Lattice Point Geometry: Applications and Generalisations of Theorems of Pick and Minkowski

Charles Spruce, Diogo Santos, Jakub Bober, Jason Xu, Dylan Crook

June 30, 2021

Contents

1 Introduction **2**

2 Preliminary results in Lattice Point Geometry **3**

3 Pick's Theorem **7**
3.1 Proof by additivity of polygons 9
3.2 Proof using Euler's Formula 13
3.3 Interesting Corollaries 15

4 Pick-esque theorem in higher dimensions **16**
4.1 Reeve tetrahedron: a counterexample in R^3 16
4.2 Reeve's formula for volume of convex polyhedra 16
4.3 Generalization in R^n 19

5 Minkowski's Theorem **19**
5.1 Applications 20
5.1.1 Fermat's two-square theorem 21
5.1.2 Lagrange's four-square theorem 22
5.1.3 Dirichlet's theorem 24

6 Ehrhart Polynomials and Triangulation **25**
6.1 Definitions 25
6.2 Ehrhart Polynomials of Simple Polygons in R^2 26
6.3 The d-cube 26
6.4 The standard d-simplex 27
6.5 Triangulation 27

References **30**

1 Introduction

Lattices can be loosely described as a discrete analogy to a vector space; a disconnected subgroup of R^n, in the sense that the points of the lattice are isolated in some regular way. Their study dates back at least to the 18^{th} century, however it could be argued that the realisation of their usefulness did not truly dawn until a variety of theorems relating the volumes of geometric objects in Euclidean space, and the lattice points which they bound, were discovered and then connected to other branches of mathematics. It is likely from these developments that the topic of lattice point geometry grew, and it has gone on to prove itself useful in a variety of mathematical fields, ranging from those with an algebraic flavour (e.g. the theory of modular forms, algebraic number theory) and more applied mathematical subfields, such as cryptography, where it has seen use since the early 1980s, starting with work by Lenstra, Lenstra and Lovasz, or crystallography, where mathematical lattices can be helpful in describing the structure of regular crystal lattices.

The objective of this paper is to serve as an introductory exploration of the field of lattice point geometry, wherein we will aim to develop a sufficient toolkit to prove some of the most well-known results, some of their corollaries so as to highlight their general utility, and some of the ways that mathematicians have attempted to extend these results into higher dimensions. The first of these results will be Pick's theorem, which allows one to compute the area of a lattice polygon from the data of the lattice points it contains; the second will be Minkowski's theorem, which conversely allows us to obtain information on the lattice points contained within a symmetric, convex body given its volume.

In section 2, we will lay the groundwork for the proceeding sections. It largely consists of the various definitions which will be used to later state the theorems, and contains some lemmas and theorems which will later prove necessary for some of the larger proofs - in particular, the computations of the volumes of fundamental parallelopipeds, and primitive triangles, in n-dimensional and 2-dimensional lattices respectively.

Section 3 provides two proofs of Pick's theorem. The first of these by way of proving that it holds for a general lattice triangle, that the property is maintained for polygons which share sides in common, and that any lattice polygon can be triangulated. The second of these relies upon the fact that any lattice polygon yields a primitive triangulation, the result that any primitive lattice triangle has a constant area, and a combinatorial result utilising Euler's formula. We proceed by discussing some corollaries of Pick's theorem, namely demonstrating a powerful result on the existence of regular lattice n-gons for various positive integer values of n.

In section 4, we are motivated by the question of whether there is a generalisation of Pick's theorem which holds for integral polyhedra in three dimensions. The discussion turns to the example provided by Reeve, that a primitive tetrahedron in R^3 can have arbitrarily large volume, and hence it is impossible to compute the volume of a polyhedron given only the data of integral points it contains. However, all hope for a generalisation is not lost; we explore the formula discovered by Reeve which may be used to compute the volume of an integral polyhedron given data on secondary lattice points, to be defined later. We prove most parts of this theorem, and introduce its generalisation in R^n.

For section 5, we give a proof of Minkowski's theorem, following the style of another proof[8]. We then proceed with a short foray into number theory and explore some theorems for which, whilst earlier and more elementary proofs are known, there exists a simple proof by way of Minkowski's theorem. We chose to highlight and provide Fermat's two-square theorem, Lagrange's four-square theorem, and Dirichlet's theorem on Diophantine approximations of real numbers, to give a broad sense of the wide applicability of Minkowski's proof.

Lastly, we explore means of counting the lattice points contained in general higher-dimensional polytopes in section 6, and provide some results for basic polytopes one might encounter in n-dimensional Euclidean space, such as the generalisations of cubes and simplices. We look to generalise the notion of triangulation, looking into and making sense of simplicial decompositions in arbitrary dimensions.

2 Preliminary results in Lattice Point Geometry

In this chapter, we outline some basic definitions and results pertaining to lattice point geometry.

Definition 2.1 (Lattice)**.** An n-dimensional *lattice* $\Lambda \subset R^n$ with respect to some *basis* $\mathcal{B}$ of m linearly independent vectors in R^n is defined:

$$\Lambda := \{\sum_{i=1}^{m} \lambda_i b_i : \lambda_i \in Z, b_i \in \mathcal{B}\}$$

We sometimes denote Λ by $\Lambda(\mathcal{B})$, and we say m is the *rank* of $\Lambda(\mathcal{B})$. It is said to be a *full rank lattice* if $m = n$. Equivalently, interpreting the basis $\mathcal{B}$ of a lattice Λ as an $n \times m$ matrix B whose columns are the elements of $\mathcal{B}$, we can define Λ in the following way:

$$\Lambda := \{Bx : x \in Z^m\}$$

A *lattice point* is an element of a lattice.

Definition 2.2 (Fundamental parallelopiped)**.** The *fundamental parallelopiped* $P(\mathcal{B})$ is given by:

$$P(\mathcal{B}) := \prod_{i=1}^{m} [0, b_i), \ b_i \in \mathcal{B}$$

where $[a, b)$ denotes the set $\{(1-\lambda)a + \lambda b : \lambda \in [0, 1)\} \subset R^n$.
Equivalently, interpreting $\mathcal{B}$ as a matrix as before, we can define $P(\mathcal{B})$ in the following way:

$$P(\mathcal{B}) := \{By : y \in [0, 1)^m\}$$

Observe that the basis vectors $\mathcal{B}$ form the edges of $P(\mathcal{B})$ which meet at the origin. Further, notice that P is not closed; its construction lends itself to the expression:

$$\text{Span}(\mathcal{B}) = \bigsqcup_{a \in \Lambda(\mathcal{B})} (P + a)$$

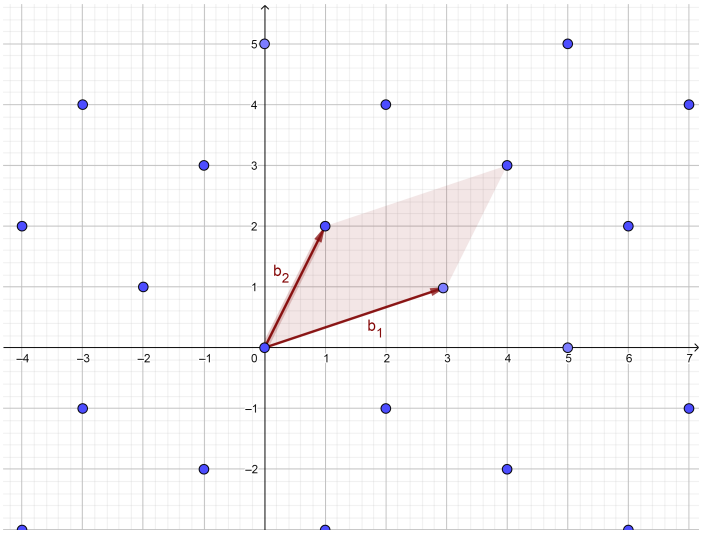

Figure 1: A lattice $\Lambda(\{b_1, b_2\})$ generated by vectors $b_1 = (3, 1)^T$ and $b_2 = (1, 2)^T$. The red shape represents a fundamental parallelogram of Λ.

We will often choose to simply refer to the fundamental parallelopiped of a lattice by P, where the meaning is clear.

Definition 2.3 (Determinant of a lattice)**.** The *determinant* of a lattice $\Lambda(\mathcal{B})$ is the volume of the fundamental parallelopiped $P(\mathcal{B})$. We denote it by $d(\Lambda) = \text{Vol}(P(\mathcal{B}))$.

We proceed by proving some basic results which build up to a proof of one of the preliminaries to Pick's theorem, wherein we show that the area of a primitive lattice triangle in a 2 dimensional lattice has a fixed volume. These proofs will largely follow the structure of those presented in the introductory chapters to the course *Lattice Algorithms and Applications*[9], and in the paper *Lattice Point Geometry: Pick's Theorem and Minkowski's Theorem*[3].

Proposition 2.1 (Determinant of a Full Rank Lattice)**.** Suppose a full-rank lattice $\Lambda(\mathcal{B}) \subset R^n$ has fundamental paralellopiped $P(\mathcal{B})$. Then $d(\Lambda) = |\det(B)|$.

Proof. $\mathcal{B}$ is a linearly independent set of vectors, and hence we can use the Gram-Schmidt process to yield the factorisation:

$$B = QR$$

where Q is the matrix whose columns q_i are the components of b_i orthogonal to $\{b_1, ..., b_{i-1}\}$, and R is an upper triangular matrix whose diagonal entries are all 1.

Using the well-known result that the volume of an n-dimensional parallelopiped is given by the product of the lengths of the mutually orthogonal projections of n of its edges which meet at a vertex, we have that:

$$d(\Lambda) = \prod_{i=1}^{n} ||q_i||$$

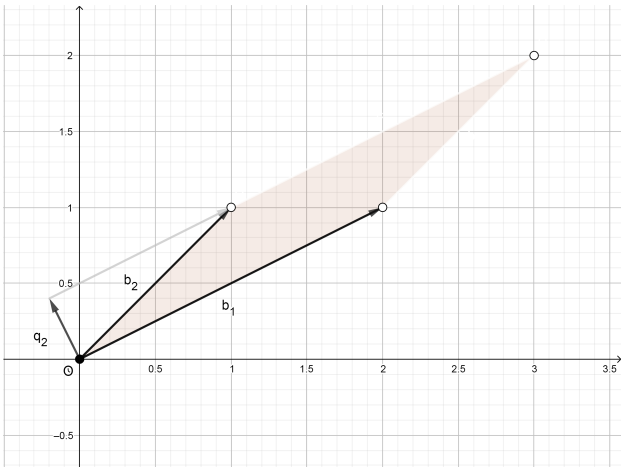

Figure 2: The orthogonalisation of the basis $\{b_1, b_2\}$, giving $\{b_1, q_2\}$

We proceed with the computation:

$$\det(B^T B) = \det(R^T Q^T Q R)$$

Since R has only 1s along the diagonal and is upper triangular, $\det(R) = \det(R^T) = 1$, and hence, using the multiplicative property of the determinant, we see:

$$\det(B^T B) = \det(Q^T Q)$$

The matrix Q is orthogonal, so we have that $Q^T Q$ must be diagonal, with i^{th} diagonal entry $[Q^T Q]_i = \langle q_i, q_i \rangle$. We obtain:

$$\det(Q^T Q) = \prod_{i=1}^{n} \langle q_i, q_i \rangle$$

Furthermore, we note:

$$\prod_{i=1}^{n} \langle q_{i,\,i} \rangle = \prod_{i=1}^{n} ||q_i||^2$$

It immediately follows that:

$$d(\Lambda)^2 = \det(B^T B)$$

And finally, as $\det(B^T B) = (\det(B))^2$, we yield the result:

$$d(\Lambda) = |\det(B)|$$

□

Proposition 2.2 (Unimodularity of the basis-change matrix for equivalent bases for a lattice)**.** Let $\mathcal{B}$ and $\mathcal{B}'$ be two bases. Then $\Lambda(\mathcal{B}) = \Lambda(\mathcal{B}')$ if and only if there exists a square matrix with integer entries and unitary determinant U such that $B = B'U$. (Such a matrix is called *unimodular*.)

