A polynomial time CVP algorithm for lattices related to zonotopes

Frank Vallentin

University of Cologne, Germany

joint work with Tom McCormick, Britta Peis, and Robert Scheidweiler



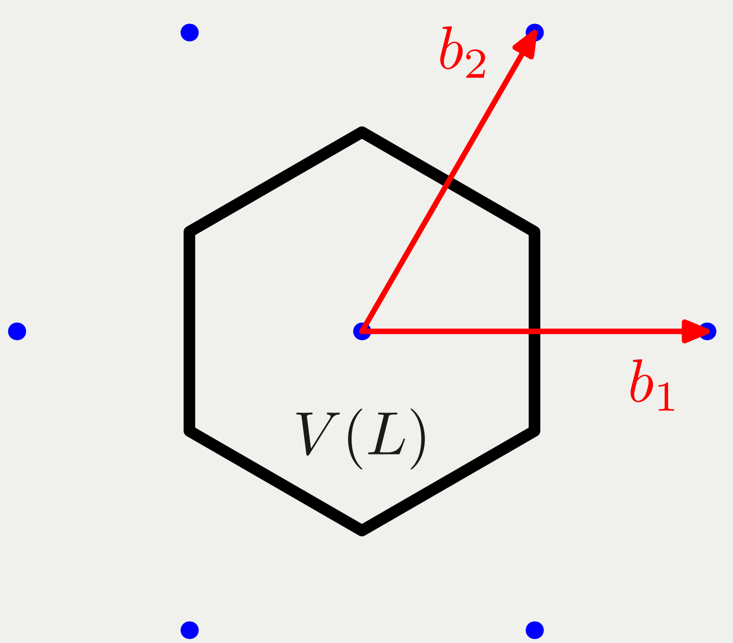
February 20, 2020

The closest vector problem

Input: Lattice $L = \left\{ \sum_{i=1}^{r} \alpha_i b_i : \alpha_i \in \mathbb{Z} \right\} \subseteq \mathbb{R}^n$ given by basis $b_1, \ldots, b_r$, and vector $x \in \mathbb{R}^n$ (wlog $x \in \operatorname{span} L$)

Output: lattice vector $u \in L$ with $|x - u| = \min_{v \in L} |x - v|$

Geometric interpretation:



Voronoi cell

$V(L) = \{x \in \mathbb{R}^n : |x| \leq |x - v| \text{ for } v \in L\}$

$V(L)$ tiles $\mathbb{R}^n$ by lattice translates $v + V(L)$

CVP: In which tile $u + V(L)$ does x lie?

Some words about algorithms and complexity

CVP has been studied intensively. Collection of important results:

CVP is NP-hard (van Emde Boas, 1981)

CVP is NP-hard to approximate within a factor $n^{c/\log\log n}$ for $c > 0$
(Dinur, Kindler, Raz, Safra, 2003)

Approximating CVP within a factor of $\sqrt{n}$ lies in NP $\cap$ co-NP.
(Aharonov, Regev, 2005)

$\tilde{O}(4^n)$-time, $\tilde{O}(2^n)$-space algorithm for exact CVP
(Micciancio, Voulgaris, 2013)

$2^{n+o(1)}$-time and space algorithm for exact CVP
(Aggarwal, Dadush, Stephens-Davidowitz, 2015)

If $V(L)$ compactly representable: reduced space complexity of MV algorithm
(Hunkenschröder, Reuland, Schymura, 2019)

