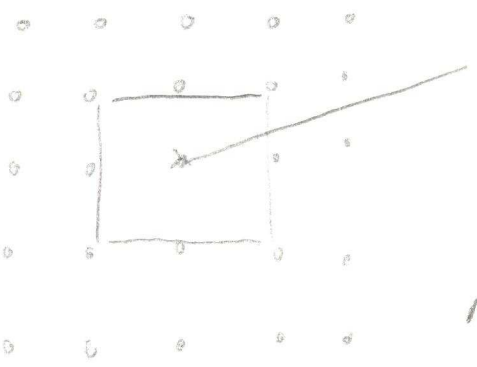
Now: Example for discrete Problem!

Lattices and Minkowski's Theorem

Ref.: Jiří Matoušek:
Lectures on Discrete Geometry (Chap. 2)

Question: Regular family of discrete sets



Can you see
an inside to point?
Or does any lie
at same time?

For $\mathrm{vol}(C) \leq 4$
the theorem might not hold!

Theorem (Minkowski's theorem)

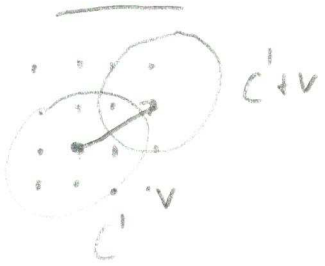
Let $C \subseteq \mathbb{R}^d$ be symmetric (around the origin, i.e. $C = -C$),
convex and bounded. Suppose that $\mathrm{vol}(C) > 2^d$.
Then C contains at least one lattice point different from 0.
(Tight)

Proof: Let $C' := \frac{1}{2}C = \{\frac{1}{2}x \mid x \in C\}$

Claim: There exists a non-zero integer vector $v \in \mathbb{Z}^d \setminus \{0\}$
with $C' \cap (C' + v) \neq \emptyset$

(Translation with v)

Situation:

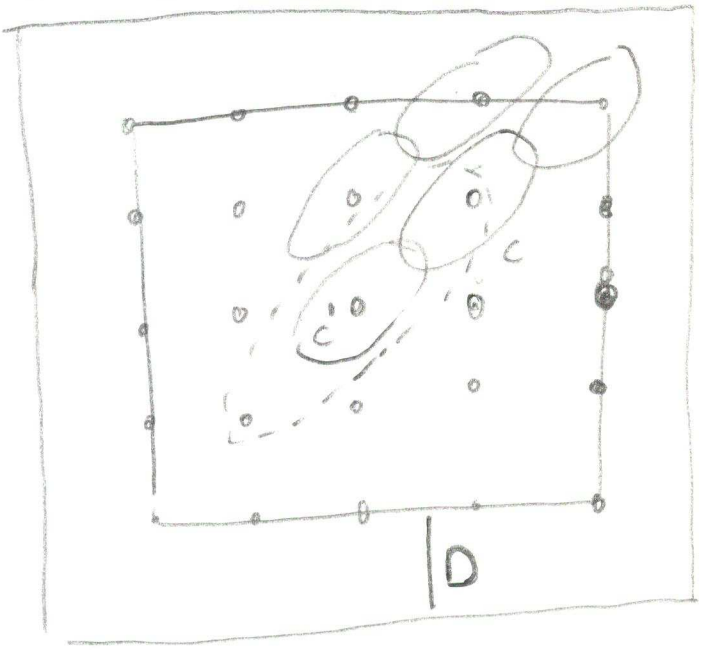


By calculation:

Assume $C' \cap (C'+v) = \emptyset$

For all $v \in \mathbb{Z}^d \setminus \{0\}$

Consider the family C_T of translates of C' in a cube $[-R,R]^d$ $\quad C_T = \{C'+v \mid v \in [-R,R]^d \cap \mathbb{Z}^d\}$



Each such translate is disjoint from C'.

Every two of them are disjoint.