Proof. Suppose $B = B'U$ for some unimodular U. Since U is unimodular, it can be shown that so is U^{-1}, hence $B' = BU^{-1}$. It follows that any vector in $\Lambda(\mathcal{B})$ can be written as an element of the integral span of $\mathcal{B}'$, and vice versa. Hence $\Lambda(\mathcal{B}) \subset \Lambda(\mathcal{B}')$ and $\Lambda(\mathcal{B}') \subset \Lambda(\mathcal{B})$, so indeed $\Lambda(\mathcal{B}) = \Lambda(\mathcal{B}')$.

Conversely, assume $\mathcal{B}$ and $\mathcal{B}'$ generate the same lattice Λ. Then we are able to write each element of $\mathcal{B}$ as an element of the integral span of $\mathcal{B}'$, and vice versa. It follows that there exist integral square matrices X and Y such that $B' = BX, B = B'Y$. We see $B = BXY$, and hence, as $\mathcal{B}$ is linearly independent, we have that $B(I - XY) = 0 \iff I = XY$. Hence, $\det(X)\det(Y) = 1$. Since $\det(X), \det(Y) \in Z$, we see that $\det(Y) = \pm 1$. □

Many times throughout the paper, we will refer to polygons, and their generalisations to higher dimensions, polytopes. We define these, and prove an initial result in R^2 showing that there is a fixed relationship between the determinant of a lattice of rank 2, and a triangle spanned by its basis.

Definition 2.4 (Polytope)**.** We define a polytope in terms of its facets, which themselves are defined recursively. A 0 dimensional facet is a point, referred to as a vertex. An n-dimensional facet is a closed region of R^n which is bounded by $(n-1)$-dimensional facets. An n-dimensional polytope is defined to be a closed region of R^n which is bounded by $(n-1)$-dimensional facets, and is such that its facets of dimension m are each bounded by facets of dimension $(m-1)$. Notice that each facet is itself a polytope.

Intuitively, polytopes are the generalisations of lines in R, polygons in R^2, and polyhedra in R^3.

A *lattice polytope* with respect to a lattice Λ is a polytope which vertices are all lattice points. We say that a lattice polytope is *primitive* with respect to a lattice Λ if it does not contain any lattice point of Λ in its interior. If a polytope is referred to as primitive without reference to a specific lattice, it is to be assumed that the lattice with respect to which it is primitive is taken to have the standard basis (i.e. all vertices are integral).

Lemma 2.3. The closure of the fundamental parallelopiped spanned by n linearly independent vectors $b_1, ..., b_n$ is primitive with respect to Λ if and only if $\mathcal{B} = \{b_1, ..., b_n\}$ is a basis for Λ.

Proof. Let $\overline{P}$ be the closure of the fundamental parallelopiped spanned by $\mathcal{B}$, and suppose that $\overline{P}$ is primitive. Since $\mathcal{B}$ is a linearly independent set of n vectors, it forms a basis for R^n. Let $v \in \Lambda$. Then we can choose $\lambda_1, ..., \lambda_n \in R$ such that $v = \sum_{i=1}^{n} \lambda_i b_i$. Let $\lambda_i = \lfloor \lambda_i \rfloor + \lambda_i'$. Let $v' = \sum_{i=1}^{n} \lambda_i' b_i$. Then $v' = v - \sum_{i=1}^{n} \lfloor \lambda_i \rfloor b_i$. Notice that $v' \in P$, and $v' \in \Lambda$. It follows that v' must be a vertex of $\overline{P}$ and since $\lambda_i' \in [0, 1)$, we have that $v' = 0$. It follows that $\lambda_i' = 0$, and hence $\lambda_i \in Z$. Since $v \in \Lambda$ was arbitrary, we have that $\mathcal{B}$ is a basis for Λ.

Now suppose that $\mathcal{B} = \{b_1, ..., b_n\}$ is a basis of Λ. Then $\forall y \in \Lambda, \exists x \in Z^n$ such that $y = Bx$. Let $\overline{P}$ be the closure of the fundamental parallelopiped of $\mathcal{B}$. Suppose $y \in \overline{P}$. Since $\overline{P}$ is spanned by $\mathcal{B}$, we can write $y = Bz$ where $z \in [0, 1]^n$. It follows that the entries of z are either 0 or 1, and hence y is a vertex of $\overline{P}$, and so $\overline{P}$ is primitive in Λ. □

Lemma 2.4. If T is a primitive triangle in the lattice $\Lambda \subset R^2$ with vertices $x, y, z \in \Lambda$, then the vectors $u = y - x$, $v = z - x$ form a basis of Λ.

Proof. Clearly, u and v are linearly independent. Let $\overline{P}$ denote the closure of the fundamental parallelogram generated by u and v. Notice that $T \subset \overline{P} + x$, and that $\overline{P} + x$ is primitive if and only if $\overline{P}$ is. Let ρ denote the rotation through π about the midpoint of the edge with vertices y and z on either end. Suppose for a contradiction that there is a point w of Λ in $(\overline{P} + x) \setminus T$, and w is not a vertex of $\overline{P} + x$. Then $w' = \rho(w) \in T$, and w' is not a vertex of T, a contradiction as T is primitive. Hence $\overline{P} + x$ is a primitive parallelogram, and so is $\overline{P}$. It follows from the previous lemma that $\mathcal{B} = \{u, v\}$ is a basis for Λ.

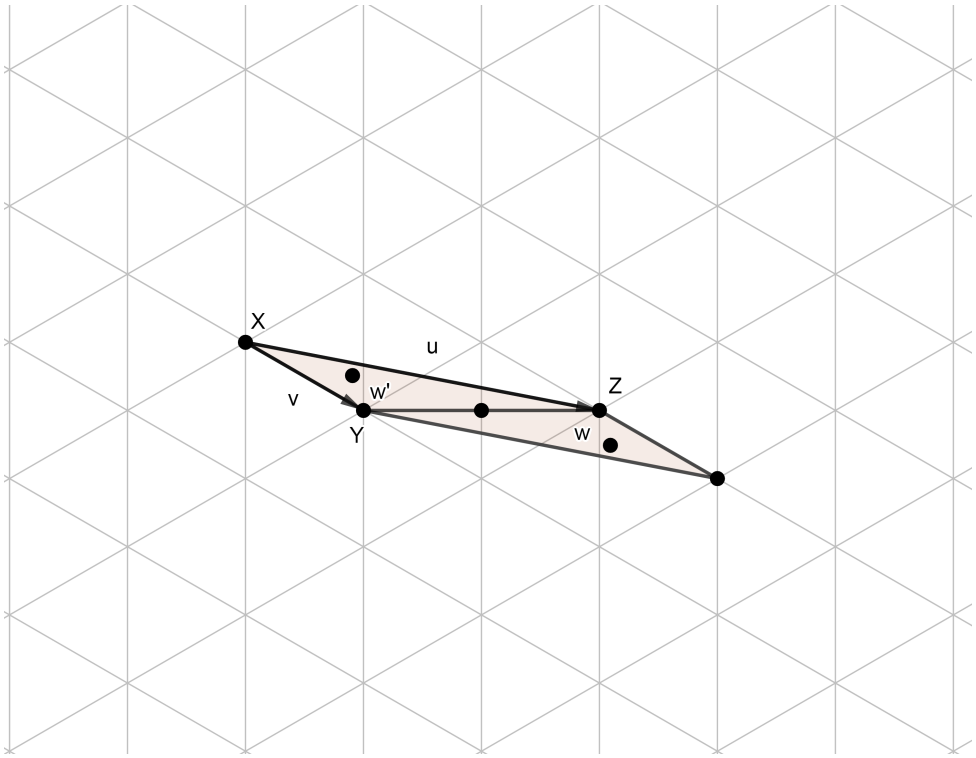

Figure 3: Visual proof that a primitive lattice triangle extends to a primitive lattice parallelogram.

□

Proposition 2.5. If T is a triangle primitive with respect to a full rank lattice $\Lambda \subset R^2$, then the area of T is $\frac{1}{2}A(P)$, where P is the fundamental parallelogram of Λ.

Proof. It follows from the previous lemmas that we can take two vectors u and v corresponding to edges of T as a basis for Λ, $\mathcal{B} = \{u, v\}$. It follows from the unimodularity of the change of basis matrices for Λ that any primitive parallelogram generated by a basis of Λ has the same area. Since T has the same base and height as the parallelogram it generates, $A(T) = \frac{1}{2}A(P)$.

□

Lemma 2.6. All primitive triangles have area $\frac{1}{2}$.

Proof. Given the previous theorem, we need only show that a primitive parallelogram in Z^2 has area 1. Taking $\mathcal{B} = \{(1,0),(0,1)\}$ as our basis, we get that the corresponding matrix $B = I$. $\det(I) = 1$, so we are done. □

Note: For the remainder of this paper, when we refer to lattices and lattice polygons, we are referring to the lattice generated by $(1,0)$ and $(0,1)$. The points in this lattice are sometimes called *integral points*.

3 Pick's Theorem

The main concentration of the report is *Pick's Theorem*, invented by an Austrian mathematician, Georg Alexander Pick, in 1899. The statement of the theorem is fairly simple:

Theorem 3.1 (Pick's Theorem)**.** Consider a simple lattice polygon P. Then the area of P can be expressed as:

$$A(P) = I + \frac{B}{2} - 1$$

Where I and B are the numbers of lattice points inside and on the boundary of P respectively. These are sometimes called *interior points* and *boundary points*.

Note: here when we refer to a *simple lattice polygon*, we mean a simple polygon (2D-shape with straight edges which doesn't intersect itself or have any holes) whose vertices are lattice points.

Let us demonstrate the theorem. Consider the green pentagon in Figure 4:

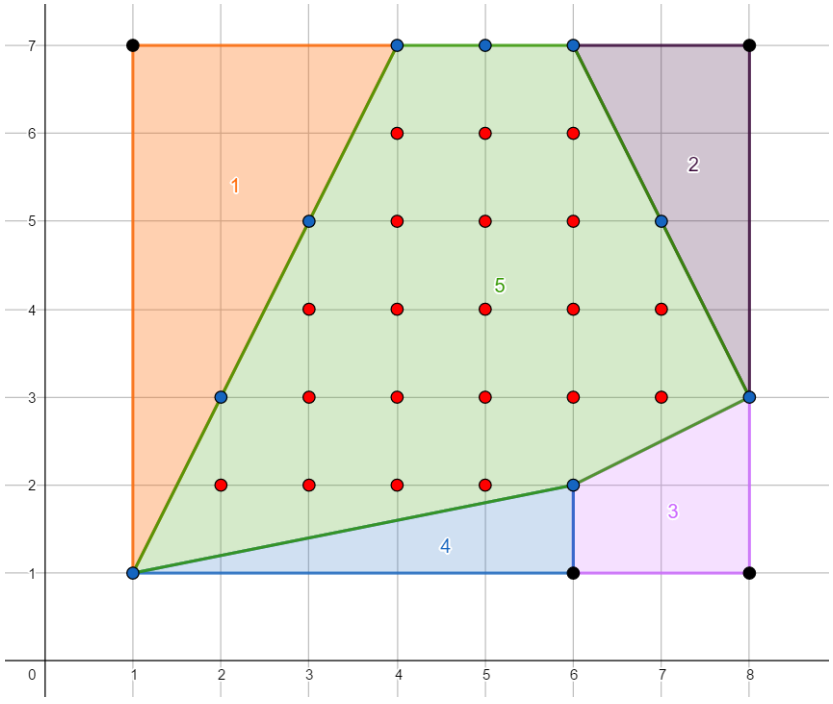

Figure 4: Pentagon 5 (green) with highlighted 20 interior points (red) and 9 boundary points (blue). Together with triangles 1 (orange), 2 (black) and 4 (blue) and trapezium 3 (purple) creates a 6 by 7 rectangle.

