Minkowski's Theorem

Manuel Eberl

July 15, 2017

Abstract

Minkowski's theorem relates a subset of $\mathbb{R}^n$, the Lebesgue measure, and the integer lattice $\mathbb{Z}^n$: It states that any convex subset of $\mathbb{R}^n$ with volume greater than 2^n contains at least one lattice point from $\mathbb{Z}^n \setminus \{0\}$, i. e. a non-zero point with integer coefficients.

A related theorem which directly implies this is Blichfeldt's theorem, which states that any subset of $\mathbb{R}^n$ with a volume greater than 1 contains two different points whose difference vector has integer components.

The entry contains a proof of both theorems.

Contents

1 Minkowski's theorem

theory *Minkowskis-Theorem*
imports *Analysis*
begin

1.1 Miscellaneous material

lemma *bij-betw-UN*:
assumes *bij-betw f A B*
shows $(\bigcup n{\in}A.\ g\ (f\ n)) = (\bigcup n{\in}B.\ g\ n)$
using *assms* **by** (*auto simp*: *bij-betw-def*)

instance *vec* :: (*countable*, *finite*) *countable*
proof
have *countable* (*UNIV* :: ('*a*, '*b*) *vec set*)
proof (*rule countableI-bij2*)
show *bij-betw vec-nth UNIV* (*Pi* (*UNIV* :: '*b set*) (λ-. *UNIV* :: '*a set*))
by (*intro bij-betwI*[*of - - - vec-lambda*]) (*auto simp*: *vec-eq-iff*)
have *countable* (*PiE* (*UNIV* :: '*b set*) (λ-. *UNIV* :: '*a set*))
by (*intro countable-PiE*) *auto*
also have (*PiE* (*UNIV* :: '*b set*) (λ-. *UNIV* :: '*a set*)) = *Pi UNIV* (λ-. *UNIV*)

by *auto*
finally show *countable* ... **.**
qed
thus ∃ *t*::('*a*, '*b*) *vec* ⇒ *nat*. *inj t*
by (*auto elim*!: *countableE*)
qed

definition *of-int-vec* **where**
of-int-vec v = (χ *i*. *of-int* (*v* $ *i*))

lemma *of-int-vec-nth* [*simp*]: *of-int-vec v* $ *n* = *of-int* (*v* $ *n*)
by (*simp add*: *of-int-vec-def*)

lemma *of-int-vec-eq-iff* [*simp*]:
(*of-int-vec a* :: ('*a* :: *ring-char-0*) ^ '*n*) = *of-int-vec b* ⟷ *a* = *b*
by (*simp add*: *of-int-vec-def vec-eq-iff*)

lemma *inj-axis*:
assumes *c* ≠ *0*
shows *inj* (λ*k*. *axis k c* :: ('*a* :: {*zero*}) ^ '*n*)
proof
fix *x y* :: '*n*
assume ∗: *axis x c* = *axis y c*
have *axis x c* $ *x* = *axis x c* $ *y*
by (*subst* ∗) *simp*
thus *x* = *y* **using** *assms*
by (*auto simp*: *axis-def split*: *if-splits*)

qed

1.2 Auxiliary theorems about measure theory

lemma *emeasure-lborel-cbox-eq'*:
  emeasure lborel (*cbox a b*) = *ennreal* ($\prod$ *e*∈*Basis*. *max 0* ((*b* − *a*) · *e*))
proof (*cases* ∀ *ba*∈*Basis*. *a* · *ba* ≤ *b* · *ba*)
  case *True*
  hence *emeasure lborel* (*cbox a b*) = *ennreal* (*prod* (*op* · (*b* − *a*)) *Basis*)
    unfolding *emeasure-lborel-cbox-eq* **by** *auto*
  also have *prod* (*op* · (*b* − *a*)) *Basis* = ($\prod$ *e*∈*Basis*. *max 0* ((*b* − *a*) · *e*))
    using *True* **by** (*intro prod.cong refl*) (*auto simp*: *max-def inner-simps*)
  finally show *?thesis* **.**
next
  case *False*
  hence *emeasure lborel* (*cbox a b*) = *ennreal 0*
    by (*auto simp*: *emeasure-lborel-cbox-eq*)
  also from *False* **have** *0* = ($\prod$ *e*∈*Basis*. *max 0* ((*b* − *a*) · *e*))
    by (*auto simp*: *max-def inner-simps*)
  finally show *?thesis* **.**
qed

