The purpose of this paper is to elucidate a proof of the following theorem, which basically says that a lattice polytope with many vertices must also have large volume (or, contrariwise, a lattice polytope with small volume cannot have very many vertices).

Theorem 1. *For any lattice polytope P in $\mathbb{R}^d$,*

$$|\operatorname{vert}(P)| \leq c_d \operatorname{Vol}(P)^{\frac{d-1}{d+1}}.$$

The constant c_d depends only on the dimension d.

In comparison, $|\mathbb{Z}^d \cap P| \leq c'_d \operatorname{Vol}(P)$ is the best possible inequality comparing the volume of a lattice polytope to the number of lattice points it contains (see Lemma 2).

As Imre Bárány's notes in his paper *Random points and lattice points in convex bodies* [1], the original proof of G. E. Andrews in 1963 is not easy and while "there are several other proofs available, ... none of them is simple."[1] That's a shame, because this is a very nice theorem: It's tight up to the constant (see Section 4.2), and it exhibits a fundamental difference between the number of lattice points *contained in* a lattice polytope and the number of *vertices* of a lattice polytope.

This note is a retelling of Konyagin and Sevast'yanov's proof of Theorem 1 in [2], with the goal of making the overall strategy more evident and the underlying geometry more apparent. Reading their proof is like being grabbed firmly by the arms and marched steadily and unyieldingly through a formidable concrete hallway until you stumble over the conclusion you were trying to reach. It's there, sure enough, but you have to wonder why you took such an odd journey to get there, and why in the middle of the march you had to pirouette several times, and now that you think about it, why you walked the whole way backwards rather than forwards. That said, their proof *does* have an appealing structure, and if you dismiss the guide, re-plot the journey, and do a bit of interior decorating, it's actually very satisfying.

Let's get to it.

1. THE STRATEGY

In broadest terms, the strategy is simple: Induction on the dimension.

The case $d = 1$ is easy, since any polytope in $\mathbb{R}^1$ has at most two vertices. Now we move up.

Suppose $P \subseteq \mathbb{R}^d$ has m vertices and k facets, which we'll call $F_1, \ldots, F_k$; suppose that F_i has m_i vertices. The hyperplane containing F_i intersects $\mathbb{Z}^d$ in an affine sublattice of dimension $d-1$; let Π_i be its fundamental parallelotope. Theorem 1 applied to F_i in this sublattice tells us that

$$m_i \leq c_{d-1} \Big(\frac{\operatorname{Vol}_{d-1}(F_i)}{\operatorname{Vol}_{d-1}(\Pi_i)} \Big)^{\frac{d-2}{d}}. \tag{$*$}$$

To use induction, we bound m by $\sum_{i=1}^k m_i$ and then use the previous inequality to bound each term in this sum by some function of the $(d-1)$-dimensional volume of the facets. The problem with this is that it's impossible to upper bound the surface measure by *any* function of the volume. As an example, take the usual unit hypercube $\operatorname{conv}(\{0,1\}^d)$ and slide the top facet far away from the bottom facet. (For example, so that the vertices are $\{0,1\}^{d-1} \times \{0\}$ and $\{a, a+1\} \times \{0,1\}^{d-2} \times \{1\}$ for some $a \in \mathbb{Z}$.) The volume of this polytope is always 1, but the surface measure tends toward infinity.