Using basic school mathematics we can calculate the area of the pentagon.
For the rest of the document, let us introduce the notation for areas of 2-dimensional shapes: let $A(x)$ denote the area of the polygon x.

1. Calculate the area of the 6 by 7 rectangle consisting of all the polygons in Figure 4. Its area is obviously 42.
2. Calculate the area of the triangles and the trapezium: $A(1) = \frac{1}{2} \cdot 3 \cdot 6 = 9$, $A(2) = \frac{1}{2} \cdot 2 \cdot 4 = 4$, $A(3) = \frac{1}{2} \cdot (1 + 2) \cdot 2 = 3$, $A(4) = \frac{1}{2} \cdot 1 \cdot 5 = \frac{5}{2}$.
3. Subtract the sum of the areas from the area of the big rectangle to get the area of the green pentagon: $A(5) = 42 - (9 + 4 + 3 + \frac{5}{2}) = 23\frac{1}{2}$.

Now let us calculate $A(5)$ using Pick's theorem. The green pentagon has 20 interior points and 9 boundary points, so substituting $I = 20$ and $B = 9$ into the formula from the theorem we get $A(5) = 20 + \frac{9}{2} - 1 = 23\frac{1}{2}$, which is indeed a correct result.

There are many different ways to prove Pick's theorem. Here, we will present two that we find the most interesting:

3.1 Proof by additivity of polygons

Proof. This proof combines the ideas of additivity of polygons[6], and triangulation of polygons[1]. The proof consists of several steps: firstly, we must confirm the additive property, that if two polygons share a side, and Pick's Theorem holds for each polygon, then it also holds for the polygon consisting of their composition removing the shared side. Then, we check the theorem holds for rectangles, and subsequently for right-angled triangles. We use this result to show it holds for any triangle, and from here we need only prove any polygon can be split entirely into triangles by adding edges inside it joining boundary points, or rather, triangulated. Then we are done, as we use the additive property to confirm Pick's Theorem holds for the polygon.

Proving our additive property is easy. Choose two polygons P_1 and P_2 with I_1 and I_2 interior points respectively and B_1 and B_2 boundary points respectively. We also assume that these polygons share one or more edges, i.e. removing these edges gives their composition P, a new polygon, and these edges contain k boundary points (not including vertices of P). We assume Pick's theorem holds for P_1 and P_2, and show it also must hold for P.

Then P has $I = I_1 + I_2 + k$ interior points, and $B = B_1 + B_2 - 2k - 2$ boundary points. So $I + \frac{B}{2} - 1 = I_1 + I_2 + k + \frac{B_1+B_2}{2} - k - 1 - 1 = \left(I_1 + \frac{B_1}{2} - 1\right) + \left(I_2 + \frac{B_2}{2} - 1\right)$ which is the sum of the areas of P_1 and P_2, so Pick's Theorem holds for P.

We prove Pick's Theorem for an m by n rectangle. We easily establish its number of interior points is $(m-1)(n-1)$ and number of boundary points is $2(m+1) + 2(n-1) = 2(m+n)$. Hence we have:

$$I + \frac{B}{2} - 1 = (m-1)(n-1) + (m+n) - 1 = mn - m - n + 1 + m + n - 1 = mn$$

Correctly giving us the area of the rectangle.

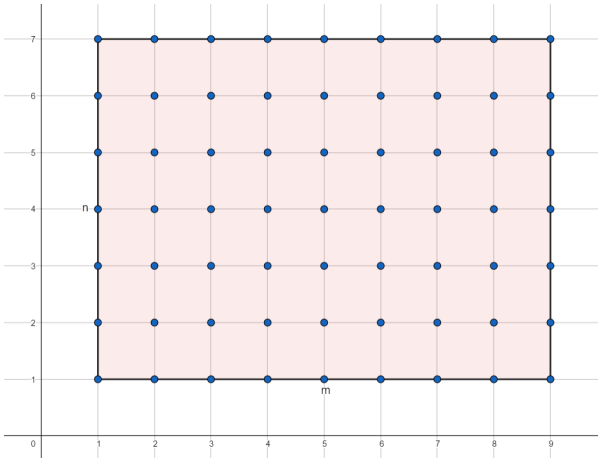

Figure 5: An m by n rectangle on the integer lattice

Now see Figure 6 for our next shape, a right-angled triangle with non-hypotenuse edges of length m and n. This is our rectangle from Figure 5 split in half down its diagonal.

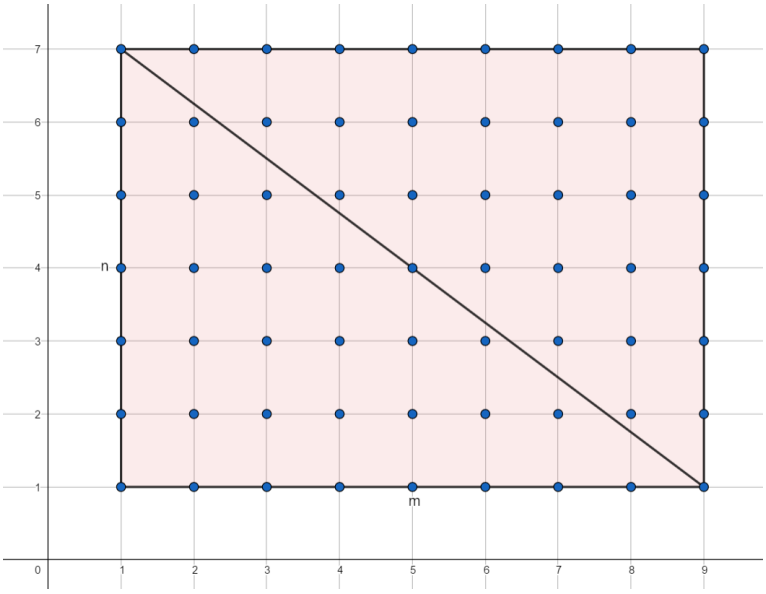

Figure 6: A rectangle split in half down the diagonal

We assume that the hypotenuse of the triangle contains k points, not including our vertices. We have the number of interior points is $\frac{1}{2}[(m-1)(n-1)-k]$ and our number of boundary points is $m+n+1+k$. The we arrive at this number of interior points because after subtracting the points on the hypotenuse, we can see both the upper and lower right-angled triangles contain the same number of points, so we divide by 2. Substituting these values into our Pick's Theorem expression we have:

$$\frac{1}{2}[(m-1)(n-1)-k]+\frac{1}{2}[m+n+1+k]-1=\frac{1}{2}[mn-m-n+m+n]=\frac{1}{2}mn$$

giving us the area we want.

Now we move on to our proof for a generalised triangle. Figure 7 shows how any triangle with integral-points as vertices can be made interior to some rectangle so that it partitions said rectangle into 3 right-angled triangles and itself, the (potentially) not right-angled triangle. We do this by drawing lines from our left/right/top/bottom-most vertices of our triangle T to make the rectangle. If there exists a point that is not top/bottom/left/right-most, we can create this rectangle using 3 right angled triangles and a further rectangle, see Figure 6. The proof is identical to the first case, which we discuss below.

Note: if one side of T is parallel to the x or y axis, then we need only 2 other right-angled triangles to make a rectangle, and if two sides are parallel, then it is right-angled and we refer to our previous proof. The first case has a very similar proof to the one below. We denote our rectangle R and name $I_R, ..., I_T$ the interior points of R, X, Y, Z, T respectively, and similar notation for boundary points B and area A.

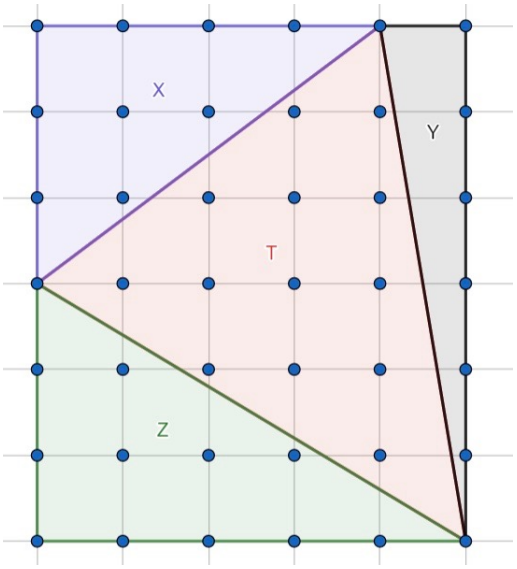

Figure 7: A triangle "inscribed" in a rectangle

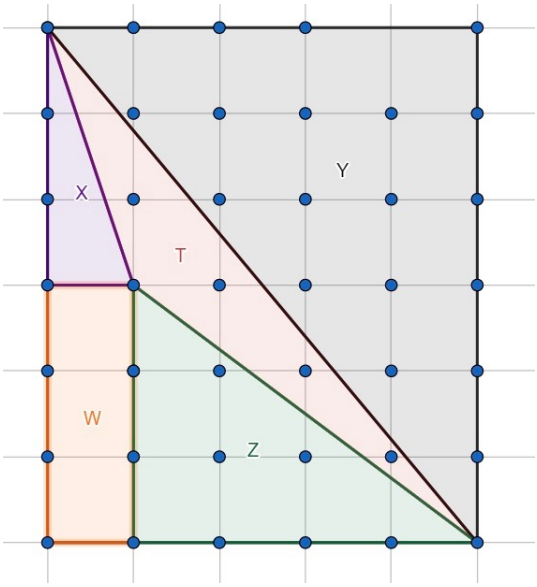

Figure 8: Special case where a vertex is not top/bottom/right/left-most

Considering our general case, we have:

$$I_T = I_R - (I_X + I_Y + I_Z + B_T) + 3$$

Here we add the 3 on the end as we have have included the vertices of T in taking away B_T which needs to be accounted for. For boundary points:

$$B_T = B_X + B_Y + B_Z - B_R$$

Here the 3 "overlaps" at the vertices of T are taken care of when we subtract the boundary points of R at the end of the sum. We substitute these values of I_T and B_T into our expression:
$\mathrm{I}_T + \frac{B_T}{2} - 1 = I_R - (I_X + I_Y + I_Z + B_T) + 3 + \frac{B_T}{2} - 1$
$= I_R - (I_X + I_Y + I_Z) + 3 - \frac{B_T}{2} - 1$
$= I_R - (I_X + I_Y + I_Z) + \frac{B_R - (B_X + B_Y + B_Z)}{2} + 2$

$= \left(I_R + \frac{B_R}{2} - 1\right) - \left(I_X + \frac{B_X}{2} - 1\right) - \left(I_Y + \frac{B_Y}{2} - 1\right) - \left(I_Z + \frac{B_Z}{2} - 1\right)$
$= A_R - A_X - A_Y - A_Z$ The area of our triangle T.

Finally, we have to prove that any polygon can be triangulated. We do this by induction, by first proving the statement for 3 vertices, then assuming it for less than $n-1$ vertices and using it to prove the n case. Consider a polygon P with n vertices, if $n = 3$, then trivially it is, as P is a triangle.
Let x denote the leftmost vertex of P, and y, z its adjacent edges. Consider 2 cases:

1. $\overline{yz}$ is contained inside P (see Figure 9). Then we have that $\overline{yz}$ partitions P into 2 polygons with less vertices, so that case is covered.