lemma *emeasure-lborel-cbox-cart-eq*:
  fixes *a b* :: *real* ^ ('*n* :: *finite*)
  shows *emeasure lborel* (*cbox a b*) = *ennreal* ($\prod$ *i* ∈ *UNIV*. *max 0* ((*b* − *a*) $ *i*))
proof −
  have *emeasure lborel* (*cbox a b*) = *ennreal* ($\prod$ *e*∈*Basis*. *max 0* ((*b* − *a*) · *e*))
    unfolding *emeasure-lborel-cbox-eq'* **..**
  also have (*Basis* :: (*real* ^ '*n*) *set*) = *range* (λ*k*. *axis k 1*)
    unfolding *Basis-vec-def* **by** *auto*
  also have ($\prod$ *e*∈... *max 0* ((*b* − *a*) · *e*)) = ($\prod$ *i* ∈ *UNIV* . *max 0* ((*b* − *a*) $ *i*))
    by (*subst prod.reindex*) (*auto intro*!: *inj-axis simp*: *algebra-simps inner-axis*)
  finally show *?thesis* **.**
qed

lemma *sum-emeasure'*:
  assumes [*simp*]: *finite A*
  assumes [*measurable*]: ⋀*x*. *x* ∈ *A* ⟹ *B x* ∈ *sets M*
  assumes ⋀*x y*. *x* ∈ *A* ⟹ *y* ∈ *A* ⟹ *x* ≠ *y* ⟹ *emeasure M* (*B x* ∩ *B y*) = *0*
  shows ($\sum$ *x*∈*A*. *emeasure M* (*B x*)) = *emeasure M* ($\bigcup$ *x*∈*A*. *B x*)
proof −
  define *C* **where** *C* = ($\bigcup$ *x*∈*A*. $\bigcup$ *y*∈(*A*−{*x*}). *B x* ∩ *B y*)
  have *C*: *C* ∈ *null-sets M*
    unfolding *C-def* **using** *assms*
    by (*intro null-sets.finite-UN*) (*auto simp*: *null-sets-def*)
  hence [*measurable*]: *C* ∈ *sets M* **and** [*simp*]: *emeasure M C* = *0*
    by (*simp-all add*: *null-sets-def*)
  have ($\bigcup$ *x*∈*A*. *B x*) = ($\bigcup$ *x*∈*A*. *B x* − *C*) ∪ *C*

```
    by (auto simp: C-def)
  also have emeasure M ... = emeasure M (⋃x∈A. B x − C)
    by (subst emeasure-Un-null-set) (auto intro!: sets.Un sets.Diff)
  also from assms have ... = (∑x∈A. emeasure M (B x − C))
    by (subst sum-emeasure)
       (auto simp: disjoint-family-on-def C-def intro!: sets.Diff sets.finite-UN)
  also have ... = (∑x∈A. emeasure M (B x))
    by (intro sum.cong refl emeasure-Diff-null-set) auto
  finally show ?thesis ..
qed

lemma sums-emeasure':
  assumes [measurable]: ⋀x. B x ∈ sets M
  assumes ⋀x y. x ≠ y ⟹ emeasure M (B x ∩ B y) = 0
  shows   (λx. emeasure M (B x)) sums emeasure M (⋃x. B x)
proof −
  define C where C = (⋃x. ⋃y∈−{x}. B x ∩ B y)
  have C: C ∈ null-sets M
    unfolding C-def using assms
    by (intro null-sets-UN') (auto simp: null-sets-def)
  hence [measurable]: C ∈ sets M and [simp]: emeasure M C = 0
    by (simp-all add: null-sets-def)
  have (⋃x. B x) = (⋃x. B x − C) ∪ C
    by (auto simp: C-def)
  also have emeasure M ... = emeasure M (⋃x. B x − C)
    by (subst emeasure-Un-null-set) (auto intro!: sets.Un sets.Diff)
  also from assms have (λx. emeasure M (B x − C)) sums ...
    by (intro sums-emeasure)
       (auto simp: disjoint-family-on-def C-def intro!: sets.Diff sets.finite-UN)
  also have (λx. emeasure M (B x − C)) = (λx. emeasure M (B x))
    by (intro ext emeasure-Diff-null-set) auto
  finally show ?thesis .
qed
```

1.3 Blichfeldt's theorem

Blichfeldt's theorem states that, given a subset of $\mathbb{R}^n$ with $n > 0$ and a volume of more than 1, there exist two different points in that set whose difference vector has integer components.

This will be the key ingredient in proving Minkowski's theorem.

