Covering convex bodies and the closest vector problem

Márton Naszódi
Alfréd Rényi Inst. of Math. and Eötvös Univ., Budapest

joint with

Moritz Venzin
EPFL, Lausanne

Closest Vector Problem (CVP)

Given a lattice $\Lambda = \{Ax \ : \ x \in \mathbb{Z}^n\}$, with $A \in \mathbb{Q}^{n\times n}$ and a target $t \in \mathbb{Q}^n$.

Find a closest vector in Λ to t with respect to **a given norm**.

Exact solution: NP-hard for ℓ_p for any $p \in [1, \infty]$.

$(1+\varepsilon)$-**approximate CVP solver** for a norm: find a $v \in \Lambda$ with $\|t - v\| \leq (1+\varepsilon) \times$ (the minimum).

Notation: $(1+\varepsilon)$-CVP$_K$, or for ℓ_p^n, $(1+\varepsilon)$-CVP$_p$.

Approximate CVP solvers

Blömer – Naewe '09 extended the algorithm of Ajtai, Kumar and Sivakumar to solve $(1+\varepsilon)$-CVP$_p$ for all p. TIME $O(1/\varepsilon)^{2n}$.

Dadush '12 extended the Ajtai–Kumar–Sivakumar sieve to solve $(1+\varepsilon)$-CVP in any norm. TIME $O(1/\varepsilon)^{2n}$.

For ℓ_2: better results.

Eisenbrand – Hähnle – Niemeier '11: For $p=\infty$ boosted the Blömer–Naewe-algorithm for $(1+\varepsilon)$-CVP$_\infty$. TIME $O(\log(1+1/\varepsilon))^n$.
Main idea: a covering problem to do *divide and conquer*.

Dadush – Kun '16: Using lattice sparsification, deterministic algorithm for $(1+\varepsilon)$-CVP for any norm. TIME $2^{O(n)}(1/\varepsilon)^n$.

Definition 1

$K \subseteq \mathbb{R}^n$ a convex body.

Definition: $(2, \varepsilon)$-covering

A sequence of convex bodies $\{Q_i\}_{i=1}^N$ is a $(2, \varepsilon)$-*covering* of K if

$$K \subseteq \bigcup_{i=1}^{N} Q_i \subseteq \bigcup_{i=1}^{N} 2 \odot Q_i \subseteq (1+\varepsilon)K,$$

where $2 \odot Q$ means: enlarge Q by factor 2 about the centroid.

Definition 1

$K \subseteq \mathbb{R}^n$ a convex body.

Definition: $(2, \varepsilon)$-covering

A sequence of convex bodies $\{Q_i\}_{i=1}^N$ is a $(2, \varepsilon)$-*covering* of K if

$$K \subseteq \bigcup_{i=1}^N Q_i \subseteq \bigcup_{i=1}^N 2 \odot Q_i \subseteq (1+\varepsilon)K,$$

where $2 \odot Q$ means: enlarge Q by factor 2 about the centroid.

Easy:

- If $\mathrm{centroid}(K) = o$ than K has a $(2, \varepsilon)$-covering by $(\frac{10}{\varepsilon})^n$ translates of $\frac{\varepsilon}{2}(K \cap -K)$.
- By loosing a 10^n factor, we may restrict to centrally symmetric Q_i.

A lower bound: $\mathbf{B}_2^n$ needs $2^{-O(n)}(1/\varepsilon)^{(n-1)/2}$ bodies.

Definition 2

$K \subseteq \mathbb{R}^n$ a convex body. Assume $K = -K$.

Definition: modulus of smoothness

The *modulus of smoothness* of K is the function

$$\rho_K(\tau) = \frac{1}{2} \sup_{\|x\|_K = \|y\|_K = 1} \left(\|x + \tau y\|_K + \|x - \tau y\|_K - 2 \right).$$

Easy: $\rho_K(\tau) \le \tau$ for any K (subadditivity of $\|\cdot\|$).