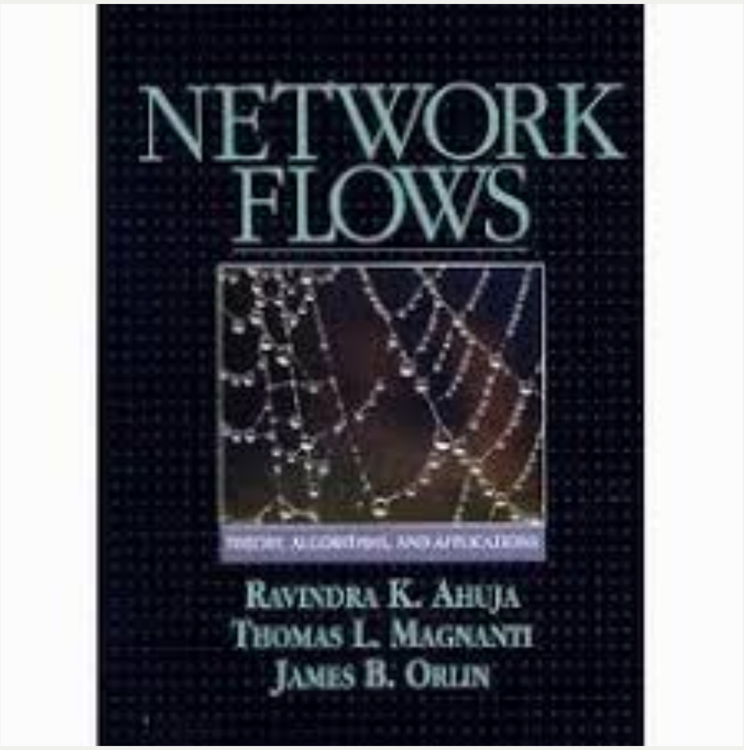
Special cases

Polynomial time algorithms for special classes of lattices:

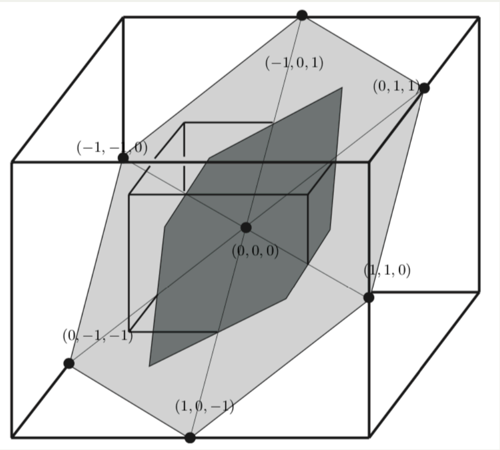
lattices of Voronoi's first kind
(McKilliam, Grant, Clarkson, 2014)

tensor products $A_n \otimes A_m$
(Ducas, van Woerden, 2018)

both based on network flows



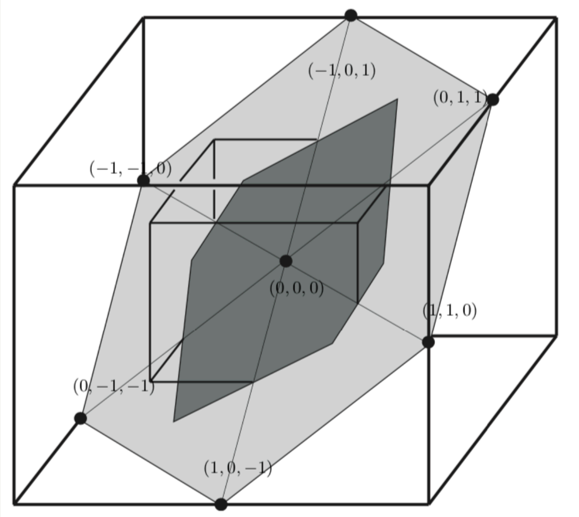
Goal: Unify and generalize these two cases.



Lattices and zonotopes - Setup

Consider *zonotopal lattices*: lattices L where $V(L)$ is a zonotope

$$\begin{aligned} \text{zonotope } &= \text{projection of regular cube } [-1,+1]^m \\ &= \text{Minkowski sum of line segments } \textstyle\sum_{i=1}^m [-s_i,+s_i] \end{aligned}$$



$\mathcal{L} \subseteq \mathbb{R}^m$ linear subspace

for $x \in \mathcal{L}$ define $\operatorname{supp} x = \{i : x_i \neq 0\}$

$x \in \mathcal{L} \setminus \{0\}$ is called *elementary* $\iff$ (i) x has minimal support in $\mathcal{L}$