Note that in the HOL Light version, it is additionally required – both for Blichfeldt's theorem and for Minkowski's theorem – that the set is bounded, which we do not need.

```
proposition blichfeldt:
  fixes S :: (real ^ 'n) set
  assumes [measurable]: S ∈ sets lebesgue
  assumes emeasure lebesgue S > 1
  obtains x y where x ≠ y and x ∈ S and y ∈ S and ⋀i. (x − y) $ i ∈ ℤ
```

proof −
— We define for each lattice point in $\mathbb{Z}^n$ the corresponding cell in $\mathbb{R}^n$.
define $R :: int\ \hat{}\ 'n \Rightarrow (real\ \hat{}\ 'n)\ set$
where $R = (\lambda a.\ cbox\ (of\text{-}int\text{-}vec\ a)\ (of\text{-}int\text{-}vec\ (a + 1)))$

— For each lattice point, we can intersect the cell it defines with our set S to obtain a partitioning of S.
define $T :: int\ \hat{}\ 'n \Rightarrow (real\ \hat{}\ 'n)\ set$
where $T = (\lambda a.\ S \cap R\ a)$

— We can then translate each such partition into the cell at the origin, i. e. the unit box $R\ 0$.
define $T' :: int\ \hat{}\ 'n \Rightarrow (real\ \hat{}\ 'n)\ set$
where $T' = (\lambda a.\ (\lambda x.\ x - of\text{-}int\text{-}vec\ a)\ `\ T\ a)$
have $T'\text{-}altdef$: $T'\ a = (\lambda x.\ x + of\text{-}int\text{-}vec\ a) -`\ T\ a$ **for** a
unfolding $T'\text{-}def$ **by** *force*

— We need to show measurability of all the defined sets.
have [*measurable*, *simp*]: $R\ a \in sets\ lebesgue$ **for** a
unfolding $R\text{-}def$ **by** *simp*
have [*measurable*, *simp*]: $T\ a \in sets\ lebesgue$ **for** a
unfolding $T\text{-}def$ **by** *auto*
have $(\lambda x{::}real\hat{}'n.\ x + of\text{-}int\text{-}vec\ a) \in lebesgue \rightarrow_M lebesgue$ **for** a
using *lebesgue-affine-measurable*[*of* $\lambda\text{-}.\ 1\ of\text{-}int\text{-}vec\ a$]
by (*auto simp*: *euclidean-representation add-ac*)
from *measurable-sets*[*OF this*, *of* $T\ a\ a$ **for** a]
have [*measurable*, *simp*]: $T'\ a \in sets\ lebesgue$ **for** a
unfolding $T'\text{-}altdef$ **by** *simp*

— Obviously, the original set S is the union of all the lattice point cell partitions.

have $S\text{-}decompose$: $S = (\bigcup a.\ T\ a)$ **unfolding** $T\text{-}def$
proof *safe*
fix x **assume** x: $x \in S$
define a **where** $a = (\chi\ i.\ \lfloor x\ \$\ i \rfloor)$
have $x \in R\ a$
unfolding $R\text{-}def$
by (*auto simp*: *cbox-interval less-eq-vec-def of-int-vec-def a-def*)
with x **show** $x \in (\bigcup a.\ S \cap R\ a)$ **by** *auto*
qed