Luckily, there is a fix, called the *reverse isoperimetric inequality*: (see Section 4.1 for a proof[2])

Lemma 1. *For any convex body C in $\mathbb{R}^d$, there is a volume-preserving linear transformation A so that*

$$\operatorname{Vol}_{d-1}\big(\partial A(C)\big) \leq c_d \operatorname{Vol}\big(A(C)\big)^{\frac{d-1}{d}}.$$

Our new strategy is to use the bound

$$m_i \leq c_{d-1} \Big(\frac{\operatorname{Vol}_{d-1}\big(A(F_i)\big)}{\operatorname{Vol}_{d-1}\big(A(\Pi_i)\big)} \Big)^{\frac{d-2}{d}},$$

[1] See the citations after Theorem 13.1 in [1] for references to other proofs.
[2] To focus on the main ideas of the proof, proofs of various lemmas and tangential statements have been moved to Section 4.

which follows from $(*)$ simply because the *ratio* of two volumes is invariant under linear transformation (even though the actual quantity $\mathrm{Vol}_{d-1}\big(A(F_i)\big)$ is likely different). The outline of the proof is then:

1. Calculate $\mathrm{Vol}_{d-1}\big(A(\Pi_i)\big)$ to obtain an upper bound for m_i in terms of $\mathrm{Vol}_{d-1}\big(A(F_i)\big)$.
2. Use the reverse isoperimetric inequality to convert this into a bound on volume.

That's it! Now it's time to follow through.

2. THE CALCULATIONS

2.1. VOLUME BOUND ON FUNDAMENTAL PARALLELOTOPES

Instead of estimating $\mathrm{Vol}_{d-1}\big(A(\Pi_i)\big)$ directly, let's start with the easier task of estimating $\mathrm{Vol}_{d-1}(\Pi_i)$. To do this, we'll introduce the vector h_i, which is a normal vector to Π_i of length $|h_i| = \mathrm{Vol}_{d-1}(\Pi_i)$. The excellently convenient fact about this vector is that it has integer coordinates. There are two ways to see this, one by matrix manipulation and the other geometrically; both can be found in Section 4.3. Either way, now comes the clever bit.

Order the indices so that $|h_1| \leq \cdots \leq |h_k|$ (in other words, so that the volumes of Π_i form a nondecreasing sequence). For any ℓ, we have

$$\mathrm{Vol}\big(\mathrm{conv}(0, h_1, \ldots, h_\ell)\big) \leq \mathrm{Vol}(B^d)|h_\ell|^d,$$

since all the vectors $h_1, \ldots, h_\ell$ are contained inside the ball of radius $|h_\ell|$. (B^d is the unit ball.) But we can also get a lower bound for the volume based only on the fact that it contains at least ℓ integer points: the points $h_1, \ldots, h_\ell$ themselves.

Lemma 2. *If $X \subseteq \mathbb{Z}^d$ does not lie in a single hyperplane, then*

$$\mathrm{Vol}\big(\mathrm{conv}(X)\big) \geq \frac{|X| - d}{d!}.$$

For a proof, see Section 4.4. At this point, we want to write

$$\frac{\ell - d}{d!} \leq \mathrm{Vol}(B^d)|h_\ell|^d$$

and conclude that $|h_\ell| \gtrsim (\ell - d)^{1/d}$. (The symbol $\gtrsim$ means that the inequality is true up to a constant that depends only on the dimension.) However, this is only true if $h_1, \ldots, h_\ell$ span $\mathbb{R}^d$. But if this condition holds, combining this inequality with $(*)$ tells us that

$$m_i^{d/(d-2)}(\ell - d)^{1/d} \lesssim \mathrm{Vol}_{d-1}(F_i).$$

It turns out that we can still bound m even under this restriction on ℓ:

Lemma 3. *If t is the largest index such that $h_1, \ldots, h_t$ is contained in a proper subspace of $\mathbb{R}^d$, then $m \leq \sum_{i=t+1}^k m_i$.*

Proof. Let w be any vector orthogonal to the $(d-1)$-dimensional subspace containing $h_1, \ldots, h_t$. Each vertex of P is contained in a facet whose normal vector is not perpendicular to w (in other words, a facet that is not parallel to w), so

$$m \leq \sum_{\langle h_i, w\rangle \neq 0} m_i \leq \sum_{i=t+1}^k m_i. \qquad \square$$