Key example: Assume $\rho_K(\tau) \le \tau^2$. Let y be parallel to a tangent of K at x, and $\tau = \sqrt{\varepsilon}$.
Then, $\|x + \tau y\|_K, \|x - \tau y\|_K \ge 1$, and hence

$$\boxed{\|x + \tau y\|_K \le 1 + 2\varepsilon.}$$

Main results: Good mod. of smooth. $\Longrightarrow$ good covering

Theorem

If K has modulus of smoothness $\leq C\tau^q$, then there is a $(2, \varepsilon)$-covering of K using $C^{O(n)}(\frac{1}{\varepsilon})^{n/q}$ convex bodies.

Corollary: There is a $(2, \varepsilon)$-covering for ℓ_p balls using $2^{O(n)}(\frac{1}{\varepsilon})^{n/2}$ bodies for $p \geq 2$ and $2^{O(n)}(\frac{1}{\varepsilon})^{n/p}$ for $p \in [1, 2]$.

Sharp: matching lower bound for the ℓ_2^n (ie., Euclidean) ball.

Main results: Good covering $\Longrightarrow$ Fast approx. CVP solver

Theorem (Boosting 2-CVP by a $(2, \varepsilon)$-covering)

Given a $(2, \varepsilon)$-covering of K with N bodies. Then we can solve the $(1 + 7\varepsilon)$-CVP$_K$ with $O\left(N \log(\frac{1}{\varepsilon})(\log(n) + \log(b))\right)$ calls to a 2-approximate CVP solver for general norms, where b is the input length.

Main results: Good covering $\Longrightarrow$ Fast approx. CVP solver

Theorem (Boosting 2-CVP by a $(2,\varepsilon)$-covering)

Given a $(2,\varepsilon)$-covering of K with N bodies. Then we can solve the $(1+7\varepsilon)$-CVP_K with $O\left(N\log(\frac{1}{\varepsilon})(\log(n)+\log(b))\right)$ calls to a 2-approximate CVP solver for general norms, where b is the input length.

Corollary: Fast approx. CVP solver for ℓ_p

We have a simple, randomized $(1+\varepsilon)$-CVP_p algorithm for $1 \le p \le \infty$.
TIME $2^{O(n)}\left(\frac{1}{\varepsilon}\right)^{n/2}$ for $p \ge 2$, and $2^{O(n)}(\frac{1}{\varepsilon})^{n/p}$ for $p \in [1,2]$.

Compare with Dadush – Kun, where TIME is $2^{O(n)}(1/\varepsilon)^n$, but works for any norm.

Good modulus $\Longrightarrow$ Good covering :: Proof

$K = -K \subset \mathbb{R}^n$ convex body.

Assume $\rho_K(\tau) \leq C\tau^q$

Then, there is a $(2, \varepsilon)$-covering with

$$2^{O(n)} \log(1/\varepsilon) \left(\frac{C}{\varepsilon}\right)^{n/q} + O(C)^{n/(q-1)}$$

bodies.

Good modulus $\Longrightarrow$ Good covering :: Proof

$K = -K \subset \mathbb{R}^n$ convex body.

Assume $\rho_K(\tau) \leq C\tau^q$

Then, there is a $(2, \varepsilon)$-covering with

$$2^{O(n)} \log(1/\varepsilon) \left(\frac{C}{\varepsilon}\right)^{n/q} + O(C)^{n/(q-1)}$$

bodies.

For simplicity: Assume $\rho_K(\tau) \leq \tau^2$.

$\delta :=$ roughly $\sqrt{\varepsilon}$. May assume $\delta - \varepsilon \geq \delta/2$.

First, we give a $(2, \varepsilon)$-covering of K in the neighborhood of a point.

Then, using a packing argument, we extend this construction to obtain a $(2, \varepsilon)$-covering for K.