All contained in the cube K $[-R-D, R+D]^d$

with $D :=$ Diameter of (C')

Now: $\mathrm{vol}(K) = (2R+2D)^d \geq |C_T| \,\mathrm{vol}(C') = (2R+1)^d \,\mathrm{vol}(C')$

$$\Leftrightarrow \quad \mathrm{vol}(C') \leq \left(1 + \frac{2D-1}{2R+1}\right)^d$$

$R \to \infty$ Right hand side goes to 1

but $\quad \mathrm{vol}(C') = \frac{\mathrm{vol}(C)}{2^d} > 1$ ↯

Claim holds! Now our proof!

Let $v \in \mathbb{Z}^d \setminus \{0\}$ and $x \in C' \cap (C'+v)$

$$\Rightarrow \quad x - v \in C' \Rightarrow v - x \in C' \Rightarrow \overline{x\,(v-x)} \subseteq C'$$

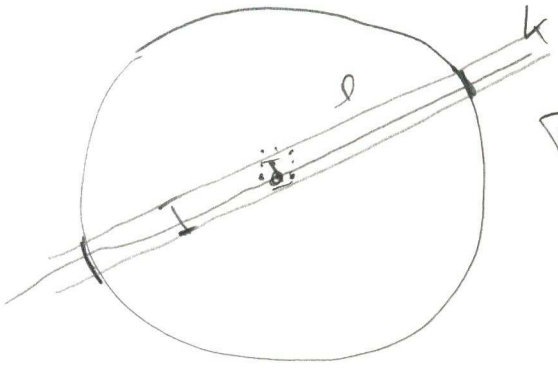
(sym. of C'; conv. of C')

$\Rightarrow$ M.d point $\frac{1}{2}x + \frac{1}{2}(v-x) = \frac{1}{2}v \in C'$

$\Rightarrow v \in C$ ∎

Example:

Regular Forest: (circular)



Diameter 26 meters

Trees of diameter 0.16

You cannot see outside from the origin!

Consider strip S of width 0.16 with l as middle line

$C = K \cap S$ contains no lattice point?

Compute $\text{vol}(C)$; $\text{vol}(C) > 4$!

$\Rightarrow$ C contains a lattice point!

Remark: C symmetric necessary !

C contains 0 necessary !

C bounded not necessary !

Arbitrary long sets without lattice point.

Application of Theorem 7 (Minkowski's Theorem)

Also non-geometric (number theory) surprisingly!

Dirichlet Theorem also helps for the regular forest problem

Theorem 8 (Dirichlet)

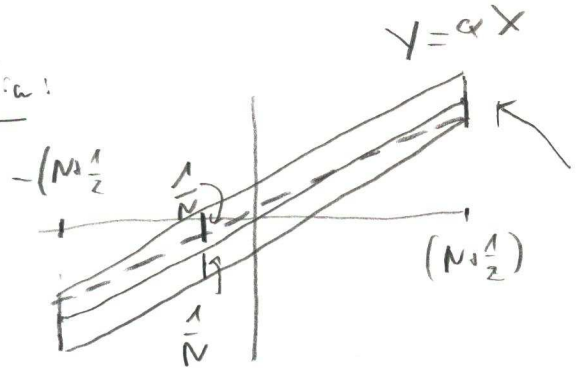
Let $\alpha \in \mathbb{R}$. Then there are infinitely many $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $\left|\alpha - \frac{m}{n}\right| < \frac{1}{n^2}$.

(Approximation of reals with rational numbers and quadratic bound)

Proof: Claim $\forall N \in \mathbb{N}\ \exists m \in \mathbb{Z}, n \in \mathbb{N}$ with $\left|\alpha - \frac{m}{n}\right| < \frac{1}{nN}$ with $n \leq N$

We consider the set $C := \{(x,y) \in \mathbb{R}^2 \mid -(N+\frac{1}{2}) \leq x \leq N+\frac{1}{2},\ |\alpha x - y| < \frac{1}{N}\}$

Situation:



Triangle Value:

$$\frac{gh}{2} = \frac{2}{N}(2N+1)/2$$

$\Rightarrow$ C fulfills conditions of Theorem 7 (convex, symmetric, bounded)

$$\mathrm{vol}(C) = (2N+1)\frac{2}{N} > 4$$

$\Rightarrow$ C contains a lattice point

$\uparrow$ $(n,m) \neq (0,0)$

Min.