The last technicality to tidy up is that we actually want a bound on the volume of $A(\Pi_i)$, not Π_i. But this is fairly simple. Let $A^{-\top}$ denote $(A^{-1})^\top = (A^\top)^{-1}$. The vector $A^{-\top}(h_i)$ is perpendicular to $A(\Pi)$, and $|A^{-\top}h_i| = \mathrm{Vol}_{d-1}\big(A(\Pi_i)\big)$. (Verifying this is straightforward linear algebra; see Section 4.5.) Now just repeat everything from above, but with $A(\Pi_i)$ in place of Π_i and $A^{-\top}h_i$ in place of h_i. If r is the largest index so that $A^{-\top}h_1, \ldots, A^{-\top}h_r$ is contained in a hyperplane, then

$$m \leq \sum_{i=r+1}^k m_i$$

and

$$m_i^{d/(d-2)}(\ell - d)^{1/d} \lesssim \mathrm{Vol}_{d-1}\big(A(F_i)\big)$$

for every $\ell \geq r+1$. Now we're ready to use this bound on volume to obtain a bound on m.

2.2. Stringing inequalities

To start, apply Hölder's inequality with $p = (d-2)/d$:

$$m \leq \sum_{i=r+1}^{k} m_i \leq \Big(\sum_{i=r+1}^{k} m_i^{\frac{d}{d-2}} (i-n)^{1/d} \Big)^{\frac{d-2}{d}} \Big(\sum_{i=r+1}^{k} (i-d)^{-\frac{d-2}{2d}} \Big)^{2/d}.$$

The main benefit of this is that the first of the two sums is now exactly what we found in the previous section, so we can bound it by $\Big(\sum_i \mathrm{Vol}_{d-1}\big(A(F_i)\big)\Big)^{(d-2)/d}$. Now we just need to tackle the second sum. Let $\hat{m} := \sum_{i=r+1}^{k} m_i$. Since $m_i \geq 1$ for each i, we have that $k \leq \hat{m}$. Therefore

$$\sum_{i=r+1}^{k} (i-n)^{-\frac{d-2}{2d}} \lesssim \int_{r+1}^{k} (x-d)^{-\frac{d-2}{2d}}\, dx \lesssim (k-d)^{\frac{d+2}{2d}} \leq k^{\frac{d+2}{2d}} \leq \hat{m}^{\frac{d+2}{2d}}.$$

Altogether, we now have that

$$\hat{m} \leq \Big(\sum_{i=r+1}^{k} \mathrm{Vol}_{d-1}\big(A(F_i)\big) \Big)^{\frac{d-2}{n}} \hat{m}^{(d+2)/d}.$$

Combining the powers of $\hat{m}$ and bounding the sum by $\mathrm{Vol}_{d-1}\big(\partial A(P)\big)$, then applying the reverse isoperimetric inequality, we get

$$\hat{m}^{(d^2-d-2)/d} \leq \mathrm{Vol}_{d-1}\big(\partial A(P)\big)^{\frac{d-2}{d}} \lesssim \mathrm{Vol}\big(A(P)\big)^{\frac{(d-1)(d-2)}{d^2}}.$$

Taking each side to the power of $d/(d+1)(d-2)$, and remembering that $m \leq \hat{m}$, finishes the proof. □

3. A stronger result

With a small addition to the proof, we can obtain something stronger. A *tower* or *flag* of a polytope P is a sequence $G_0 \subset G_1 \subset \cdots \subset G_d$ where each G_k is a k-dimensional face of P. We let $T(P)$ denote the total number of towers in P.