2. $\overline{yz}$ is not contained inside P (see Figure 10). Then the triangle xyz must contain some vertices of P. Let u be the farthest one of these from $\overline{yz}$. If $\overline{xu}$ is not contained in P then it must intersect some edge of P, meaning at the end of such an edge there must exist a vertex inside xyz farther from $\overline{yz}$ than u, contradicting its definition. Hence $\overline{xu}$ partitions P into 2 polygons with less vertices.

By induction, we know therefore that P can be triangulated.

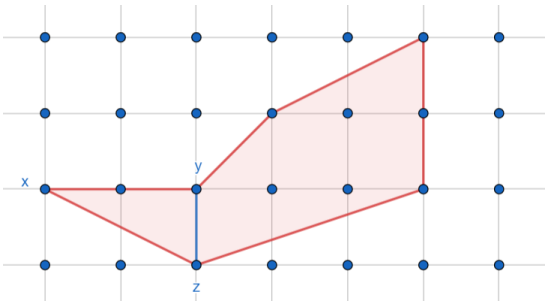

Figure 9: $\overline{yz}$ contained inside P

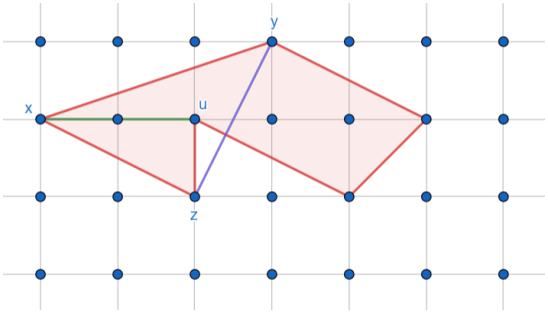

Figure 10: $\overline{yz}$ not contained inside P.

Now it is time to put all our results together. Choosing an arbitrary polygon P, we have that P can be split some N triangles, all of which satisfying Pick's theorem, by our result earlier. From our very first result, we know that if 2 polygons sharing a side both satisfy Pick's theorem, then their composition also does. Extending this result inductively to the N triangles, we have that P satisfies Pick's theorem. That is, for P with I interior points and B boundary points, the area A of P can be written:

$$A = I + \frac{B}{2} - 1$$

□

3.2 Proof using Euler's Formula

In this section, we will introduce *Euler's Characteristic*, an important topological invariant, show its special case for convex polyhedra in 2D and then use it to prove Theorem 3.1.

Definition 3.1. An *Euler Characteristic* of a topological space N is $\chi = V - E + F$, where V, E, F denote the numbers of vertices, edges and faces of N respectively.

There is a well-known result for χ for planar graphs in two dimensions (in particular) discovered by Euler:

Theorem 3.2 (Euler's formula)**.** For a planar graph, $\chi = 2$.

Proof. We will proceed by induction over V.

For $V = 1$ we only have one vertex v, so all E edges have to go from v back to v creating E loops that do not intersect each other. Hence, we have $F = E + 1$ and so $\chi = 1 - E + (E + 1) = 2$.

Now assume that $\chi = 2$ for V vertices, where $V \geq 1$. We will prove that $\chi' = 2$ for $V' = V + 1$. Consider any planar graph with $V + 1$ vertices, E edges and F faces. Then choose any edge of the graph and contract its endpoints. As a result, we get a planar graph with V vertices (two endpoints of an edge got merged into one), $E - 1$ edges and F faces that has the Euler Characteristic of 2 by our inductive hypothesis.
Hence, the Euler Characteristic of our original graph is: $\chi = (V + 1) - (E + 1) + F$
$= V - E + F$
$= 2$ □

Note that we can apply this formula not only for polygons, but also for any two-dimensional figures which edges intersect only at vertices. To prove Pick's theorem, we will need to be able to divide a polygon into primitive triangles:

Proposition 3.3. Every lattice triangle is divisible into primitive lattice triangles.

Proof. Let P be a triangle. Let I_P and B_P denote the numbers of lattice points inside and on the boundary of P, respectively. We shall prove the theorem by induction on $I_P + B_P$.

Base case: $I_P + B_P$=3. Since P is a lattice triangle, $B_P \geq 3$. Then if $I_P + B_P = 3$, it is itself a primitive lattice triangle.

Inductive case: Let $m = I_P + B_P$. Assume that the theorem holds for any triangle T with $I_T + B_T < m$. Since $m > 3$, there must be at least one lattice point on one of its edges or inside. If the point is on an edge, divide the triangle into two smaller ones by connecting the point to the vertex not on the edge. Then each of the new triangles will have less lattice points on them. Otherwise, if the point is inside T, form three new triangles by connecting it to the three vertices. Each smaller triangle will again have less lattice points on them. Either way apply the inductive hypothesis on the smaller triangles and we're done. □

Corollary 3.3.1. Every lattice polygon is divisible into primitive lattice triangles.

Proof. Let P be a lattice polygon. Then there exists a triangulation of P. We then divide P into primitive lattice triangles by applying Proposition 3.3 to each of the triangles. □

With the results above, we can now move to the proof of Pick's theorem.

Proof of Theorem 3.1 using Euler's formula. Firstly, let us divide P into primitive triangles, just like it is shown on Figure 11. (we can do that due to Corollary 3.3.1). Let us call the graph after the division of P into primitive triangles P', i.e. P' is a graph whose vertices are all the lattice points inside and on the boundary of P and edges are the edges of the primitive triangles that we divided P into. The number of such triangles is $F - 1$, where F is the number of faces of P' (we account for the outer face). Each triangle has 3 edges and each edge that is not on the boundary is an edge of 2 distinct triangles. Moreover, the edges on the boundary belong to exactly 1 triangle each. Hence, counting edges in 2 different ways, we have:

$$3(F - 1) + E_{boundary} = 2E_{total}$$

Where clearly $E_{boundary}$ and E_{total} mean the number of edges of P' on the boundary and in total, respectively. Moreover, P' is planar, so due to Theorem 3.2 we have:

$$V - E_{total} + F = 2$$

where V is the number of vertices of P'. Rearranging the two equations and substituting $V = I+B$ and $E_{boundary} = B$, we get the formula for the number of primitive triangles:

$$F - 1 = 2I + B - 2$$

As the area of each primitive triangle is $\frac{1}{2}$ (see Lemma 2.6), we get:

$$A(P) = \frac{F-1}{2} = I + \frac{B}{2} - 1$$

□

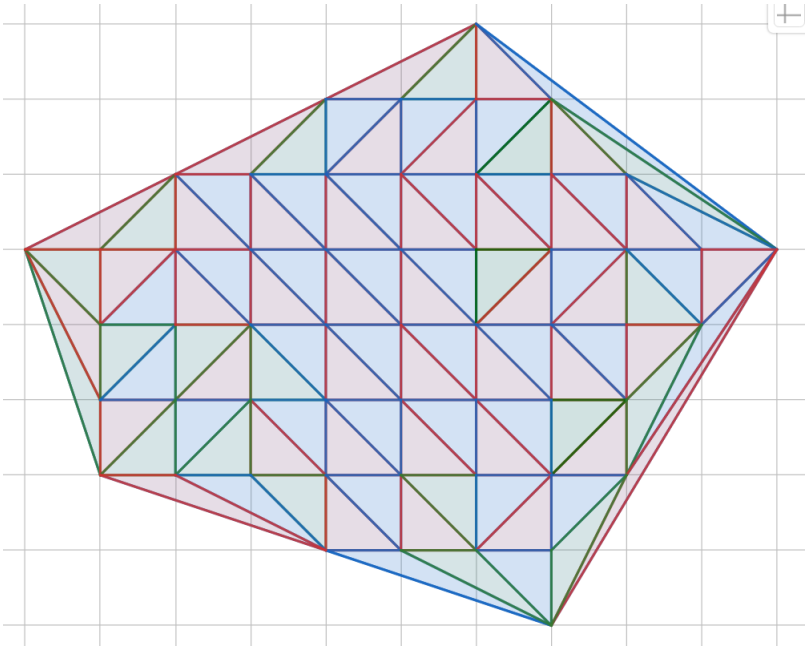

Figure 11: A convex polygon on an integer (rectangular) lattice divided into primitive triangles. Note that the division is not unique but the number of primitive triangles is.

3.3 Interesting Corollaries

With Pick's theorem, we now have a powerful tool to explore different results in lattice point geometry. We first see how in our square lattice it is impossible to make an equilateral triangle, and use a clever proof to extend this to more regular polygons.

Proposition 3.4. Let T be a triangle in R^2 with lattice points as vertices. Then T is not equilateral.

Proof. We follow a similar argument to another proof[4]. Assume there exists such an equilateral triangle with lattice points as vertices, side length a. Then a is the distance between two lattice points in R^2, and therefore a^2 is an integer, as $a^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$, with (x_1, y_1) and (x_2, y_2) being vertices of our triangle. Then using the result that the area of a triangle is equal to a half of its base multiplied by perpendicular height, we have that the area of our triangle is $a^2 \sin(\frac{\pi}{6}) = \frac{a^2\sqrt{3}}{4}$. However, by Pick's theorem we have that its area is equal to $I + \frac{B}{2} - 1$, where I and B denote interior and boundary points of our triangle respectively. Hence, since I and B are both integers, its area is equal to some integer multiple of $\frac{1}{2}$, in particular it is rational. But since a^2 is an integer, we have that the area of our triangle, $\frac{a^2\sqrt{3}}{4}$, is a nonzero rational number multiplied by an irrational number, hence irrational. Thus we arrive at a contradiction, and so our initial assumption that such an equilateral triangle exists must have been false. □

This result is actually true for all n-sided lattice polygons for $n > 4$, or rather, the square is the only regular lattice polygon, we prove without using Pick's Theorem:

Theorem 3.5. The only regular lattice polygon is a square.

Proof. We use a proof similar to that of Hamkins[5]. Let P be an n-sided lattice polygon, and assume that P is regular. First we note that our square lattice is invariant under 90° rotations around any lattice point (x_1, y_1). To see this, choose another lattice point, (x_2, y_2). Letting $a = |x_1 - x_2|$ and $b = |y_1 - y_2|$, we see that (x_2, y_2) is a distance of a away from our rotation point on the x-axis, and b away on the y-axis. When we rotate by 90° (say anticlockwise w.l.o.g.), (x_2, y_2) is now a distance of b away from our rotation point on the x-axis, and a on the y-axis. Since a and b are clearly integers, we have that (x_2, y_2) has been mapped to another lattice point. With this noted, we can continue with our proof. Starting with some arbitrary vertex of P, label the vertices $v_1, \ldots, v_n$ moving anticlockwise. Rotating the edges $\overline{v_1v_2}, \ldots, \overline{v_{n-1}v_n}, \overline{v_nv_1}$ clockwise, from our previous result we have that the endpoints of these rotated edges are themselves lattice points. Label these new points $w_1, \ldots, w_n$. Then by drawing edges $\overline{w_1w_2}, \ldots, \overline{w_{n-1}w_n}, \overline{w_nw_1}$ between these points as in Figure 12, we have made a new lattice polygon Q, with the same number of edges and angles between the edges as P, hence also regular. Note here that since the area of Q is clearly smaller than that of P, we can continue this process inductively to create regular lattice polygons with smaller and smaller area, eventually being smaller than that of the unit square. But this is clearly impossible, since $n > 4$, so we have a contradiction, and no such lattice polygon can exist. □

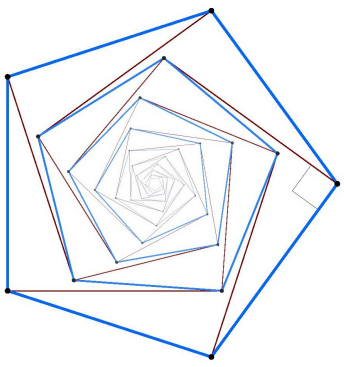

Figure 12: Taken from *jdh.hamkins.org*[5]

4 Pick-esque theorem in higher dimensions

It is only natural at this point to ask if formulas similar to Pick's Theorem exist for polyhedra in R^3.