$\Rightarrow$ o.E. $n > 0$ $\quad n \leq N$ clear

(Symmetry)

$\Rightarrow$ $|\alpha n - m| < \frac{1}{N}$ $\Rightarrow$ $|\alpha - \frac{m}{n}| < \frac{1}{nN}$

Def C

□

(Proof Claim)

Now the main proof:

$\alpha \in \mathbb{Q} \Rightarrow \alpha = \frac{m}{n}$ $\quad |\alpha - \frac{mn}{nn}| = 0 < \frac{1}{(nn)^2}$ trivial ✓

So $\alpha \in \mathbb{R} \setminus \mathbb{Q}$:

From the claim above $|\alpha - \frac{m}{n}| < \frac{1}{nN} \leq \frac{1}{n^2}$ $\quad n \leq N$

(For every N there is such a pair (n,m))

Infinitely many?

Suppose there are only finitely many pairs

$(n_1, m_1), \dots, (n_k, m_k)$ with $|\alpha - \frac{m_i}{n_i}| < \frac{1}{(n_i)^2}$

Let N go to infinity, then one pair (say (n_1, m_1)) appears infinitely many times. Use a subsequence $N_s \to \infty$

$|\alpha - \frac{m_1}{n_1}| < \frac{1}{n_1 N_s} \underset{s \to \infty}{\Rightarrow} \alpha = \frac{m_1}{n_1} \in \mathbb{Q}$ ↯

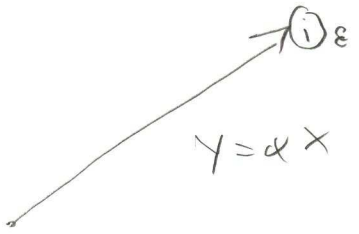
There are infinitely many such pairs ✓

□

Example:

Now a general solution for the regular fast problem with infinite ports!

Let $Y = \alpha X$ be the Visibility beam



$\Rightarrow$ there are arbitrary great n, m with

w.l.o.g.

$$|\alpha - \frac{m}{n}| < \frac{1}{n^2} \iff |n\alpha - m| < \frac{1}{n} \leq \varepsilon$$

Choose n big enough!

Generalization for arbitrary lattices! (different from $\mathbb{Z}^d$)

Regular lattice with linear independent vectors

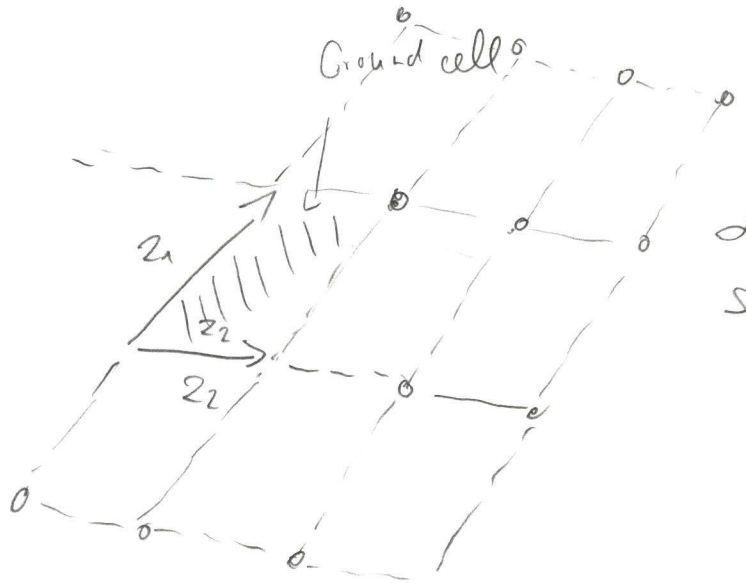
$z_1, \dots, z_d \in \mathbb{R}^d$ linearly independent

