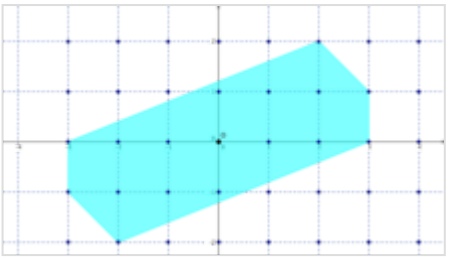
Minkowski's theorem

In mathematics, **Minkowski's theorem** is the statement that every convex set in $\mathbb{R}^n$ which is symmetric with respect to the origin and which has volume greater than 2^n contains a non-zero integer point (meaning a point in $\mathbb{Z}^n$ that is not the origin). The theorem was proved by Hermann Minkowski in 1889 and became the foundation of the branch of number theory called the geometry of numbers. It can be extended from the integers to any lattice L and to any symmetric convex set with volume greater than $2^n d(L)$, where $d(L)$ denotes the covolume of the lattice (the absolute value of the determinant of any of its bases).



A set in $\mathbb{R}^2$ satisfying the hypotheses of Minkowski's theorem.

Formulation

Suppose that L is a lattice of determinant $\mathrm{d}(L)$ in the n-dimensional real vector space $\mathbb{R}^n$ and S is a convex subset of $\mathbb{R}^n$ that is symmetric with respect to the origin, meaning that if x is in S then $-x$ is also in S. Minkowski's theorem states that if the volume of S is strictly greater than $2^n \mathrm{d}(L)$, then S must contain at least one lattice point other than the origin. (Since the set S is symmetric, it would then contain at least three lattice points: the origin 0 and a pair of points $\pm x$, where $x \in L \setminus 0$.)

Example

The simplest example of a lattice is the integer lattice $\mathbb{Z}^n$ of all points with integer coefficients; its determinant is 1. For $n = 2$, the theorem claims that a convex figure in the Euclidean plane symmetric about the origin and with area greater than 4 encloses at least one lattice point in addition to the origin. The area bound is sharp: if S is the interior of the square with vertices $(\pm 1, \pm 1)$ then S is symmetric and convex, and has area 4, but the only lattice point it contains is the origin. This example, showing that the bound of the theorem is sharp, generalizes to hypercubes in every dimension n.

Proof

The following argument proves Minkowski's theorem for the specific case of $L = \mathbb{Z}^2$.

Proof of the $\mathbb{Z}^2$ case: Consider the map

$$f : S \to \mathbb{R}^2/2L, \qquad (x, y) \mapsto (x \bmod 2, y \bmod 2)$$

Intuitively, this map cuts the plane into 2 by 2 squares, then stacks the squares on top of each other. Clearly $f(S)$ has area less than or equal to 4, because this set lies within a 2 by 2 square. Assume for a contradiction that f could be injective, which means the pieces of S cut out by the squares stack up in a non-overlapping

way. Because f is locally area-preserving, this non-overlapping property would make it area-preserving for all of S, so the area of $f(S)$ would be the same as that of S, which is greater than 4. That is not the case, so the assumption must be false: f is not injective, meaning that there exist at least two distinct points p_1, p_2 in S that are mapped by f to the same point: $f(p_1) = f(p_2)$.

Because of the way f was defined, the only way that $f(p_1)$ can equal $f(p_2)$ is for p_2 to equal $p_1 + (2i, 2j)$ for some integers i and j, not both zero. That is, the coordinates of the two points differ by two even integers. Since S is symmetric about the origin, $-p_1$ is also a point in S. Since S is convex, the line segment between $-p_1$ and p_2 lies entirely in S, and in particular the midpoint of that segment lies in S. In other words,

$$\tfrac{1}{2}(-p_1 + p_2) = \tfrac{1}{2}(-p_1 + p_1 + (2i, 2j)) = (i, j)$$

is a point in S. But this point (i, j) is an integer point, and is not the origin since i and j are not both zero. Therefore, S contains a nonzero integer point.

