note that $\log(en/2\sqrt{n}d) > 0.5 \log(2n/d^2)$. It thus follows that the convex hull of our n vectors contains every lattice vector which is 0 in the last $n-m$ coordinates, at most $c_2 d$ in absolute value in each other coordinate, and the sum of squares of the coordinates is at most some $c_4 d^2 \log(2n/d^2)$. For an appropriate choice of c_4 this quantity is smaller than m. In particular, the convex hull contains all vectors in which at most $c_4 d^2 \log(2n/d^2)$ of the first m coordinates are in $\{-1, 1\}$ and all other coordinates are 0. The number of such points is larger than

$$\binom{m}{c_4 d^2 \log(2n/d^2)} \geq [\frac{m}{c_4 d^2 \log(2n/d^2)}]^{c_4 d^2 \log(2n/d^2)} = [\frac{\sqrt{n}}{c_4 d \log(2n/d^2)}]^{c_4 d^2 \log(2n/d^2)}.$$

Since n/d^2 is at least a large constant, $\frac{\sqrt{n}}{c_4 d \log(2n/d^2)} \geq (2n/d^2)^{1/4}$ implying that the above lower bound is at least some

$$[2n/d^2]^{c_5 d^2 \log(2n/d^2)} = e^{\Omega(d^2 (\log(2n/d^2))^2)}.$$

This completes the proof of part 1 of the theorem. □

Proof of Theorem 1.3, part 2. By monotonicity $f(n, n, d) \geq f(m, 2m, d)$, where m is the largest integer smaller than $n/2$ so that there is a Hadamard matrix of order m. As is well known $m = (0.5 - o(1))n$.

Let the $2m$ vectors in R^m be d times the rows of a Hadamard matrix of order m and their inverses. The convex hull of these vectors is a centrally symmetric convex polytope of volume exactly $d^m 2^m m^{m/2}/m!$ By Minkowski's Theorem it contains at least

$$d^m m^{m/2}/m! = (1 + o(1)) \frac{1}{\sqrt{2\pi m}} (ed/\sqrt{m})^m = e^{\Omega(n \log(e^2 d^2/n))}$$

lattice points, as needed. □

The proof of Theorem 1.4 is similar to the last proof, where the main difference, besides the choice of the parameters, is the replacement of the Hadamard matrix by random vectors and their inverses.

Proof of Theorem 1.4, part 1. If $t \leq 2c_1 n$ where c_1 is the constant from Theorem 3.1 the result follows by monotonicity from the assertion of part 1 of Theorem 1.3, (which gives in fact a slightly stronger estimate). We thus assume that $t \geq 2c_1 n$. We can also assume that $d\sqrt{\log(et/n)} \leq c_6\sqrt{n}$ for some small constant c_6 since otherwise we use monotonicity and observe that the required estimates stay having the same shape.

Define $m = \sqrt{n}d\sqrt{\log(et/n)}$ and take as before $t/2$ random vectors in $\{-d, d\}^m$ and their inverses. Applying Theorem 3.1 we can fix such vectors whose convex hull contains the set

$$c_2 d(B_\infty^m \cap \sqrt{\log(et/2n)}B_2^m).$$

(It is possible to improve it slightly replacing $(et/2n)$ by $(et/2m)$.) This contains all lattice vectors with any set of $c_7 d^2 \log(et/2n)$ nonzero coordinates in $\{-1, 1\}$ among the first m coordinates. The lower bound obtained here is thus

$$\binom{m}{c_7 d^2 \log(et/2n)} \geq [\frac{\sqrt{n}}{c_7 d\sqrt{\log(et/2n)}}]^{c_7 d^2 \log(et/2n)} = e^{\Omega(d^2 \log(et/n) \log(2n/d^2 \log(et/n)))}$$

as needed. □

Proof of Theorem 1.4, part 2. Here we may assume that $t > 2c_1 n$ and that $d \geq c_8$ for some large constant c_8. Indeed, the case $t \leq 2c_1 n$ follows from the assertion of Theorem 1.3. For d smaller than some absolute constant t has to be exponential in $\Omega(n)$, and then the desired result holds from the trivial estimate $f(n, t, 1) \geq t$ (or $f(n, t, 1) \geq 3^{\log_2 t}$). As before there is a choice of $t/2$ random vectors in $\{-d, d\}^n$ so that the convex hull of these vectors and their inverses contains all lattice vectors in Z^n in which the absolute value of each coordinate is at most $c_9 d$ and the sum of squares of the coordinates is at most $c_{10} d^2 \log(et/2n)$. In particular the convex hull contains all vectors in which each coordinate is an integer with absolute value at most

$$\min\{c_{11} d, c_{11} \frac{\sqrt{d^2 \log(et/2n)}}{\sqrt{n}}\}.$$

This supplies the required estimate. □

4 Open problems

- The results here determine the logarithm of the function $f(n, t, d)$ up to a constant factor for nearly all the admissible range of the parameters, besides the range in which $d^2 \log(et/n)$ is very close to n. It may be interesting to obtain a tight behaviour in this range as well.
- It is also interesting to decide if the methods here can provide any randomized constructions of sparse polynomials with factors that are denser than the examples described in [3].

Acknowledgment: I thank Shubhangi Saraf, Ilya Volkovich and Avi Wigderson for telling me about the problem considered here.

References

[1] N. Alon, T. Lee and A. Shraibman, The cover number of a matrix and its algorithmic applications, Proc. APPROX 2014, 34-47.

[2] N. Alon and J. H. Spencer, *The Probabilistic Method, Fourth Edition*, Wiley, 2016, xiv+375 pp.

[3] V. Bhargava, S. Saraf and I. Volkovich, Deterministic factorization of sparse polynomials with bounded individual degree, J. ACM 67 (2020), no. 2, Art. 8, 28 pp.

[4] S. Barman, Approximating Nash equilibria and dense bipartite subgraphs via an approximate version of Carathéodory's Theorem, Proceedings of the forty-seventh Annual ACM Symposium on Theory of Computing (STOC), pages 361–369, 2015.

[5] O. Guédon, A. E. Litvak and K. Tatarko, Random polytopes obtained by matrices with heavy tailed entries, Commun. Contemp. Math. 22 (2020), no. 4, 1950027, 28 pp.

[6] S. Mendelson, On the geometry of random polytopes, Geometric aspects of functional analysis. Vol. II, 187–198, Lecture Notes in Math., 2266, Springer, (2020)

[7] S. Saraf, I. Volkovich and A. Wigderson, Private communication.

[8] S. Saraf and N. Varadarajan, Integer points in dilated polytopes, arXiv 2510.1648

[9] J. G. Wendel, A problem in geometric probability, Math. Scand. 11 (1962), 109–111.