Theorem 2. *For any lattice polytope P in $\mathbb{R}^d$,*

$$T(P) \lesssim \mathrm{Vol}(P)^{\frac{d-1}{d+1}}.$$

The towers satisfy the recurrence $T(P) = \sum_{i=1}^{k} T(F_i)$, which means that you can nearly prove Theorem 2 by copying the proof of Theorem 1, replacing m by $T(P)$ and m_i by $T(F_i)$. The only part that falters is Lemma 3. It's simply never true that $T(P) \leq \sum_{i=r+1}^{k} T(F_i)$. However, throw in a constant and everything is fine:

Lemma 4. *If t is the largest index such that $h_1, \ldots, h_t$ is contained in a proper subspace of $\mathbb{R}^d$, then $\sum_{i=t+1}^{k} T(F_i) \geq \frac{1}{d} T(P)$.*

Proof. As before, let w be any vector orthogonal to the $(d-1)$-dimensional subspace containing $h_1, \ldots, h_t$. We will show that

$$\sum_{\langle h_i, w\rangle \neq 0} T(F_i) \geq \frac{1}{d} T(P).$$

The left-hand sum is equal to the number of towers of P that do not include a face that is parallel to w. (A face is *parallel* to w if its affine span contains a translate of w.) Given a vertex v, let $\mathcal{T}_v(P)$ denote the set of towers of P whose 0-dimensional face is v, and let $\mathcal{T}_v^w(P)$ denote the subset of towers in $T_v^w(P)$ which do not include a face parallel to w. We will prove that $|\mathcal{T}_v^w(P)| \geq \frac{1}{d}|\mathcal{T}_v(P)|$. Since $T(P) = \sum_v |\mathcal{T}_v(P)|$, that suffices to prove the lemma.

If G_k is a k-dimensional face not parallel to w, then it is contained in at least $d-k$ faces of dimension $k+1$ and at most one of them is parallel to w. Using this fact starting from a single vertex, we have

$$|\mathcal{T}_v^w(P)| \geq \frac{d-1}{d}\frac{d-2}{d-1}\cdots\frac{2}{3}\frac{1}{2}|\mathcal{T}_v(P)| = \frac{1}{d}|\mathcal{T}_v(P)|. \qquad \square$$

Theorem 2 also implies a version of Theorem 1 for faces of all dimension:

Theorem 3. *There exists a constant c_d so that for every lattice polytope P in $\mathbb{R}^d$, the number of k-dimensional faces of P is at most $c_d \operatorname{Vol}(P)^{\frac{d-1}{d+1}}$.*

4. THE REST OF THE PROOFS

4.1. REVERSE ISOPERIMETRIC INEQUALITY

John's theorem quickly proves this theorem, though not with an optimal constant.

Choose A so that the largest-volume ellipsoid contained inside $A(C)$ is a ball B. Since both sides of the inequality are linear under scaling by a constant factor, we may assume that $\mathrm{Vol}\big(A(C)\big) = 1$. It suffices therefore to show that $\mathrm{Vol}_{d-1}\big(\partial A(C)\big)$ is bounded by a constant. This follows from John's theorem, which implies that $A(C) \subseteq d \cdot B \subseteq d \cdot B^d$, where B^d is the unit ball. So we can take $c_d = d^{d-1}\,\mathrm{Vol}_{d-1}(\partial B)$.

4.2. Theorem 1 is tight

The example is surprisingly simple. Let X be the set of points

$$X = \big\{(x, \|x\|^2) \in \mathbb{Z}^d \,:\, x \in \{-n, -n+1, \dots, n-1, n\}^{d-1}\big\}.$$

We will take $P = \mathrm{conv}(X)$.

Since $x \mapsto \|x\|^2$ is a convex function, X is a set of points in convex position, so $P = \mathrm{conv}(X)$ has exactly $|X| = (2n+1)^{d-1}$ vertices. The exact volume of P might be difficult to calculate, but P certainly contains the pyramid with apex at the origin and whose base has vertices $\{\pm n\}^{d-1} \times \{dn^2\}$. The volume of this cone is

$$\frac{1}{d}(2n)^{d-1} dn^2 = 2^{d-1} n^{d+1}.$$

Thus

$$\mathrm{Vol}(P)^{\frac{d-1}{d+1}} \geq C_d\, |\mathrm{vert}(P)|$$

for a suitable choice of constant C_d.