— Translating the partitioned subsets does not change their volume.
have $emeasure\text{-}T'$: $emeasure\ lebesgue\ (T'\ a) = emeasure\ lebesgue\ (T\ a)$ **for** a
proof −
have $T'\ a = (\lambda x.\ 1 *_R x + (-\ of\text{-}int\text{-}vec\ a))\ `\ T\ a$
by (*simp add*: $T'\text{-}def$)
also have $emeasure\ lebesgue\ \ldots = emeasure\ lebesgue\ (T\ a)$
by (*subst emeasure-lebesgue-affine*) *auto*
finally show *?thesis*

```
    by simp
  qed

  — Each translated partition of S is a subset of the unit cell at the origin.
  have T'-subset: T' a ⊆ cbox 0 1 for a
    unfolding T'-def T-def R-def
    by (auto simp: algebra-simps cbox-interval of-int-vec-def less-eq-vec-def)

  — It is clear that the intersection of two different lattice point cells is a null set.
  have R-Int: R a ∩ R b ∈ null-sets lebesgue if a ≠ b for a b
  proof −
    from that obtain i where i: a $ i ≠ b $ i
      by (auto simp: vec-eq-iff)
    have R a ∩ R b = cbox (χ i. max (a $ i) (b $ i)) (χ i. min (a $ i + 1) (b $ i + 1))
      unfolding inter-interval-cart R-def interval-cbox
      by (simp add: of-int-vec-def max-def min-def if-distrib cong: if-cong)
    hence emeasure lebesgue (R a ∩ R b) = emeasure lborel ...
      by simp
    also have ... = ennreal (∏ i∈UNIV. max 0 (((χ x. real-of-int (min (a $ x + 1) (b $ x + 1))) −
                                        (χ x. real-of-int (max (a $ x) (b $ x)))) $ i))
      (is - = ennreal ?P)
      unfolding emeasure-lborel-cbox-cart-eq by simp
    also have ?P = 0
      using i by (auto simp: max-def intro!: exI[of - i])
    finally show ?thesis
      by (auto simp: null-sets-def R-def)
  qed

  — Therefore, the intersection of two lattice point cell partitionings of S is also a
null set.
  have T-Int: T a ∩ T b ∈ null-sets lebesgue if a ≠ b for a b
  proof −
    have T a ∩ T b = (R a ∩ R b) ∩ S
      by (auto simp: T-def)
    also have ... ∈ null-sets lebesgue
      by (rule null-set-Int2) (insert that, auto intro: R-Int assms)
    finally show ?thesis .
  qed
  have emeasure-T-Int: emeasure lebesgue (T a ∩ T b) = 0 if a ≠ b for a b
    using T-Int[OF that] unfolding null-sets-def by blast

  — The set of lattice points ℤ^n is countably infinite, so there exists a bijection
f : ℕ → ℤ^n. We need this for summing over all lattice points.
  define f :: nat ⇒ int ^ 'n where f = from-nat-into UNIV
  have countable (UNIV :: (int ^ 'n) set) infinite (UNIV :: (int ^ 'n) set)
    using infinite-UNIV-char-0 by simp-all
  from bij-betw-from-nat-into [OF this] have f: bij f
```

by (*simp add*: *f-def*)

— Suppose all the translated cell partitions T' are disjoint.
{
assume *disjoint*: $\bigwedge a\ b.\ a \neq b \Longrightarrow T'\ a \cap T'\ b = \{\}$
— We know by assumption that the volume of S is greater than 1.
have *1* $<$ *emeasure lebesgue S* **by** *fact*
also have *emeasure lebesgue S* $=$ *emeasure lebesgue* $(\bigcup n.\ T'\ (f\ n))$
proof −
— The sum of the volumes of all the T' is precisely the volume of their union, which is *S*.
have $S = (\bigcup a.\ T\ a)$ **by** (*rule S-decompose*)
also have $\ldots = (\bigcup n.\ T\ (f\ n))$
by (*rule bij-betw-UN* [*OF f*, *symmetric*])
also have $(\lambda n.$ *emeasure lebesgue* $(T\ (f\ n)))$ *sums emeasure lebesgue* $\ldots$
by (*intro sums-emeasure' emeasure-T-Int*) (*insert f*, *auto simp*: *bij-betw-def inj-on-def*)
also have $(\lambda n.$ *emeasure lebesgue* $(T\ (f\ n))) = (\lambda n.$ *emeasure lebesgue* $(T'\ (f\ n)))$
by (*simp add*: *emeasure-T'*)
finally have $(\lambda n.$ *emeasure lebesgue* $(T'\ (f\ n)))$ *sums emeasure lebesgue S* **.**
moreover have $(\lambda n.$ *emeasure lebesgue* $(T'\ (f\ n)))$ *sums emeasure lebesgue* $(\bigcup n.\ T'\ (f\ n))$
using *disjoint* **by** (*intro sums-emeasure*)
(*insert f*, *auto simp*: *disjoint-family-on-def bij-betw-def inj-on-def*)
ultimately show *?thesis*
by (*auto simp*: *sums-iff*)
qed
— On the other hand, all the translated partitions lie in the unit cell *cbox 0 1*, so their combined volume cannot be greater than 1.
also have *emeasure lebesgue* $(\bigcup n.\ T'\ (f\ n)) \leq$ *emeasure lebesgue* (*cbox 0* (*1* :: *real* ^ *'n*))
using *T'-subset* **by** (*intro emeasure-mono*) *auto*
also have $\ldots =$ *1*
by (*simp add*: *emeasure-lborel-cbox-cart-eq*)
— This leads to a contradiction.
finally have *False* **by** *simp*
}
— Therefore, there exists a point that lies in two different translated partitions, which obviously corresponds two two points in the non-translated partitions whose difference is the difference between two lattice points and therefore has integer components.
then obtain *a b x* **where** $a \neq b\ x \in T'\ a\ x \in T'\ b$
by *auto*
thus *?thesis*
by (*intro that*[*of x* + *of-int-vec a x* + *of-int-vec b*])
(*auto simp*: *T'-def T-def algebra-simps*)
qed