In this section we shall first present the Reeve tetrahedron, a counterexample showing that in general there exists no such relation connecting the volume of a polyhedron and the number of lattice points inside and on the boundary of the polyhedron. Then we shall discuss several theorems concerning the volume of a lattice polyhedron[7].

4.1 Reeve tetrahedron: a counterexample in R^3

Theorem 4.1 (Reeve tetrahedron)**.** There exists no formula connecting the volume of a convex polyhedron to the number of lattice points inside and on the boundary of the polyhedron.

Proof. Assume such formula exists. Then given convex polyhedron P, there exists function f such that $\mathrm{Vol}(P) = f(I(P), B(P))$, where $I(P)$ and $B(P)$ are respectively the number of lattice points inside and on the boundary of P. Consider the lattice tetrahedron T_h defined by its four vertices $(0,0,0)$, $(1,0,1)$, $(0,1,0)$ and $(0,0,h)$ where $h > 0$. Notice that regardless of the choice of h the tetrahedron always has the same amount of lattice points either inside or on its boundary. However, $\mathrm{Vol}(T_h) = \frac{h}{6}$, therefore such formula does not exist. □

As it turns out we can obtain a formula for convex lattice polyhedra by making use of a *secondary lattice* in addition to the normal lattice. We shall give its definition and a theorem by Reeve in the following section.

4.2 Reeve's formula for volume of convex polyhedra

Before we introduce the formula derived by Reeve we first have to introduce the concept of *secondary lattice*.

Definition 4.1 (Secondary lattice)**.** Let n be a positive integer and L be the lattice generated by the standard basis in R^3. Then we define the n^{th} lattice

$$L_n = \left\{x : x \in R^3, nx \in L\right\}$$

Remark. L_1 is exactly the basic lattice L.

Lemma 4.2. Given two lattice points x, y, if there are m lattice points on line segment $\overline{xy}$ besides x and y, then for every positive integer n, there are exactly $mn + n + 1$ nth lattice points on $\overline{xy}$, including x and y.

The following theorem was given by Reeve:

Theorem 4.3 (Reeve)**.** Let n be a positive integer and P be a convex lattice polyhedron. Then we have the following relations:

$$2(n-1)n(n+1)\mathrm{Vol}(P) = 2I_n(P) + B_n(P) - nB(P) - 2nI(P)$$

$$B_n(P) - n^2(B(P)) = 2\left(1 - n^2\right)$$

The following lemmas and proofs for them are mostly adapted from Reeve's original 1956 paper. For proofs that are too long to be included in this report an outline is provided. We first need some additional theorems and definitions.

Definition 4.2. Let P be a convex polyhedron. Define function

$$M_n(P) = I_n(P) + B_n(P) - nI(P) - nB(P) + (n-1)\,\chi(P)$$

where $\chi(P)$ denotes the Euler characteristic of P.

Lemma 4.4. Let P be a finite path in R^3 that crosses itself only at lattice points and whose vertices are lattice points. Then $M_n(P) = 0$.

Proof. Fix n. Since P finite, we can prove the lemma by induction on the number of edges of P.

Base case: Suppose P has only one edge with $I(P) = m$. Then it contains exactly $m + 1$ segments that each contains no lattice points in its interior. Since it cannot contain a loop, its has two endpoints. Then $B(P) = 2$, and $I_n(P) + B_n(P) = mn + n + 1$ by Lemma 4.2. Since P has two vertices, one edge and no face, $\chi(P) = V - E + F = 1$. Then

$$M_n(P) = mn + n + 1 - n\,(m + 2) + n - 1 = 0.$$

Inductive case: Suppose that P contains $m > 2$ edges and suppose further that the lemma holds for paths with at most $m - 1$ edges. There then exist P_1 and P_2, each contains at most $m - 1$ edges, such that $P = P_1 \cup P_2$ and P_1 only intersects P_2 at lattice points (we can split at vertices). Let $P_0 = P_1 \cup P_2$. Then $P_0 \subset L \subset L_n$. By induction hypothesis $M_n(P_1) = M_n(P_2) = 0$.

Since

$$I_n(P) + B_n(P) = I_n(P_1) + B_n(P_1) + I_n(P_2) + B_n(P_2) - |P_0 \cap L_n|$$

and similarly

$$I(P) + B(P) = I(P_1) + B(P_1) + I(P_2) + B(P_2) - |P_0 \cap L|\,.$$

Then,

$$M_n(P) = M_n(P_1) + M_n(P_2) + (n - 1)\,(\chi(P_1) + \chi(P_2) - \chi(P) + |P_0|)\,.$$

Since P_0 discrete, $\chi(P_0) = |P_0|$. Then $\chi(P) = \chi(P_1 \cup P_2) = \chi(P_1) + \chi(P_2) - \chi(P_0)$ by inclusion-exclusion and therefore $M_n(P) = 0$ as required. □

Definition 4.3. Let F be a lattice, 2-dimensional polyhedron in R^3. Define:

$$G(F) := 2I_n(F) + (2 + n)\,B_n(F) - n\,(2n + 1)\,B(F) - 2n^2 I(F) + 2\left(n^2 - 1\right)\chi(F)$$

Proposition 4.5. Let F be the boundary of a convex polyhedron. Then $G(F) = 0$.

Similar to how we proved Pick's Theorem, we shall first show the additivity of G, show that it is true for any primitive lattice triangle, and then show the existence of triangulation.

Lemma 4.6 (Additivity of G)**.** Let F_1, F_2 be two lattice 2-dimensional polyhedra such that $G(F_1) = G(F_2) = 0$, $p = F_1 \cap F_2$ a lattice path and on the boundary of both F_1 and F_2. Then

$$G(F) = G(F_1) + G(F_2)$$

Proof. Let x be a point on ∂F_1, the boundary of F_1. Then if $x \notin \partial F_2$, $x \in F$. Similarly, $\forall x, x \in F_2 \wedge x \notin F_1 x \in F$. Since $\partial F \subseteq \partial F_1 \cap \partial F_2$, $B_n(F) = B_n(F_1) + B_n(F_2) - 2B_n(p) + |\partial F \cap p|$. Since $F^\circ \subseteq F_1^\circ \cup F_2^\circ \cup p$ (which are disjoint), $I_n(F) = I_n(F_1) + I_n(F_2) + B_n(p) - |\partial F \cap p|$. Then
$\mathrm{G(F_1)} + G(F_2) - G(F) = -2(n + 1)B_n(p) + 2n(n + 1)B(p) - 2\left(n^2 - 1\right)\chi(p)$
$= -2(n + 1)(B_n(p) - nB(p) + (n - 1)\chi(p))$
$= 0 * ByLemma\ 4.4, since \mathrm{I_n(p)} = I(p) = 0$
Therefore $G(F) = G(F_1) + G(F_2)$ as required. □

Lemma 4.7 ($G(P) = 0$ for primitive triangles)**.** Let P be a primitive lattice triangle in R^3. Then

$$G(P) = 0$$

Proof. Let x, y, z be the vertices of P. Then let Q be the triangle defined by the vertices $(0,0,0), u = y-x, v = z-x$ (using vector subtraction). It should be easy to see that $G(P) = G(Q)$.
Claim. Let R be the rectangle defined by vertices $(0,0,0), (1,0,0), (0,1,0)$ and $(1,1,0)$ and S be the parallelogram spanned by the vectors v and w. Then $G(R) = G(S)$.

Proof of claim. Since R is a rectangle and S a parallelogram, $\chi(R) = \chi(S)$. Let $A_n = L_n \cap R$ and $B_n = L_n \cap S$. We will show that there exists a bijection between A_n and B_n, thereby proving that $B_n(R) + I_n(R) = B_n(S) + I_n(S)$.

Let $U = \{u, v\}$. Then $S \subset U$. Define $f{:}\, U \to R^2$, $xu + yv \mapsto xe_1 + ye_2$. Easy to verify that f bijective on U. Let $p = xu + yv$ be an arbitrary element of B_n. Since $p \in L_n np \in Lnx, ny \in Nf(p) \in L_n$ and $p \in S0 \leq x, y \leq 1f(p) \in S$, $f(p) \in A_n$. Therefore $f(B_n) \subseteq A_n$. Similarly $f^{-1}(A_n) \subseteq B_n$. Then $|A_n| = |B_n|\, I_n(R) + B_n(R) = I_n(S) + B_n(S)$. As both R and S are primitive parallelograms, $B_n(R) = B_n(S)$. Therefore $I_n(R) = I_n(S)$. Substituting into $G(R)$ we get $G(R) = G(S)$. □

By additivity of G we have $G(Q) = G(S)/2$. Then $G(P) = G(R)/2$. Easy to verify that $I_n(R) = (n-1)^2, B_n(R) = 4n, B(R) = 4G(R) = 0G(P) = 0$ as desired. □

Definition 4.4. Let P be a polyhedron in R^3. Define

$$H(P) = 2(n-1)n(n+1)V(P) - 2M_n(P) - M_n(\partial P)$$

where ∂P is the boundary of P.

Proposition 4.8. Let P be a convex polyhedron. Then

$$H(P) = 0$$

Due to the length of the proof and the relative unimportance of its technical details the proof is not included in this report. The original proof was given in Reeve's 1957 paper *On the Volume of Lattice Polyhedra*[10]. It proceeds in a similar way to the proof of Theorem 4.5: we first show the additivity of H_n when two polyhedra only share a subset of their faces and then prove that the theorem is true for primitive tetrahedra. Then the theorem is true by the existence of simplicial decomposition of convex polyhedra, a proof of which can be found in another section.

With Proposition 4.5 and 4.8 we can finally prove Theorem 4.3:

Proof of Theorem 4.3. Since P is a convex polyhedron, $\chi(P) = 1$ and $\chi(\partial P) = 2$.
Then by Proposition 4.8,
2 (n - 1) n (n + 1) V(P) = 2 $M_n(P) - M_n(\partial P)$
$= 2\,[I_n(P) + B_n(P) - nI(P) + nB(P) + (n-1)\chi(P)]$
$- I_n(\partial P) - B_n(\partial P) + nI(\partial P) + nB(\partial P) - (n-1)\chi(\partial P)$.
Since $B_n(P) = B_n(\partial P) + I_n(\partial P)$,

$$2(n-1)n(n+1)V(P) = 2I_n(P) + B_n(P) - nB(P) - 2nI(P)$$

which is exactly first part of Theorem 4.3. As for the second part, notice that $B_n(\partial P) = 0$ since all its edges coincide with two faces. Then by Proposition 4.5

$$2\left(1 - n^2\right) = B_n(P) - n^2 B(P)$$

which is exactly the second part of Theorem 4.3. □

4.3 Generalization in R^n

In his 1957 paper[10] Reeve also conjectured a formula for the volume of convex lattice polytopes (defined in section 6) in R^4 that involves not one but two secondary lattices. His conjecture was later generalized by I.G. Macdonald[7] into R^n:

Theorem 4.9 (Macdonald)**.** Let P be a lattice polytope in R^n. Then
(N - 1) N! V(P) = $\sum_{i=1}^{N-1}(-1)^{i-1}\binom{N-1}{i-1}(2I_n(P) + B_n(P))$
$+ (-1)^{N-1}(2\chi(P) - \chi(\partial P))$

Corollary 4.9.1. Let P be a lattice polygon in R^2. Then

$$A(P) = \frac{1}{2}B(P) + I(P) - \chi(P) + \frac{1}{2}\chi(\partial P)$$

Remark. We are indeed aware of that using Theorem 4.9 is probably not the best way to prove Corollary 4.9.1, which is a somewhat generalized Pick's Theorem that applies to polygons with holes as well. Also notice that if P convex then $2\chi(P)$ and $\chi(\partial P)$ would cancel out.