4.3. NORMAL VECTOR TO THE PARALLELOTOPE

Proposition 5. *Given $d-1$ vectors $v_1, \dots, v_{d-1} \in \mathbb{Z}^d$, either vector orthogonal to their span and whose length is equal to the $(d-1)$-dimensional volume of the parallelotope generated by $v_1, \dots, v_{d-1}$ is a member of $\mathbb{Z}^d$.*

We prove this in two ways.

THE MATRIX METHOD

Arrange the vectors $v_1, \dots, v_{d-1}$ as columns in a matrix M, and define h by its coordinates: h_i is the determinant of M after deleting the ith row. This is a general way of producing a vector orthogonal to $d-1$ others. To verify that h is orthogonal to v_i, we can use the cofactor formula for the determinant to see that $\langle h, v_i\rangle$ is equal to the determinant of the matrix with columns $v_1, \dots, v_{d-1}, v_i$, which is 0, since 1 column is repeated.

If $v_1, \dots, v_{d-1} \in \mathbb{Z}^d$, then by definition $h \in \mathbb{Z}^d$. We need to calculate $|h|$. Let B be the $(d-1)$-dimensional volume of the parallelotope generated by $v_1, \dots, v_{d-1}$. On the one hand, $|h|^2 = h_1^2 + \cdots + h_d^2$. Also, since h is orthogonal to $v_1, \dots, v_{d-1}$, we know that $\det(h, v_1, \dots, v_{d-1}) = |h| \cdot B$. On the other hand, direct calculation using the cofactor formula shows that $\det(h, v_1, \dots, v_{d-1}) = h_1^2 + \cdots + h_d^2$. We conclude that $|h|^2 = |h| \cdot B$, so $|h| = B$, as desired.

THE GEOMETRIC METHOD

If $v \in \mathbb{Z}^d$ and the set of coordinates of v has greatest common divisor 1 (in which case v is called *primitive*), then the projection of $\mathbb{Z}^d$ onto $\mathrm{span}(v)$ is the set of points $\frac{k}{|v|}v$ with $k \in \mathbb{Z}$. (This is because the vector w projects onto the point $\frac{\langle w,v\rangle}{|v|}v$, and if v is primitive, then there is a solution to $\langle w, v\rangle = k$ for every $k \in \mathbb{Z}$.) If $v \notin \mathbb{Z}^d$, then the projection of $\mathbb{Z}^d$ onto $\mathrm{span}(v)$ is dense.

Let h' be a unit vector orthogonal to $v_1, \dots, v_{d-1}$. The projection of a lattice onto the orthogonal complement of any sublattice is also a lattice, so the projection of $\mathbb{Z}^d$ onto $\operatorname{span}(h')$ is a sublattice. Let B be the $(d-1)$-dimensional volume of the parallelotope generated by $v_1, \dots, v_{d-1}$, let B_f be the volume of a fundamental parallelotope in $\operatorname{span}(v_1, \dots, v_{d-1})$, and let w be a vector that projects to a minimal nonzero vector $\rho(w)$ in $\operatorname{span}(h')$. Then $v_1, \dots, v_{d-1}, w$ generate a fundamental parallelotope in $\mathbb{Z}^d$. The volume of this parallelotope is therefore 1, which means that the orthogonal component of w is $1/B_f$. In other words, $|\rho(w)| = 1/B_f$.

Therefore the projection of $\mathbb{Z}^d$ onto $\operatorname{span}(h')$ is $\frac{k}{B_f}h'$. Using the reasoning from the first paragraph, we conclude that $B_f \cdot h'$ is a lattice vector. Since B_f divides B, we also have that $h := B \cdot h'$ is a lattice vector.