Remarks:

- The argument above proves the theorem that any set of volume $> \det(L)$ contains two distinct points that differ by a lattice vector. This is a special case of Blichfeldt's theorem.[1]
- The argument above highlights that the term $2^n \det(L)$ is the covolume of the lattice $2L$.
- To obtain a proof for general lattices, it suffices to prove Minkowski's theorem only for $\mathbb{Z}^n$; this is because every full-rank lattice can be written as $B\mathbb{Z}^n$ for some linear transformation B, and the properties of being convex and symmetric about the origin are preserved by linear transformations, while the covolume of $B\mathbb{Z}^n$ is $|\det(B)|$ and volume of a body scales by exactly $\frac{1}{\det(B)}$ under an application of B^{-1}.

Applications

Bounding the shortest vector

Minkowski's theorem gives an upper bound for the length of the shortest nonzero vector. This result has applications in lattice cryptography and number theory.

Theorem (Minkowski's bound on the shortest vector): Let L be a lattice. Then there is a $x \in L \setminus \{0\}$ with $\|x\|_\infty \leq |\det(L)|^{1/n}$. In particular, by the standard comparison between l_2 and l_∞ norms, $\|x\|_2 \leq \sqrt{n}\,|\det(L)|^{1/n}$.

> **Proof**
> Let $l = \min\{\|x\|_\infty : x \in L \setminus \{0\}\}$, and set $C = \{y : \|y\|_\infty < l\}$. Then $\mathrm{vol}(C) = (2l)^n$. If $(2l)^n > 2^n |d(L)|$, then C contains a non-zero lattice point, which is a contradiction. Thus $l \leq |d(L)|^{1/n}$. Q.E.D.

Remarks:

- The constant in the L^2 bound can be improved, for instance by taking the open ball of radius $< l$ as C in the above argument. The optimal constant is known as the Hermite constant.
- The bound given by the theorem can be very loose, as can be seen by considering the lattice generated by $(1,0),(0,n)$. But it cannot be further improved in the sense that there exists a global constant c such that there exists an n-dimensional lattice L satisfying $\|x\|_2 \geq c\sqrt{n} \cdot |\det(L)|^{1/n}$ for all $x \in L \setminus \{0\}$. Furthermore, such lattice can be self-dual. [2]
- Even though Minkowski's theorem guarantees a short lattice vector within a certain magnitude bound, finding this vector is in general a hard computational problem. Finding the vector within a factor guaranteed by Minkowski's bound is referred to as Minkowski's Vector Problem (MVP), and it is known that approximation SVP reduces to it (https://cseweb.ucsd.edu/classes/sp07/cse206a/lec8.pdf) using transference properties of the dual lattice. The computational problem is also sometimes referred to as HermiteSVP.[3]
- The LLL-basis reduction algorithm can be seen as a weak but efficiently algorithmic version of Minkowski's bound on the shortest vector. This is because a δ-LLL reduced basis $b_1, \ldots, b_n$ for L has the property that $\|b_1\| \leq \left(\frac{1}{\delta - .25}\right)^{\frac{n-1}{4}} \det(L)^{1/n}$; see these lecture notes of Micciancio (http://cseweb.ucsd.edu/classes/sp14/cse206A-a/lec5.pdf) for more on this. As explained in,[3] proofs of bounds on the Hermite constant contain some of the key ideas in the LLL-reduction algorithm.

Applications to number theory

Primes that are sums of two squares

The difficult implication in Fermat's theorem on sums of two squares can be proven using Minkowski's bound on the shortest vector.

Theorem: Every prime with $p \equiv 1 \mod 4$ can be written as a sum of two squares.