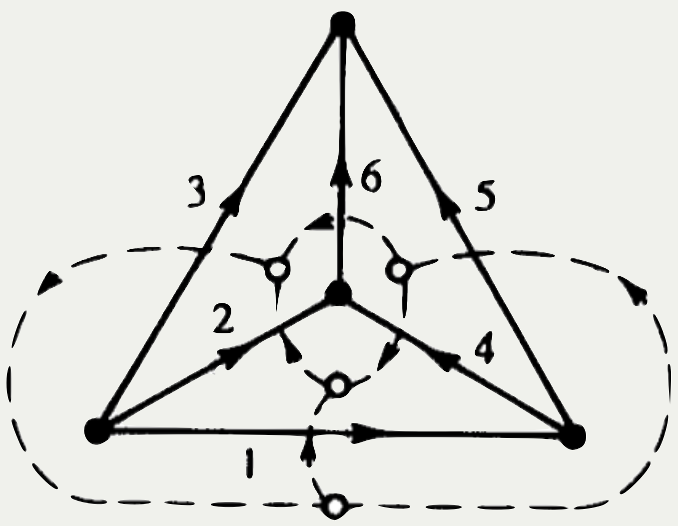
(ii) $x \in \{-1, 0, +1\}^m$

$\mathcal{L}$ is called *regular* $\iff$ for all $y \in \mathcal{L} \setminus \{0\}$ with minimal support there is $\alpha \in \mathbb{R}$ and $x \in \mathcal{L}$ elementary so that $y = \alpha x$

Lattices and zonotopes - Main examples

come from digraphs $D = (V, A)$

$M \in \{-1, 0, +1\}^{V \times A}$ incidence matrix



graphical case

$\mathcal{L}(D) = \{x \in \mathbb{R}^A : Mx = 0\}$ is regular

elementary vectors = circuits (unoriented)

cographical case

$\mathcal{L}(D)^\perp = \{y \in \mathbb{R}^A : x^\mathsf{T} y = 0 \text{ for all } x \in \mathcal{L}(D)\}$ is also regular

elementary vectors = minimal cuts (cocircuits)

Lattices and zonotopes - Voronoi cells

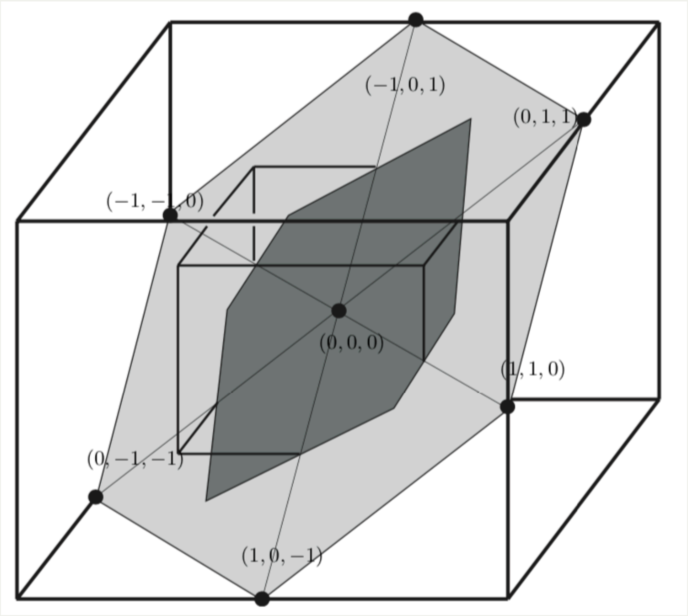
Regular subspaces define lattices $L = \mathcal{L} \cap \mathbb{Z}^m$

Positive vector $g \in \mathbb{R}^m_{>0}$ defined Euclidean structure on L $(x, y)_g = \sum_{i=1}^{m} g_i x_i y_i$

Facts about Voronoi cell of L:

$\{\text{Voronoi vectors}\} = \{\text{facet normals of } V(L)\} = \{\text{elementary vectors}\}$

$V(L) = \pi([-1/2, 1/2]^m)$ $\pi : \mathbb{R}^m \to \mathcal{L}$ orthogonal projection



L is zonotopal lattice; if $V(L)$ is zonotope, then L comes by this construction

Lattices and zonotopes - All examples

(a) Lattices of Voronoi's first kind

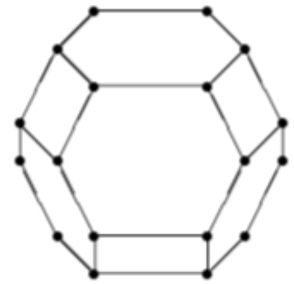
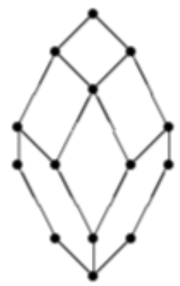
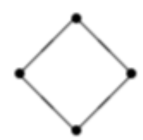
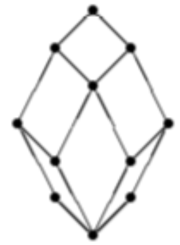
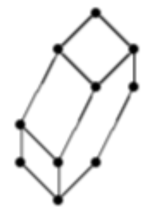
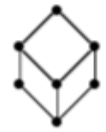
defined by obtuse superbasis $b_1, \ldots, b_n, b_{n+1}$
where $b_1, \ldots, b_n$ forms a lattice basis
where $b_i^\top b_j \leq 0$ if $i \neq j$ and $\sum_{i=1}^{n+1} b_i = 0$.