5 Minkowski's Theorem

One of the most well known and frequently cited results in lattice point geometry is Minkowski's theorem. In this section, we present a proof of the theorem, following the style of the proof presented in *Lectures in Discrete Geometry*[8], and some results in number theory which may be derived by way of it, so as to demonstrate its utility. We say a set $S \subset R^n$ is *convex* if $\forall s \in S, \forall t \in S,\ \{\lambda s + (1-\lambda)t : \lambda \in [0,1]\} \subset S$. We say a set $S \subset R^n$ is *symmetric* if $\forall s \in S, -s \in S$.

Theorem 5.1 (Minkowski 1889)**.** Suppose $S \subset R^n$ is *convex* and *symmetric*, $\Lambda(\mathcal{B}) \subset R^n$ is a full rank lattice and $\mathrm{Vol}(S) > 2^n d(\Lambda)$. Then S contains a nonzero element of Λ.

Proof. Consider the set $S' := \frac{1}{2}S$. Then $\mathrm{Vol}(S') > d(\Lambda)$. Suppose for a contradiction that the set $S' - S' := \{u - v : u \in S', v \in S'\}$ contains no points of Λ other than 0.
Then $\forall u \in \Lambda, \forall v \in \Lambda \setminus \{u\}$, the sets $S' + u$, $S' + v$ must be disjoint. Were this not the case, then we would meet the contradiction:

$$x \in (S' + u) \cap (S' + v)x - u \in S', x - v \in S'v - u \in (S' - S') \cap (\Lambda \setminus \{0\})$$

Let $N \in Z_{\geq 0}$, $C := \Lambda \cap \prod_{i=1}^{n}[-Nb_i, Nb_i]$, $b_i \in \mathcal{B}$, and let $D := \mathrm{Diam}(S')$. Notice that $\frac{1}{2}(\prod_{i=1}^{n}[-b_i, b_i])$ is congruent to the fundamental parallelopiped P. Then we have:

$$\bigcup_{a \in C}(S' + a) \subset \prod_{i=1}^{n}[-(N+D)b_i, (N+D)b_i]$$

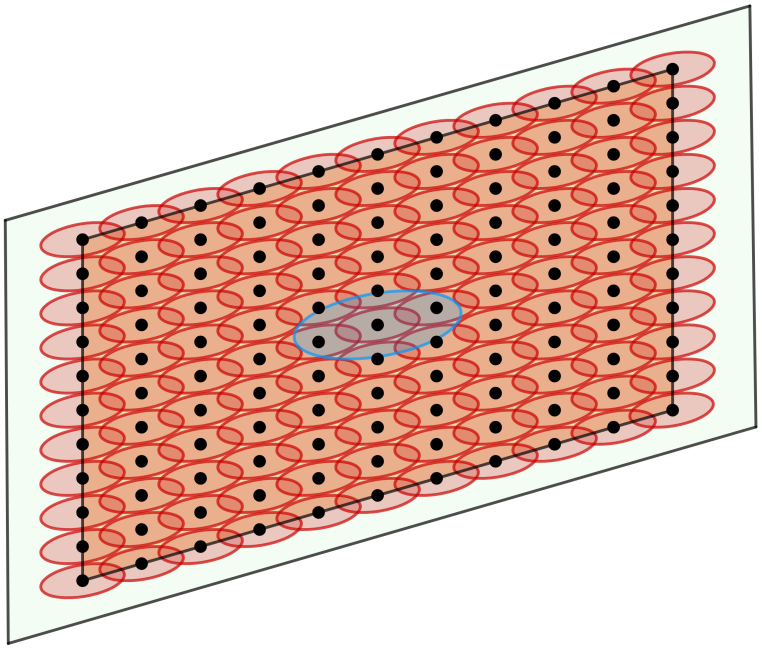

Figure 13: The union of the $S' + a$ being contained in $\prod_{i=1}^{n}[-(N+D)b_i, (N+D)b_i]$

Considering the volume on both sides, we get:

$$(2N+1)^n \text{Vol}(S') \leq (2(N+D))^n d(\Lambda)$$

It follows that:

$$\text{Vol}(S') \leq \left(\frac{2(N+D)}{2N+1}\right)^n d(\Lambda)$$

Taking the limit as $N \to \infty$, we see that $\text{Vol}(S') \leq d(\Lambda)$, a contradiction. Hence:

$$\exists v \in S' - S' \cap (\Lambda \setminus \{0\}) \exists x, x + v \in S'$$

By symmetry, $-x \in S'$. By convexity, $\frac{1}{2}v = \frac{1}{2}(-x) + \frac{1}{2}(x+v) \in S'$. By the definition of S', we yield the result:

$$\frac{1}{2}v \in S' v \in S$$

□

Having stated and proved Minkowski's theorem, we can start discussing its usefulness.

5.1 Applications

We will show two applications of Minkowski's theorem, both of which concern representing an integer as a sum of squares of integers. Hence, we will find the following definition useful:

Definition 5.1 (Quadratic residue)**.** An integer q is called a *quadratic residue* modulo $n \in Z$ if it is congruent to a perfect square modulo n, i.e. if there exists an integer x such that:

$$x^2 \equiv q \pmod{n}$$

Moreover, we will need a theorem regarding the number of quadratic residues modulo a given odd prime number:

Proposition 5.2. There are $\frac{p+1}{2}$ quadratic residues modulo an odd prime number p.

Proof. Consider two integers a and b. We have that: $a^2 \equiv b^2 \pmod{p} \iff a^2 - b^2 \equiv 0 \pmod{p}$
$\iff (a-b)(a+b) \equiv 0 \pmod{p}$
$\iff a \equiv b \pmod{p} \vee a \equiv -b \pmod{p}$ where the last equivalence comes from the definition of a prime number. Hence, we can see that two perfect squares of two integers are congruent, or equal, modulo p if and only if these integers are equal modulo p or one of them is equal to the negation of the other modulo p. Consider a set $S = \{1, ..., p-1\}$, the set of all non-zero residues modulo p. Due to the second case and because p is odd, we deduce that we can divide S into distinct pairs $(x, p-x)$ for $x = 1, ..., \frac{p-1}{2}$ so that the squares of the numbers in each pair are congruent modulo p. There are $\frac{p-1}{2}$ such pairs and there are no two numbers from distinct pairs which squares are congruent modulo p (due to the above equivalence). This means that there are $\frac{p-1}{2}$ non-zero quadratic residues modulo p. As 0 is trivially a quadratic residue modulo p, we have that in general there are $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ distinct quadratic residues modulo p. □

Also, we need to recall the famous *Wilson's theorem*, following a proof by Stein W.[12]:

Theorem 5.3 (Wilson's theorem)**.** An integer p is prime if and only if:

$$(p-1)! \equiv -1 \pmod{p}$$

5.1.1 Fermat's two-square theorem

Fermat's two-square theorem is well-known in the world of number theory. It was stated by Pierre de Fermat in 1640, however he did not provide any proof of the statement. Only in 1747 was it officially proved by Leonhard Euler. We will state the theorem and prove it using Minkowski's theorem in two dimensions. However, firstly we need to introduce a helpful lemma:

Lemma 5.4. Consider a prime number p such that $p \equiv 1 \pmod{4}$. Then there exists an integer a such that:

$$a^2 \equiv -1 \pmod{p}$$

Proof. From Proposition 5.3: -1$\equiv (p-1)!$
$\equiv 1 \cdot 2 \cdot 3 \cdot \cdot (p-2)(p-1)$
$\equiv 1 \cdot 2 \cdot 3 \cdot \cdot \left(\frac{p-1}{2}\right) \cdot \left(-\frac{p-1}{2}\right) \cdot \cdot (-2) \cdot (-1)$
$\equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \cdot (-1)^{\frac{p-1}{2}}$
$\equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}$ where the last congruence follows from the assumption that $p \equiv 1 \pmod{4}$ (then $p-1$ is divisible by 4, so $\frac{p-1}{2}$ is even). Setting $a = \left(\frac{p-1}{2}\right)!$ yields the result. □

Theorem 5.5 (Fermat's two-square theorem)**.** Consider an odd prime number p. Then p can be represented as a sum of two integer squares if and only if $p \equiv 1 \pmod 4$.

Proof. Firstly, we prove the "if" part.

Take a prime number $p \equiv 1 \pmod 4$. Using Lemma 5.4, we take $a \in Z$ such that $a^2 \equiv -1 \pmod p$. Consider a lattice $\Lambda = \Lambda((a,1)^T, (p,0)^T)$. Then $d(\Lambda) = p$. Take a 2D ball $\mathcal{F} = B_0(\sqrt{2p})$. We have:

$$\mathrm{Vol}(\mathcal{F}) = 2p\pi > 4p = 4d(\Lambda)$$

Hence, due to Minkowski's theorem, $\mathcal{F}$ contains a non-zero lattice point $(na + mp, n)$, where $n, m \in Z$. This implies $0 < \sqrt{(na+mp)^2 + n^2} < \sqrt{2p}$, so that $0 < (na+mp)^2 + n^2 < 2p$. Moreover, we have: $(\mathrm{na}+\mathrm{mp})^2 + n^2 \equiv (na)^2 + n^2$
$\equiv n^2(a^2+1)$
$\equiv 0 \pmod p$ due to the construction of a. Hence $(na+mp)^2 + n^2$ is a multiple of p in the range $(0, 2p)$, so we must have $p = (na+mp)^2 + n^2$. This yields the left hand side of the thesis.

The proof of the converse is much simpler. We know that 0 and 1 are the only quadratic residues modulo 4, (for an even number $2n$ we have $(2n)^2 \equiv 4n^2 \equiv 0 \pmod 4$ and for an odd number $2n+1$ we have $(2n+1)^2 \equiv 4n^2 + 4n + 1 \equiv 1 \pmod 4$, $n \in Z$). Hence, a sum of two squares cannot give a remainder 3 modulo 4, so if an odd prime number p can be represented as a sum of two squares, it must give a remainder of 1 modulo 4. □

5.1.2 Lagrange's four-square theorem

Lagrange's four-square theorem is another very powerful result in number theory describing a similar problem. It states that every positive (also non-negative, because the zero case is trivial) integer can be expressed as a sum of four integer squares. In order to prove it, let us firstly introduce two lemmas that we will find helpful in the proof of the theorem.

Lemma 5.6 (Euler)**.** If two integers k, l can both be expressed as sums for four integer squares, then their also product kl can be expressed as a sum of four integer squares.

Proof. Let $k = a^2 + b^2 + c^2 + d^2$ and $l = x^2 + y^2 + u^2 + v^2$. Then: $\mathrm{kl} = (\mathrm{a}^2 + b^2 + c^2 + d^2)(x^2 + y^2 + u^2 + v^2)$
$= (ax + by + cu + dv)^2 + (ay - bx + cv - du)^2$
$+ (au - bv - cx + dy)^2 + (av + bu - cy - dx)^2$

So kl can indeed be expressed as a sum of four integer squares. □

Lemma 5.7. Let p be an odd prime number. Then there exist $a, b \in Z$ such that $a^2 + b^2 + 1 \equiv 0 \pmod p$

Proof. Consider an equivalent congruence:

$$a^2 \equiv -b^2 - 1 \pmod p$$

Notice that we have $\frac{p+1}{2}$ distinct possibilities for values modulo p on both sides of the congruence due to Proposition 5.2. However, there are only p distinct residues modulo p. Hence, due to the *Pigeonhole principle*, there exist a, b that satisfy the congruence (otherwise, we would have to have $\frac{p+1}{2} + \frac{p+1}{2} = p + 1$ distinct residues modulo p, which is a contradiction). □

Using the above lemmas and Minkowski's theorem, we should now be able to prove the four-square theorem:

Theorem 5.8 (Lagrange's four-square theorem)**.** Every positive integer can be expressed as a sum of four integer squares.