Proof

Since $4 \mid p-1$ and a is a quadratic residue modulo a prime p if and only if $a^{\frac{p-1}{2}} = 1 \pmod p$ (Euler's Criterion) there is a square root of -1 in $\mathbb{Z}/p\mathbb{Z}$; choose one and call one representative in $\mathbb{Z}$ for it j. Consider the lattice L defined by the vectors $(1,j),(0,p)$, and let B denote the associated matrix. The determinant of this lattice is p, whence Minkowski's bound tells us that there is a nonzero $x = (x_1, x_2) \in \mathbb{Z}^2$ with $0 < \|Bx\|_2^2 < 2p$. We have $\|Bx\|^2 = \|(x_1, jx_1 + px_2)\|^2 = x_1^2 + (jx_1 + px_2)^2$ and we define the integers $a = x_1, b = (jx_1 + px_2)$. Minkowski's bound tells us that $0 < a^2 + b^2 < 2p$, and simple modular arithmetic shows that $a^2 + b^2 = x_1^2 + (jx_1 + px_2)^2 = 0 \mod p$, and thus we conclude that $a^2 + b^2 = p$. Q.E.D.

Additionally, the lattice perspective gives a computationally efficient approach to Fermat's theorem on sums of squares:

Algorithm

First, recall that finding any nonzero vector with norm less than $2p$ in L, the lattice of the proof, gives a decomposition of p as a sum of two squares. Such vectors can be found efficiently, for instance using LLL-algorithm. In particular, if b_1, b_2 is a $3/4$-LLL reduced basis, then, by the property that $\|b_1\| \leq (\frac{1}{\delta - .25})^{\frac{n-1}{4}} \det(B)^{1/n}$, $\|b_1\|^2 \leq \sqrt{2}p < 2p$. Thus, by running the LLL-lattice basis reduction algorithm with $\delta = 3/4$, we obtain a decomposition of p as a sum of squares. Note that because every vector in L has norm squared a multiple of p, the vector returned by the LLL-algorithm in this case is in fact a shortest vector.

Lagrange's four-square theorem

Minkowski's theorem is also useful to prove Lagrange's four-square theorem, which states that every natural number can be written as the sum of the squares of four natural numbers.

Dirichlet's theorem on simultaneous rational approximation

Minkowski's theorem can be used to prove Dirichlet's theorem on simultaneous rational approximation.

Algebraic number theory

Another application of Minkowski's theorem is the result that every class in the ideal class group of a number field K contains an integral ideal of norm not exceeding a certain bound, depending on K, called Minkowski's bound: the finiteness of the class number of an algebraic number field follows immediately.

Complexity theory

The complexity of finding the point guaranteed by Minkowski's theorem, or the closely related Blichfeldt's theorem, have been studied from the perspective of TFNP search problems. In particular, it is known that a computational analogue of Blichfeldt's theorem, a corollary of the proof of Minkowski's theorem, is PPP-complete.[4] It is also known that the computational analogue of Minkowski's theorem is in the class PPP, and it was conjectured to be PPP complete.[5]

See also

- Danzer set
- Pick's theorem
- Dirichlet's unit theorem
- Minkowski's second theorem
- Ehrhart's volume conjecture

References

1. Olds, C. D.; Lax, Anneli; Davidoff, Giuliana P. (2000). "Chapter 9: A new principle in the geometry of numbers". *The Geometry of Numbers*. Anneli Lax New Mathematical Library.