4.4. VOLUME VS. TOTAL LATTICE POINTS

Here is the fundamental fact that connects volume to lattice points:

Lemma 6. *The volume of a lattice simplex in $\mathbb{R}^d$ is at least $1/d!$.*

Proof. By elementary calculus, the volume of a cone in $\mathbb{R}^d$ with base $(d-1)$-volume B and height h is hB/d. Suppose that S is a simplex, and let $v_1, \dots, v_d$ be the vectors corresponding to the edges emanating from one of its vertices. Induction shows that the volume of S is exactly equal to $1/d!$ times the volume of the parallelotope determined by $v_1, \dots, v_d$. That volume is given by $|\det(v_1, \dots, v_d)|$. If S is a lattice simplex, then $v_1, \dots, v_d$ are integer vectors. Since $\det(v_1, \dots, v_d) \neq 0$, we have

$$\operatorname{Vol}(S) \geq \frac{|\det(v_1, \dots, v_d)|}{d!} \geq \frac{1}{d!}. \qquad \square$$

One way to prove Lemma 2 is to actually prove the stronger statement that any lattice polytope can be decomposed into at least $|X| - d$ lattice simplices. Lemma 6 then implies Lemma 2. The proof of this stronger statement goes by induction on $|X|$. Intuitively, it's pretty clear: remove one vertex v from X and find a lattice simplex in $\operatorname{conv}(X) \setminus \operatorname{conv}(X \setminus v)$; then repeat. Writing it out in full is somewhat tedious, so I'll leave it for you to think about.

There are many examples that show that Lemma 2 is tight (up to the constant). One simple example is taking $X = \{0, 1, 2, \dots, n\}^{d-1} \times \{0, 1\}$, which has $2(n+1)^{d-1}$ lattice points and a convex hull with volume n^{d-1}.

4.5. MISCELLANEOUS LINEAR ALGEBRA

Lemma 7. *If $u, v \in \mathbb{R}^d$ are orthogonal and A is any linear transformation, then $A^{-\top}v$ is orthogonal to Au.*

Proof. Calculate: $\langle A^{-\top}v, Au\rangle = \langle v, A^{-1}Au\rangle = \langle v, u\rangle = 0$. $\square$

Lemma 8. *Given $v_1, \dots, v_{d-1} \in \mathbb{R}^d$, let Q be the parallelotope they generate, and let h be a vector orthogonal to $v_1, \dots, v_{d-1}$ with length $|h| = \operatorname{Vol}_{d-1}(Q)$. If A is a volume-preserving linear transformation, then $A^{-\top}h$ is orthogonal to $A(Q)$ and has length $|A^{-\top}h| = \operatorname{Vol}_{d-1}\big(A(Q)\big)$.*

Proof. Let R be the parallelotope generated by $v_1, \dots, v_{d-1}, h$. Since A is volume-preserving and h is orthogonal to Q,

$$\operatorname{Vol}\big(A(R)\big) = \operatorname{Vol}(R) = \operatorname{Vol}_{d-1}(Q)^2.$$

On the other hand, the volume of $A(R)$ is the volume of the base times the length of the orthogonal component of Ah:

$$\operatorname{Vol}\big(A(R)\big) = \frac{\langle Ah, A^{-\top}h\rangle}{|A^{-\top}h|}\operatorname{Vol}_{d-1}(Q) = \frac{|h|^2}{|A^{-\top}h|}\operatorname{Vol}_{d-1}(Q) = \frac{\operatorname{Vol}_{d-1}(Q)^3}{|A^{-\top}h|}.$$

Chain the inequalities and cancel terms to get $|A^{-\top}h| = \operatorname{Vol}_{d-1}(Q)$. $\square$

References

[1] Imre Bárány, *Random points and lattice points in convex bodies*, Bulletin of the American Mathematical Society **45** (2008), 339–365.

[2] V. Konyagin S. and A. Sevast'yanov K. *A bound, in terms of its volume, for the number of vertices of a convex polyhedron when the vertices have integer coordinates*, Functional Analysis and its Applications **18** (1984), 11–13.