Proof. Cases of $1 = 1^2 + 0^2 + 0^2 + 0^2$ and $2 = 1^2 + 1^2 + 0^2 + 0^2$ are trivial. Now it suffices to show the theorem for any odd prime number p. Then we can just use Lemma 5.6 to deduce the theorem in the general case (due to the *Fundamental Theorem of Arithmetic*).

The proof is conceptually similar to the proof of Theorem 5.5. Consider an odd prime number p and integers a, b such that:

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}$$

(such a and b exist due to Lemma 5.7). Consider the following four vectors in Z^4: $\mathrm{v}_1 = (p, 0, 0, 0)^T$
$v_2 = (0, p, 0, 0)^T$
$v_3 = (a, b, 1, 0)^T$
$v_4 = (b, -a, 0, 1)^T$ Let $\mathcal{B} = \{v_1, v_2, v_3, v_4\}$. Consider a lattice $\Lambda = \Lambda(\mathcal{B})$. We have, due to Theorem 2.1:

$$d(\Lambda) = |det(\mathcal{B})| = p^2$$

Now consider a 4D ball $\mathcal{F} = B_{\sqrt{2p}}(0)$. The volume of $\mathcal{F}$ is:

$$\mathrm{Vol}(\mathcal{F}) = \frac{1}{2}\pi^2(\sqrt{2p})^4 = 2\pi^2 p^2$$

Hence, we have:

$$\mathrm{Vol}(\mathcal{F}) = 2\pi^2 p^2 > 16p^2 = 2^4 d(\Lambda)$$

So, using Minkowski theorem in 4 dimensions, there exists a non-zero lattice point T in $\mathcal{F}$:

$$T = t_1 v_1 + t_2 v_2 + t_3 v_3 + t_4 v_4 \in (\Lambda(\mathcal{B}) \setminus \{0\}) \cap \mathcal{F}$$

where $t_1, t_2, t_3, t_4 \in Z$. Let $||X||$ denote the distance from a point $X \in R^n$ to the origin. Consider $||T||^2$ modulo p: $||\mathrm{T}||^2 \equiv ||(t_1 p + t_3 a + t_4 b, t_2 p + t_3 b - t_4 a, t_3, t_4)^T||^2$
$\equiv (t_1 p + t_3 a + t_4 b)^2 + (t_2 p + t_3 b - t_4 a)^2 + t_3^2 + t_4^2$
$\equiv (t_3 a + t_4 b)^2 + (t_3 b - t_4 a)^2 + t_3^2 + t_4^2$
$\equiv (a^2 + b^2 + 1)(t_3^2 + t_4^2)$
$\equiv 0 \pmod{p}$ where the last congruence follows from the choice of a and b. So p divides $||T||^2$. Moreover, note that, for any $x_1, x_2, x_3, x_4 \in R$, we have:

$$v = (x_1, x_2, x_3, x_4) \in \mathcal{F} \iff x_1^2 + x_2^2 + x_3^2 + x_4^2 < (\sqrt{2p})^2 = 2p$$

So, from the choice of T, we have that $0 < ||T||^2 < 2p$. This means that $||T||^2 = p$, because p is the only integer multiple of p in $(0, 2p)$. Hence, we have found a representation of p as a sum of four integer squares as intended $\big(p = (t_1 p + t_3 a + t_4 b)^2 + (t_2 p + t_3 b - t_4 a)^2 + t_3^2 + t_4^2\big)$. □

5.1.3 Dirichlet's theorem

Here we present a proof[11] on Dirichlet's theorem on Diophantine approximations of real numbers:

Theorem 5.9 (Dirichlet)**.** Let α be a real number, and Q a positive integer. Then there exist integers p and q, with $q \in (0, Q]$, such that $|\alpha - \frac{p}{q}| \leq \frac{1}{Q}$.

Proof. We assume $Q > 1$. Consider the set of points in R^2 which satisfy the following inequalities:

$$y \leq \alpha x + \frac{1}{Q}$$

$$y \geq \alpha x - \frac{1}{Q}$$

$$x \leq Q$$

$$x \geq -Q$$

This defines a closed parallelogram with area $4Q\frac{1}{Q} = 4$ which is symmetric about the origin, and hence, using Minkowski's theorem in two dimensions, it follows that it contains some nonzero integral point $(p, q) \in Z^2$. Since q cannot equal 0, our inequalities imply:

$$|p - \alpha q| \leq \frac{1}{Q}$$

□

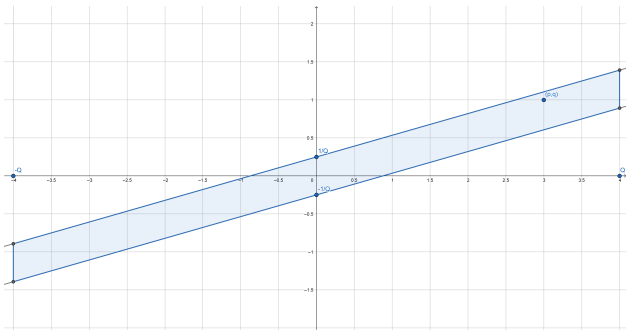

Figure 14: Region satisfying the inequalities

6 Ehrhart Polynomials and Triangulation

In this section we focus mostly on Ehrhart polynomials and simple results for convex polytopes in any dimension. Each section aims to show different properties of Ehrhart polynomials and/or methods for computing said polynomial. Finally, section 6.5 gives us a generalisation of the triangulation theorem from section 3.1. This section is based on the textbook by Beck and Robbins [2]; section 6.2 on Ehrhart polynomials was inspired by section 2.6 of the text, the basic examples of sections 6.3 and 6.4 are based on sections 2.2 and 2.3 of the text, with alterations and some generalisations, and section 6.5 is adapted slightly from section 3.1 of the text.

6.1 Definitions

Here we find a generalisation of Pick's formula to R^n as Ehrhart polynomials. These polynomials relate integral points of a polytope to various properties of the shape. We need definitions and begin by generalising polygons and polyhedra. We can define convex polytopes in terms of their vertices.

Definition 6.1 (Convex Polytope)**.** We denote our convex polytope by $\mathcal{P}$. Given $\{v_1, v_2, ..., v_k\} \subset R^n$ defined as the vertices of $\mathcal{P}$, we say $\mathcal{P}$ is the *convex hull* of the given vertices. That is:

$$\mathcal{P} = \text{Conv}(v_1, v_2, ..., v_k) = \{\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_k v_k : \ \alpha_i \geq 0, \alpha_1 + \alpha_2 + ... + \alpha_k = 1\}.$$

We define the dimension of $\mathcal{P}$ by the dimension of the affine space

$$\text{Span}\, \mathcal{P} = \{\mathbf{x} + \lambda(\mathbf{y} - \mathbf{x}) : \mathbf{x}, \mathbf{y} \in \mathcal{P}, \lambda \in R\}.$$

If $\mathcal{P}$ has dimension d we call it a *d-polytope*, and if $d = n$ we say $\mathcal{P}$ has *full rank* or *full dimension*. If the vertices of $\mathcal{P}$ are all lattice points, we call it a convex *lattice* polytope. It is called *primitive* if it has no interior points.

Definition 6.2 (Faces)**.** Let $\mathcal{P}$ be a d-polytope of full-dimension. A *supporting hyperplane* of $\mathcal{P}$ is a hyperplane $H = \{x \in R^d : a \cdot x = b\}$ such that $\mathcal{P}$ lies on either side of H, i.e. $\mathcal{P} \subset a \cdot x \leq b$ or $\mathcal{P} \subset a \cdot x \geq b$.

A *face* of $\mathcal{P}$ is the intersection of $\mathcal{P}$ and H. For example, considering a polyhedron, vertices, edges and faces all count as faces in the general definition, along with the polyhedron as a whole. A vertex is also face (of dimension 0), an *edge* is a face of dimension 1, and a *facet* is a face of dimension $d - 1$.

Now we need to define Erthart polynomials for a polytope $\mathcal{P}$. We define the t^{th} dilate of $\mathcal{P}$ as:

$$t\mathcal{P} = \{t\mathbf{x} : \mathbf{x} \in \mathcal{P}\}$$

Definition 6.3 (Erthart Polynomial and Erthart Series)**.** Let $\mathcal{P}$ be a polytope in R^d. The *Ehrhart polynomial* of $\mathcal{P}$, also called the *lattice-point enumeration* of $\mathcal{P}$, is defined as the number of integral points in Z^d contained in $\mathcal{P}$ (note this includes both points on the boundary and interior). We denote it by

$$L_{\mathcal{P}}(t) := \#(t\mathcal{P} \cap Z^d).$$

Note: stricly speaking, $L_{\mathcal{P}}(t)$ is the lattice-point enumerator of $t\mathcal{P}$.

The *Ehrhart series* is a generating function for the Ehrhart polynomial, defined by

$$Ehr_{\mathcal{P}}(z) := 1 + \sum_{t \geq 1} L_{\mathcal{P}}(t) z^t$$

6.2 Ehrhart Polynomials of Simple Polygons in R^2

This section uses Pick's theorem to find the lattice-point enumerator of any simple polygon, and to prove and showcase general properties of Ehrhart polynomials in R^2.

Theorem 6.1. The Ehrhart polynomial of any convex integral polygon $\mathcal{P}$ is given by

$$L_{\mathcal{P}}(t) = At^2 + \frac{1}{2}Bt + 1$$

Proof. By Pick's theorem, the amount of integral points in $\mathcal{P}$ (both interior and boundary points) is given by

$$L_{\mathcal{P}}(1) = I + B = A - \frac{B}{2} + 1 + B = A + \frac{B}{2} + 1.$$

Now we notice that the area of the t^{th} dilate of $\mathcal{P}$ is given by At^2 and the boundary points by Bt giving us

$$L_{\mathcal{P}}(t) = At^2 + \frac{1}{2}t + 1.$$

□

This gives us a taste of a general property of Ehrhart polynomials; the leading co-efficient of $L_{\mathcal{P}}(t)$ (co-efficient of t^d) is always the d-dimensional volume of the polytope; the co-efficient of t^{d-1} is the number of lattice points of the boundary of $\mathcal{P}$ (analogous to boundary points of our convex polygons); the constant term is given by the Euler characteristic of the polytope (a generalisation of the Euler characteristic used in section 3.2).

6.3 The d-cube

The simplest example of a d-dimensional polytope is the unit *d-cube*. It is defined by convex hull of the 2^d points containing either 0 or 1 in each component. We will denote the d-cube by the symbol . The Ehrhart polynomial for this can easily be seen to be

$$L_{(}(t) = (t+1)^d = \sum_{k=0}^{d} \binom{d}{k} t^k$$

Looking now at the interior of the d-cube, we see that

$$L(t) = (t-1)^d,$$

and hence we see that $(-1)^d L_{(}(-t) = L(t)$. This turns out to be a general result that applies to the interior of any polytope as we will soon see.