1.4 Minkowski's theorem

Minkowski's theorem now states that, given a convex subset of $\mathbb{R}^n$ that is symmetric around the origin and has a volume greater than 2^n, that set must contain a non-zero point with integer coordinates.

theorem *minkowski*:
  fixes B :: (*real* ^ 'n) *set*
  assumes *convex* B **and** *symmetric*: *uminus* ‘ $B \subseteq B$
  assumes *meas-B* [*measurable*]: $B \in$ *sets lebesgue*
  assumes *measure-B*: *emeasure lebesgue* $B >$ *2* ^ *CARD*('n)
  obtains x **where** $x \in B$ **and** $x \neq 0$ **and** $\bigwedge i.\ x\ \$\ i \in \mathbb{Z}$
proof −
  — We scale B with $\frac{1}{2}$.
  define B' **where** $B' = (\lambda x.\ 2 *_R x) -‘ B$
  have *meas-B'* [*measurable*]: $B' \in$ *sets lebesgue*
    using *measurable-sets*[*OF lebesgue-measurable-scaling*[*of 2*] *meas-B*]
    by (*simp add*: *B'-def*)
  have *B'-altdef*: $B' = (\lambda x.\ (1/2) *_R x)$ ‘ B
    unfolding *B'-def* **by** *force*

  — The volume of the scaled set is 2^n times smaller than the original set, and therefore still has a volume greater than 1.
  have *1* < *ennreal* ((*1* / *2*) ^ *CARD*('n)) ∗ *emeasure lebesgue B*
  proof (*cases emeasure lebesgue B*)
    case (*real x*)
    have *ennreal* (*2* ^ *CARD*('n)) = *2* ^ *CARD*('n)
      by (*subst ennreal-power* [*symmetric*]) *auto*
    also from *measure-B* **and** *real* **have** ... < *ennreal x* **by** *simp*
    finally have (*2* ^ *CARD*('n)) < *x*
      by (*subst* (*asm*) *ennreal-less-iff*) *auto*
    thus *?thesis*
      using *real* **by** (*simp add*: *ennreal-1* [*symmetric*] *ennreal-mult'* [*symmetric*]
                ennreal-less-iff field-simps del: *ennreal-1*)
  qed (*simp-all add*: *ennreal-mult-top*)
  also have ... = *emeasure lebesgue B'*
    unfolding *B'-altdef* **using** *emeasure-lebesgue-affine*[*of 1/2 0 B*] **by** *simp*
  finally have ∗: *emeasure lebesgue B'* > *1* **.**

  — We apply Blichfeldt's theorem to get two points whose difference vector has integer coefficients. It only remains to show that that difference vector is itself a point in the original set.
  obtain *x y*
    where *xy*: $x \neq y\ x \in B'\ y \in B' \bigwedge i.\ (x - y)\ \$\ i \in \mathbb{Z}$
    by (*erule blichfeldt* [*OF meas-B'* ∗])
  hence *2* ∗$_R$ *x* ∈ *B* *2* ∗$_R$ *y* ∈ *B* **by** (*auto simp*: *B'-def*)
  — Exploiting the symmetric of B, the reflection of *2* ∗$_R$ *y* is also in B.
  moreover from *this* **and** *symmetric* **have** −(*2* ∗$_R$ *y*) ∈ *B* **by** *blast*
  — Since B is convex, the mid-point between *2* ∗$_R$ *x* and − *2* ∗$_R$ *y* is also in B, and that point is simply $x - y$ as desired.

```
  ultimately have (1 / 2) *R 2 *R x + (1 / 2) *R (- 2 *R y) ∈ B
    using ‹convex B› by (intro convexD) auto
  also have (1 / 2) *R 2 *R x + (1 / 2) *R (- 2 *R y) = x - y
    by simp
  finally show ?thesis using xy
    by (intro that[of x - y]) auto
qed

end
```

References

[1] E. Dummit. Number Theory: The Geometry of Numbers. https://web.math.rochester.edu/people/faculty/edummit/docs/numthy_7_geometry_of_numbers.pdf, 2014.