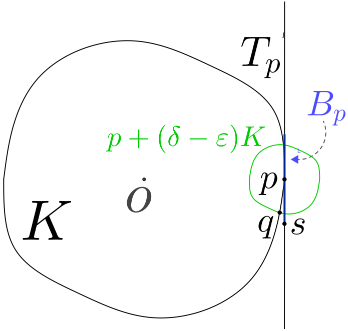
Proof cont'd

Fix $p \in \operatorname{bd} K$. T_p: a supporting hyperplane of K at p.
$B_p := \{x \in T_p \ : \ \|x - p\| \leq \delta\}$.
Claim: $\operatorname{bd} K \cap (p + (\delta - \varepsilon)K) \subseteq \operatorname{conv}(0, B_p)$.

Indeed, let $q \in \operatorname{bd} K \cap (p + (\delta - \varepsilon)K)$, and let
L: the two-dim linear plane spanned by p, q.

s: the lower end point of $L \cap B_p$.

$s' := s / \|s\| \in \operatorname{bd} K$.



Proof cont'd

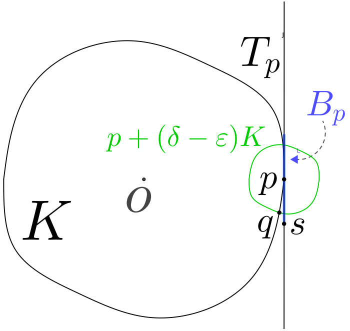
Fix $p \in \operatorname{bd} K$. T_p: a supporting hyperplane of K at p.
$B_p := \{x \in T_p \ : \ \|x - p\| \le \delta\}$.
Claim: $\operatorname{bd} K \cap (p + (\delta - \varepsilon)K) \subseteq \operatorname{conv}(0, B_p)$.

Indeed, let $q \in \operatorname{bd} K \cap (p + (\delta - \varepsilon)K)$, and let
L: the two-dim linear plane spanned by p, q.
s: the lower end point of $L \cap B_p$.
$s' := s / \|s\| \in \operatorname{bd} K$.

Mod. of smooth.: $\|s - s'\| \le \varepsilon$.
$\Rightarrow \ \|s' - p\| \ge \delta - \varepsilon = \|q - p\|$.

By *monotonicity*, s' is clockwise further from p than q from p.

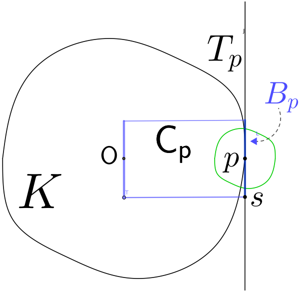
$\checkmark_{\text{Claim}}$



Still thaaat Proof (sorry!)

Instead of the cone conv$(0, B_p)$, we take the cylinder

$$C_p = B_p + [0, -p] \supset \mathrm{conv}(0, B_p).$$



Assume $\varepsilon = 2^{-k}$. Logarithmic slicing of the cylinder: k slices
$0 =$ origin to $1/2$; $1/2$ to $3/4$; $3/4$ to $7/8$; ...; $1 - \varepsilon$ to $1 = p$.

Easy: these slices enlarged by 2 are in $(1 + \varepsilon)K$.

Still thaaat Proof (sorry!)

Local to global: Take a net of $\delta - \varepsilon \approx \sqrt{\varepsilon}$ fineness of bd K. This is of size roughly

$$2^{O(n)} \left(\frac{1}{\varepsilon}\right)^{n/2}.$$

Take the cones, then the cylinders, and finally the sliced cylinders for each.

Total number of pieces: $2^{O(n)} \left(\frac{1}{\varepsilon}\right)^{n/2} \log(1/\varepsilon)$ $\square$

Good covering $\Longrightarrow$ Fast $(1+\varepsilon)$-CVP

Theorem (Boosting 2-CVP by a $(2,\varepsilon)$-covering)

Given a $(2,\varepsilon)$-covering of K with N bodies. Then we can solve the $(1+7\varepsilon)$-CVP_K with $O\left(N \log(\frac{1}{\varepsilon})(\log(n)+\log(b))\right)$ calls to a 2-approximate CVP solver for general norms, where b is the input length.