Considering now the unit d-cube, but stretched by a positive real number a_i along the standard basis e_i. We will again refer to this polytope by . The lattice point enumerator of the line segment $[0, a_i]$ is given by

$$L_{[0,a_i]}(t) = \lfloor a_i t \rfloor + 1.$$

With this we can easily calculate the Ehrhart polynomial of this more general cube as

$$L_{(}(t) = \prod_{i=1}^{d} (\lfloor a_i t \rfloor + 1).$$

6.4 The standard d-simplex

Definition 6.4 (Simplex)**.** A *d-simplex* is the convex hull of $d+1$ affinely independant points (vertices) in R^d.

Affine independance assures that this polytope is d-dimensional and not of lower dimension. The *standard simplex* or *probability simplex* is defined by the convex hull of the $d+1$ points:

$$\triangle = conv(\{0\} \cup \{e_i : i = 1, ..., d\}).$$

More importantly, we can write it (and it's t^{th} dilate) as an inequality, which we call its *hyperplane* description:

$\triangle = \{(x_1, ..., x_d) \in R^d : \sum_{i=1}^{d} x_i \leq 1, x_i \geq 0\}$
$t\triangle = \{(x_1, ..., x_d) \in R^d : \sum_{i=1}^{d} x_i \leq t, x_i \geq 0\}$
For the lattice point enumerator of $t\triangle$, we require each x_i to be an integral point. Therefore there exists x_{d+1} such that

$$\sum_{i=1}^{d+1} x_i = t \tag{1}$$

To find $L_\triangle(t)$ we must find the possible solutions to equation (1). We do this by considering the following:

$$\frac{1}{(1-z)^{d+1}} = \left(\sum_{k_1=0}^{\infty} z^{k_1}\right) \cdots \left(\sum_{k_{d+1}=0}^{\infty} z^{k_{d+1}}\right) = \sum_{k=0}^{\infty} \binom{d+k}{d} z^k.$$

Note that $\binom{d+t}{d}$ is exactly the amount of solutions to equation (1), and therefore the above is exactly an expression for the Ehrhart series of the standard simplex:

$$Ehr_\triangle(z) = 1 + \sum_{t=1}^{\infty} \binom{d+t}{d} z^t,$$

and thus our Ehrhart polynomial is given by

$$L_\triangle(t) = \binom{d+t}{d}.$$

6.5 Triangulation

Analogously to the triangulation in our proof of Pick's theorem in section 2, we can similarly decompose any convex polytope into simplices.

Definition 6.5 (Triangulation)**.** A *triangulation* of a d-polytope $\mathcal{P}$ is a finite set $\{T_1, ..., T_k\}$ of d-simplices such that

$$\mathcal{P} = \bigcup_{i=1}^{k} T_i,$$

$$\forall\, 1 \leq i, j \leq k, T_i \cap T_j is a face of both T_1 and T_2.$$

This second property means the interior of all the simplices are mutually disjoint. A triangulation *with no new vertices* is a triangulation such that all vertices of T_i are also vertices of $\mathcal{P}$.

Theorem 6.2 (Existence of triangulations)**.** Every convex polytope can be triangulated using no new vertices.

Proof. [2] We will only prove the first condition of triangulation here. Without loss of generality assume our polytope $\mathcal{P}$ is full dimensional with dimension d, and construct a $(d+1)$-dimensional polytope $\mathcal{Q}$ by adding any real value ("height") to the end of each vertex such that the resulting polytope is full-dimensional in R^{d+1}, i.e. if $\mathcal{P} = \text{Conv}(v_1, ..., v_k\}$

$$\mathcal{Q} = \text{Conv}((v_1, h_1), ..., (v_k, h_k)).$$

Here we call $\mathcal{Q}$ a *lifted polytope* of $\mathcal{P}$. Define a projection from R^{d+1} to R^d by

$$\pi : R^{d+1} \to R^d : (x_1, ..., x_d, x_{d+1}) \mapsto (x_1, ..., x_d).$$

We define a *lower hull* of $\mathcal{Q}$ as all points $x = (x_1, ..., x_{d+1}) \in \mathcal{Q}$ such that there does not exist another point $y = (y_1, ..., y_{d+1}) \in \mathcal{Q}$ with $x_{d+1} > y_{d+1}$ or, less formally, all points visible from below. We define a *lower face* of $\mathcal{Q}$ as a face of $\mathcal{Q}$ which is in the lower hull of $\mathcal{Q}$. We need to prove that the lower faces of $\mathcal{Q}$ form a triangulation of $\mathcal{P}$ once projected down using π This can be seen visually in figure 15.

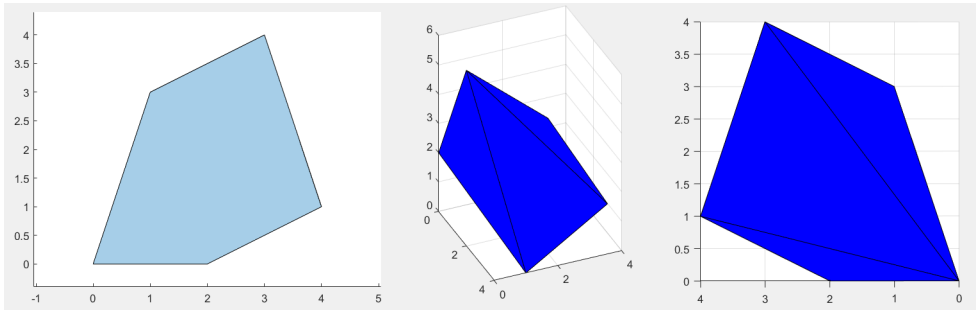

Figure 15: Triangulation of an irregular pentagon. (left) Pentagon, (middle) 3D view of the lifted polytope, (right) view from below of the lifted polytope, showing the triangulation. Note that the view from below must be reflected due to the orientation of the space.

We first prove that each lower face of $\mathcal{Q}$ is a simplex. More simply, since each face of a simplex is also a simplex, we only need to prove that every lower facet of $\mathcal{Q}$ is a simplex. This is equivalent to showing that every set of $d+1$ affinely independent vertices of $\mathcal{P}$ gets lifted to a set of $d+1$ affinely independent points in R^{d+1} that determines a hyperplane H that does not contain any other lifted vertex of $\mathcal{P}$. Given a set of $d+1$ affinely independent vertices relabel them as $v_1, ..., v_{d+1}$ such that H is given by

$$H = \left\{(x_1, ..., x_{d+1}) \equiv (x, x_{d+1}) \in R^{d+1} : \det\left(11 \cdots 11 v_1 v_2 \cdots v_{d+1} x h_1 h_2 \cdots h_{d+1} x_{d+1}\right) = 0\right\}.$$

Suppose H contains another lifted vertex of $\mathcal{P}$. Choose some $(v_j, h_j), j > d+1$. Since $\{h_i\}$ were chosen in a way such that the lifted polytope $\mathcal{Q}$ was full dimensional, inserting our new vertex into the definition of H provides a non-zero determinant since we specified $\{v_1, ..., v_{d+1}\}$ were affinely independent. Therefore we have shown that the lower faces of $\mathcal{Q}$ are simplices.

Now we just have to prove that $T = \{\pi(F) : F is a face of \mathcal{Q}\}$ does indeed triangulate $\mathcal{P}$. Note that by construction there is a bijection between the lower faces of $\mathcal{Q}$ and their projections onto R^d, and therefore T consists of simplices which are contained in $\mathcal{P}$ (this is because a projection retains the *face structure* of a polytope). Because of this, it is only necessary to show

$$\mathring{\mathcal{P}} \subset \bigcup_{T_i \in T} T_i.$$

Let $x \in \mathring{\mathcal{P}}$. Define $L := \{x + \lambda e_{d+1} : \lambda \in R\}$, such that L a line normal to our polytope (i.e. "vertical") going through x. Since $x \in \mathring{\mathcal{P}}$ we know that $L \cap \mathring{\mathcal{Q}}$ is non-empty, by construction of

$\mathcal{Q}$. Therefore $L \cap \mathcal{Q}$ is a line segment with end points (x, y) and (x, z), $y < z$, with these points being on the boundary of $\mathcal{Q}$ and $y, z \in R$. Since (x, y) is on the boundary of $\mathcal{Q}$, this implies that it is contained in some face $\mathcal{F}$ of $\mathcal{Q}$, with $\mathcal{F} \neq \mathcal{Q}$. We let H be its supporting hyperplane with equation

$$H = \{p \in R^{d+1} : a \cdot p = b\},$$

for some $a \in R^{d+1}$, such that $\mathcal{Q} \subset \{p \in R^{d+1} : a \cdot p \geq b\}$. Since x does not lie on the boundary of $\mathcal{Q}$, we know that (x, z) cannot be contained in H. Therefore we obtain $a \cdot (x, y) = b$ and $a \cdot (x, z) > b$. Therefore we have

$$a \cdot [(x, z) - (x, y)] > 0, \longrightarrow a_{d+1}(z - y) > 0,$$

and since $y < z$, we obtain that $a_{d+1} > 0$. It can then be shown that a hyperplane H must define a lower face of $\mathcal{Q}$ when $a_{d+1} > 0$. Therefore we have shown that the lower faces of $\mathcal{Q}$ are simplices who's union is equal to $\mathcal{P}$.

□

References

1. Abiy, T. and Ellinor, A. (2015). Polygon Triangulation / Grids. [online] Brilliant.org. Available at: https://brilliant.org/wiki/polygon-triangulation-grids/ [Accessed 10 June 2020].

2. Beck, M. and Robbins, S. (2015). *Computing The Continuous Discretely.* 2nd ed. New York: Springer-Verlag New York, pp.29-33, 59-61.

3. Garbett, J. (2010). Lattice Point Geometry: Pick's Theorem And Minkowski's Theorem. [online] Documents.kenyon.edu. Available at: <https://documents.kenyon.edu/math/GarbettJSenEx2011.pdf> [Accessed 11 June 2020].

4. Goh, P., Balaji, S., Lin, C., Kau, A. and Khim, J. (2015). Pick's Theorem. [online] Brilliant.org. Available at: https://brilliant.org/wiki/picks-theorem/ [Accessed 10 June 2020].

5. Hamkins, J. (2016). There Are No Nondegenerate Regular Polygons In The Integer Lattice, Except For Squares. [online] jdh.hamkins.org. Available at: http://jdh.hamkins.org/no-regular-polygons-in-the-integer-lattice/ [Accessed 10 June 2020].

6. Larsson, E. and Löfberg, H. (2014). A Proof Of Pick's Theorem. [online] Kurser.math.su.se. Available at: https://kurser.math.su.se/pluginfile.php/15491/mod_resource/content/1/picks.pdf [Accessed 10 June 2020].

7. Macdonald, I. G. (1963). The volume of a lattice polyhedron. *Mathematical Proceedings of the Cambridge Philosophical Society.* Cambridge University Press, 59(4), pp. 719–726. doi: 10.1017/S0305004100003716.

8. Matousek, J. (2002). *Lectures On Discrete Geometry.* New York, NY: Springer, pp.17-18

9. Micciancio, D. (2020). CSE206A: Lattices Algorithms And Applications (Fall 2019). [online] Cseweb.ucsd.edu. Available at: <http://cseweb.ucsd.edu/classes/fa19/cse206A-a/> [Accessed 11 June 2020].

10. Reeve, J.E. (1957). On the Volume of Lattice Polyhedra. *Proceedings of the London Mathematical Society*, s3-7: 378-395. doi:10.1112/plms/s3-7.1.378

11. Shmonin, G. (2009). Minkowski's Theorem And Its Applications. [online] Fmf.uni-lj.si. Available at: <https://www.fmf.uni-lj.si/ lavric/Shmonin%20-%20Minkowski's%20theorem %20and%20its%20applications.pdf> [Accessed 12 June 2020]

12. Stein, W. (2009). *Elementary Number Theory: Primes, Congruences And Secrets.* New York: Springer-Verlag New York, pp.27-28.d