Vol. 41. Mathematical Association of America, Washington, DC. p. 120. ISBN 0-88385-643-3. MR 1817689 (https://mathscinet.ams.org/mathscinet-getitem?mr=1817689).
2. Milnor, John; Husemoller, Dale (1973). *Symmetric Bilinear Forms* (https://dx.doi.org/10.1007/978-3-642-88330-9). p. 46. doi:10.1007/978-3-642-88330-9 (https://doi.org/10.1007%2F978-3-642-88330-9). ISBN 978-3-642-88332-3.
3. Nguyen, Phong Q. (2009). "Hermite's Constant and Lattice Algorithms". *The LLL Algorithm*. Information Security and Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg. pp. 19–69. doi:10.1007/978-3-642-02295-1_2 (https://doi.org/10.1007%2F978-3-642-02295-1_2). ISBN 978-3-642-02294-4. ISSN 1619-7100 (https://www.worldcat.org/issn/1619-7100).
4. "PPP-Completeness with Connections to Cryptography" (https://eprint.iacr.org/2018/778). *Cryptology ePrint Archive: Report 2018/778*. 2018-08-15. Retrieved 2020-09-13.
5. Ban, Frank; Jain, Kamal; Papadimitriou, Christos H.; Psomas, Christos-Alexandros; Rubinstein, Aviad (2019-05-01). "Reductions in PPP" (https://www.sciencedirect.com/science/article/abs/pii/S0020019019300018). *Information Processing Letters*. **145**: 48–52. doi:10.1016/j.ipl.2018.12.009 (https://doi.org/10.1016%2Fj.ipl.2018.12.009). ISSN 0020-0190 (https://www.worldcat.org/issn/0020-0190). S2CID 71715876 (https://api.semanticscholar.org/CorpusID:71715876). Retrieved 2020-09-13.

Further reading

- Bombieri, Enrico; Gubler, Walter (2006). *Heights in Diophantine Geometry* (https://books.google.com/books?id=3ATnwmGegvsC). Cambridge University Press. ISBN 9780521712293.
- Cassels, J.W.S. (2012) [1959]. *An Introduction to the Geometry of Numbers* (https://books.google.com/books?id=XyVrCQAAQBAJ). Classics in Mathematics. Springer. ISBN 978-3-642-62035-5.
- Conway, John; Sloane, Neil J. A. (29 June 2013) [1998]. *Sphere Packings, Lattices and Groups* (https://books.google.com/books?id=5-UlBQAAQBAJ) (3rd ed.). Springer. ISBN 978-1-4757-6568-7.
- Hancock, Harris (2005) [1939]. *Development of the Minkowski Geometry of Numbers*. Dover Publications. ISBN 9780486446400.
- Hlawka, Edmund; Schoißengeier, Johannes; Taschner, Rudolf (2012) [1991]. *Geometric and Analytic Number Theory* (https://books.google.com/books?id=-vTuCAAAQBAJ). Springer. ISBN 978-3-642-75306-0.
- Lekkerkerker, C.G. (2014) [1969]. *Geometry of Numbers* (https://books.google.com/books?id=XZ7iBQAAQBAJ). Elsevier. ISBN 978-1-4832-5927-7.
- Schmidt, Wolfgang M. (1980). *Diophantine Approximation*. Lecture Notes in Mathematics. Vol. 785. Springer. doi:10.1007/978-3-540-38645-2 (https://doi.org/10.1007%2F978-3-540-38645-2). ISBN 978-3-540-38645-2. ([1996 with minor corrections])
- Wolfgang M. Schmidt.*Diophantine approximations and Diophantine equations*, Lecture Notes in Mathematics, Springer Verlag 2000.
- Siegel, Carl Ludwig (2013) [1989]. *Lectures on the Geometry of Numbers* (https://books.google.com/books?id=dyH4CAAAQBAJ). Springer-Verlag. ISBN 9783662082874.

- Schneider, Rolf (1993). *Convex Bodies: The Brunn-Minkowski Theory* (https://archive.org/details/convexbodiesbrun0000schn). Cambridge University Press. ISBN 978-0-521-35220-8.

External links

- Stevenhagen, Peter. *Number Rings*. (http://websites.math.leidenuniv.nl/algebra/ant.pdf)
- Malyshev, A.V. (2001) [1994], "Minkowski theorem" (https://www.encyclopediaofmath.org/index.php?title=Minkowski_theorem), *Encyclopedia of Mathematics*, EMS Press
- "Geometry of numbers" (https://www.encyclopediaofmath.org/index.php?title=Geometry_of_numbers), *Encyclopedia of Mathematics*, EMS Press, 2001 [1994]