Good covering $\implies$ Fast $(1+\varepsilon)$-CVP

Theorem (Boosting 2-CVP by a $(2,\varepsilon)$-covering)

Given a $(2,\varepsilon)$-covering of K with N bodies. Then we can solve the $(1+7\varepsilon)$-CVP$_K$ with $O\left(N\log(\frac{1}{\varepsilon})(\log(n)+\log(b))\right)$ calls to a 2-approximate CVP solver for general norms, where b is the input length.

We may assume

- $$n^{-3/2}B_2^n \subseteq K \subseteq B_2^n.$$
- $$1 \leq \min_{x\in\Lambda(A)} \|x-t\|_K \leq n^{5/2}2^{(n^2+n)b}.$$

Good covering $\Longrightarrow$ Fast $(1+\varepsilon)$-CVP :: Proof

We assume

$$1 \le \min_{x \in \Lambda(A)} \|x - t\|_K \le 2^{n^2 b}. \qquad (1)$$

$(2,\varepsilon)$-covering : $K \subseteq \{c_i + Q_i\}_{i=1}^N$, where $Q_i = -Q_i$.

Goal: Find $f \in \mathbb{Z}$ such that $c_i + (1+\varepsilon)^f Q_i$ contains a lattice vector for some $i \in [N]$, but $c_i + (1+\varepsilon)^{f-1} Q_i$ contains no lattice vector for any $i \in [N]$.

Good covering $\Longrightarrow$ Fast $(1+\varepsilon)$-CVP :: Proof

We assume

$$1 \le \min_{x \in \Lambda(A)} \|x - t\|_K \le 2^{n^2 b}. \tag{1}$$

$(2,\varepsilon)$-covering : $K \subseteq \{c_i + Q_i\}_{i=1}^N$, where $Q_i = -Q_i$.

Goal: Find $f \in \mathbb{Z}$ such that $c_i + (1+\varepsilon)^f Q_i$ contains a lattice vector for some $i \in [N]$, but $c_i + (1+\varepsilon)^{f-1} Q_i$ contains no lattice vector for any $i \in [N]$.

By (1),

$$L := 0 \le f \le \log_{1+\varepsilon}\left(2^{n^2 b}\right) =: U.$$

Algorithm: binary search for f:
Call the Dadush – Kun (or any other) algorithm with $\varepsilon = 1$ for each $i \in [N]$ at each iteration. $\square$

Binary search for f

1. Initialize $L := 0$, $U := \log_{1+\varepsilon}\left(2^{n^2 b}\right)$.
2. While $U - L \geq 4$ do
    2.1 For all $i \in [N]$, solve a 2-approximate $\mathrm{CVP}_{(1+\varepsilon)^{L+(U-L)/2} Q_i}$ problem with target $t - (1+\varepsilon)^{L+(U-L)/2} c_i$.
    2.2 If a $v \in \Lambda$ is returned, update $U := \log_{1+\varepsilon} \|v - t\|_K$ and $x := v$.
    2.3 Otherwise, update $L := L + (U - L)/2$.
3. Return x.

A seemingly unrelated

question

Is there a convex polytope P with

$$(1-\varepsilon)\mathbf{B}_2^n \subseteq P \subseteq \mathbf{B}_2^n$$

A seemingly unrelated

question

Is there a convex polytope P with

$$(1-\varepsilon)\mathbf{B}_2^n \subseteq P \subseteq \mathbf{B}_2^n$$

of *combinatorial complexity* (ie., total number of all dimensional faces)

$$2^{O(n)}\left(\frac{1}{\varepsilon}\right)^{n/2}?$$

Thank you!