Definition 9 $\quad \Gamma := \{\alpha_1 z_1 + \dots + \alpha_d z_d \,;\, \alpha_1, \dots \alpha_d \in \mathbb{Z}\}$

is the lattice spanned by $z_1, \dots, z_d$

$\mathrm{Vol}(\Gamma) := \mathrm{vol}(\{x_1 z_1 + \dots + x_d z_d \mid 0 \leq x_i \leq 1 \ \forall i\})$ is the volume of the ground cell.

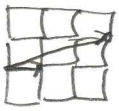
Example 2-D:



Lattice spanned by z_1, z_2

Some remarks:

I. Volume of ground cell independent from the basis

Example  $\mathbb{Z}^2$ Different Basis 1: $(1,0), (3,1)$ Basis 2: $(1,0), (0,1)$

II. Volume of the ground cell = Det. of basis vectors

Example: $\mathrm{Vol}\left(\left\{x_1\begin{pmatrix}1\\0\end{pmatrix} + x_2\begin{pmatrix}3\\1\end{pmatrix} \mid 0 \le x_{1,2} \le 1\right\}\right)$

$= \left|\det\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}\right| = 1$

Theorem 10 (general Minkowski Theorem) (without proof)

Let Γ be a general lattice of dimension d. Let $C \subseteq \mathbb{R}^d$ be convex, bounded and symmetric around 0.

$\mathrm{vol}(C) > 2^d \mathrm{vol}(\Gamma) \Rightarrow C$ contains a point of $\Gamma \setminus \{0\}$

Application in number theory.

Stands for its own.

Theorem 11 (Two square theorem)

Each prime $p \equiv 1 \bmod 4$ (5, 13, 17, ... so on)

can be written as a sum of two squares $p = a^2 + b^2$, $a, b \in \mathbb{Z}$.

Uses:

Lemma 12 If $p \equiv 1 \bmod 4$ then -1 is a quadratic residue modulo p, i.e. there is m with

$$m^2 \equiv -1 \bmod p$$

Proof: $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$

Only $-\bar{1}$ and $\bar{1}$ fulfill $(\,)^2 = \bar{1}$ (now omit $\bar{\cdot}$)

$\Rightarrow$ For all $a \neq \pm 1$ we have $a \neq a^{-1}$

$\Rightarrow$ Pairs (a, a^{-1}) for $a \neq 1, -1$ have two elements

We have $(p-1)! = 1 \cdot 2 \cdot 3 \cdots p-1 = 1 \cdot -1 \cdot a_1 a_1^{-1} \cdots a_r a_r^{-1} \equiv -1 \bmod p$

$$r = \frac{p-3}{2}$$

Assume the $i^2 = -1$ has no solution in $\mathbb{Z}_p$.

$\Rightarrow$ $a(-a^{-1}) = -1$ but $a \neq -a^{-1}$

$\Rightarrow$ Subdivide the $p-1$ elements in $\frac{p-1}{2}$ pairs
↑ even number

$(a, -a^{-1})$

$\Rightarrow (p-1)! = (-1)^{\frac{p-1}{2}} = 1$ ↯ □

Proof of Theorem 11:

We choose a number q so that $q^2 \equiv -1 \bmod p$ by the Lemma!