This defines a graph D with vertices $b_1, \ldots, b_{n+1}$
and weighted edges (b_i, b_j) if $i < j$ with weight $g_{ij} = -b_i^\top b_j$.

Then: $L(D)^\perp \simeq L$

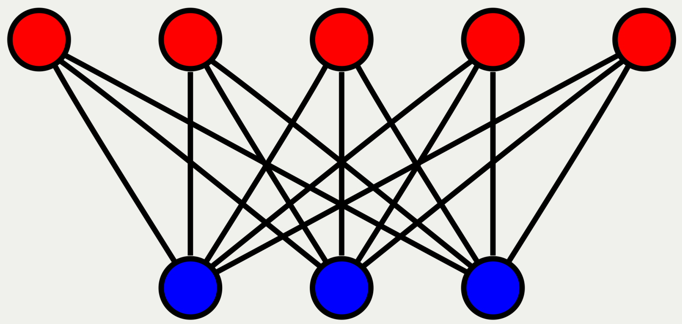
In particular: $L(C_{n+1})^\perp = A_n$ and $L(K_{n+1})^\perp = A_n^*$

3-dimensional lattices

d	Delone Graph	Polytope	Form	Name
6	 K_4		$\begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix}$	**TRUNCATED OCTAHEDRON**
5	 $K_4 - 1$		$\begin{pmatrix} 2 & -1 & 0 \\ -1 & 3 & -1 \\ 0 & -1 & 2 \end{pmatrix}$	**HEXA-RHOMBIC DODECAHEDRON**
4	 C_4		$\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$	**RHOMBIC DODECAHEDRON**
4	 $K_3 + 1$		$\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	**HEXAGONAL PRISM**
3	 $1 + 1 + 1$		$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	**CUBE**

(b) tensor products

$$A_m \otimes A_n = L(K_{m+1,n+1})$$



(c) Seymour (1980)

Classification: Every zonotopal lattice is 1-,2-,3-sum of cographical, graphical lattices or R_{10} (exceptional 5-dim. lattice)

Minimum mean cycle canceling

Karzanov, McCormick (1997):

Can solve the following problem in polynomial time

$M \in \{-1, 0, +1\}^{n \times m}$ totally unimodular matrix $\quad L = \{v \in \mathbb{Z}^m : Mv = 0\}$

$w_i : \mathbb{R} \to \mathbb{R}$ convex functions, $i = 1, \ldots, m$

minimize $\sum_{i=1}^{m} w_i(v_i)$ subject to $v \in L$

separable convex objective function

Observation: That is a perfect fit for the CVP of zonotopal lattices.

For (L, g) zonotopal lattice and $x \in \mathbb{R}^m$ set

$w_i(v_i) = g_i(v_i - x_i)^2$ convex quadratic

Then: $\sum w_i(v_i) = (x - v, x - v)_g = |x - v|_g^2$

Idea of algorithm

For $v \in L$ and for elementary vector $u \in L$

define cost of u at v by

$$c(v,u) = \sum_{i:u_i=+1} c_i^+(v_i) - \sum_{i:u_i=-1} c_i^-(v_i)$$

where
$$c_i^+(v_i) = g_i(v_i - x_i + 1)^2 - g_i(v_i - x_i)^2$$
$$c_i^-(v_i) = g_i(v_i - x_i)^2 - g_i(v_i - x_i - 1)^2$$

If cost $c(u,v)$ is negative then $v+u$ is closer to x than v:

$$(v+u-x, v+u-x)_g = (v-x, v-x)_g + c(v,u)$$

$$\lambda(v) = \max\left\{0, -\min_{u \text{ elementary}} \frac{c(v,u)}{|\text{supp } u|}\right\}$$

minimizer u defines "minimum mean cycle at v"

1. $\lambda(v) = 0 \iff v$ is closest vector to x
2. Can determine $\lambda(v)$ and u elementary attaining minimum by LP
3. Pivot: $v \leftarrow v + \varepsilon u$ for suitable step size ε
4. λ-value descreases geometrically

$\Longrightarrow$ polynomial time algorithm for CVP