Lattice Γ with $z_1 = (1, q)$ $z_2 = (0, p)$

$$\mathrm{vol}(\Gamma) = \begin{vmatrix} 1 & 0 \\ q & p \end{vmatrix} = p$$

Minkowski's Theorem for general lattices

C convex, bounded, symmetric $\mathrm{vol}(C) > 2^d \mathrm{vol}(\Gamma)$

$C = \{(x,y) \in \mathbb{R}^2,\ x^2 + y^2 < 2p\} = \bigcup_{\sqrt{2p}} (0,0)$ (open circle)

$\mathrm{vol}(C) = 2p\,\pi = \pi r^2 > 4p = 2^d \mathrm{vol}(\Gamma)$

$\Rightarrow$ C contains a lattice point $0 \neq (a,b)$
↑ Min.

with $(a,b) = i z_1 + j z_2$
$= (i,\ iq + jp)$ (Basis)

$a^2 + b^2 = i^2 + i^2 q^2 + 2ijpq + j^2 p^2 \equiv i^2 (1 + q^2) \bmod p$
$\equiv 0 \bmod p$

$a^2 + b^2 < 2p$ (C. el.) $\Rightarrow$ $p = a^2 + b^2$ □

Some remarks

- $p = 7 \equiv 3 \bmod 4$ no way
- $2 \neq p = a^2 + b^2 \Rightarrow p \equiv 1 \bmod 4$
- Lagrange: Any $n \in \mathbb{N}$ as a sum of 4 quadratic expressions

  $n = a^2 + b^2 + c^2 + d^2$ (Similar approach)

Incidence Problems (Cap. 4 Matoušek)

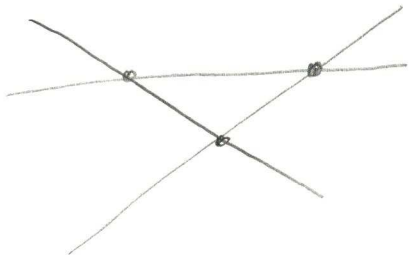
Point–line incidences

Set P of n points
Set L of n lines

Incidences: pairs (p, l) so that $p \in P$ and $l \in L$ and p lies on l

Number of such incidences: $I(P, L)$

$$I(m, n) := \max_{\substack{P, L \\ |P| = m \\ |L| = n}} I(P, L)$$



$I(3,3) \geq 6$

$I(m, n) \leq m \cdot n$ trivial

Theorem 13 (Szemerédi-Trotter)

For all $m, n \geq 1$ we have $I(m,n) = O(m^{\frac{2}{3}} n^{\frac{2}{3}} + m + n)$.

This bound is asymptotically tight.

Tightness for $I(n,n)$.

Lemma 14 We have $I(n,n) = \Omega(n^{4/3})$

So $I(m,n)$ in the above Theorem is tight.

Proof: Construction $n = 4k^3$ for $k \in \mathbb{N}$

Grid $k \times 4k^2$

$$P = \{(i,j) : i = 0, 1, \ldots, k-1,\ j = 0, 1, \ldots, 4k^2 - 1\}$$

$$L = \{ y = ax + b \mid a = 0, 1, \ldots, 2k-1,\ b = 0, 1, \ldots 2k^2 - 1 \}$$

$4k^3$ lines, $4k^3$ points

$x \in [0,k)$ we have $ax + b \leq ak + b \leq 2k^2 + 2k^2 = 4k^2$

($a \geq 0$; $a < 2k-1$, $b < 2k^2 - 1$)

Thus for, for each $i = 0, 1, \ldots, k-1$ $ax + b \in L$ has point $(i, ai + b) \in P$

$$I(P,L) \geq k \cdot |L| = \frac{1}{4} n^{\frac{4}{3}}$$

□

Graph $G = (V, E)$

Arc: Injective mapping $[0,1] \to \mathbb{R}^2$

Drawing of G: assign each $v \in V$ a unique point $v_p \in \mathbb{R}^2$
(geometric realisation) assign an arc to each edge $(v,w) \in E$
arc does not meet other vertices

Crossing number of a drawing of G:
# of crossings in the drawing

$\binom{k}{2}$ - times

Planar graph: $:\Leftrightarrow$ crossing number is 0

Crossing number of G is the smallest possible crossing number of a drawing of G

denoted by $cr(G)$