

Rácsok Voronoi-cellája

Eötvös Loránd Tudományegyetem

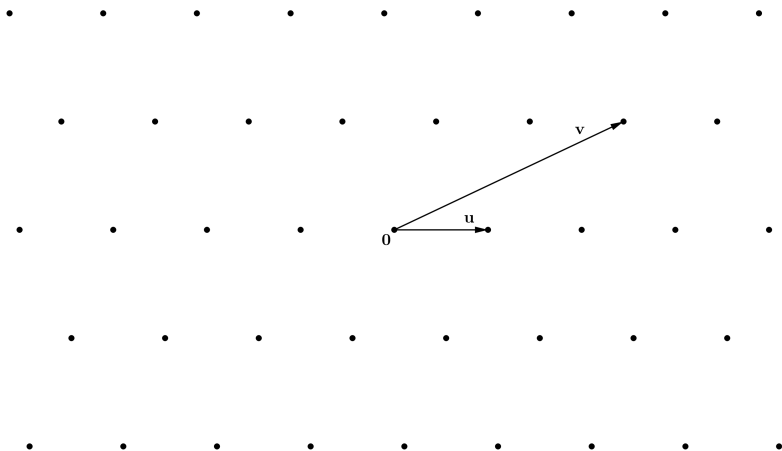
2025. január 10.

Áttekintés

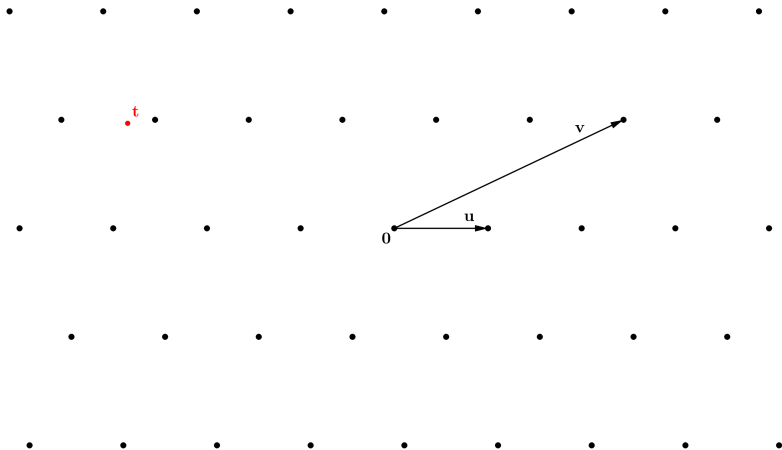
- Algoritmikus problémák rácson
- Bázis-redukció, és felsorolás algoritmusok
- Voronoi-cella
- Algoritmus Voronoi-cella számítással

Rácsok

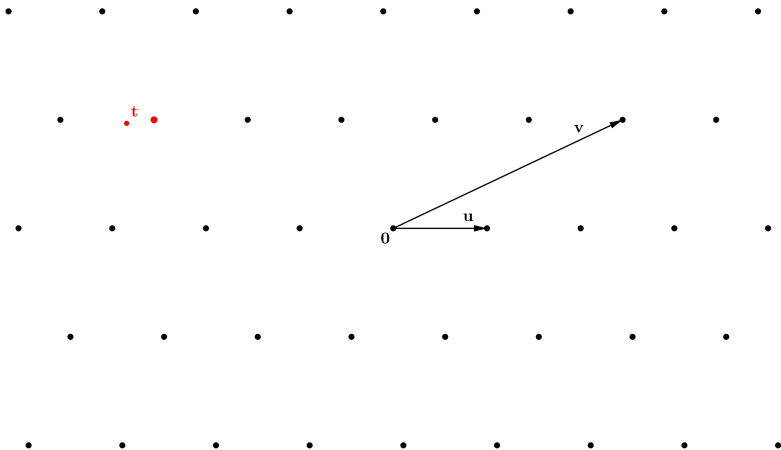
L rács: $L = \{s_1 b_1 + \dots + s_n b_n \mid s_i \in \mathbb{Z}\}$ ahol b_1, \dots, b_n az \mathbb{R}^n egy bázisa.



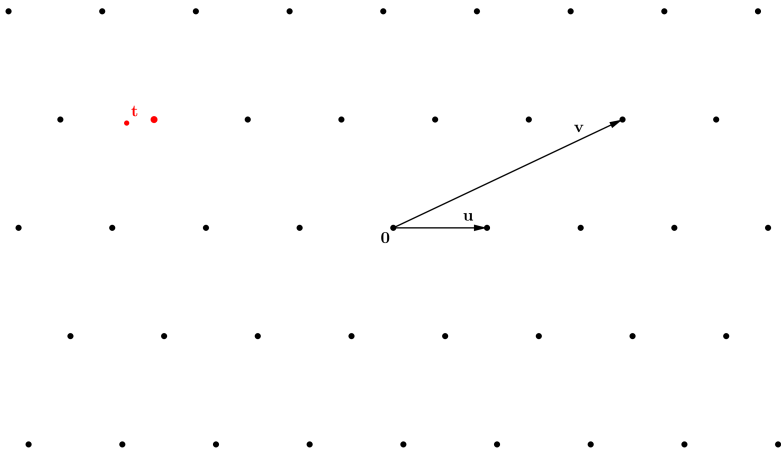
Legközelebbi vektor probléma - CVP (Closest Vector Problem)



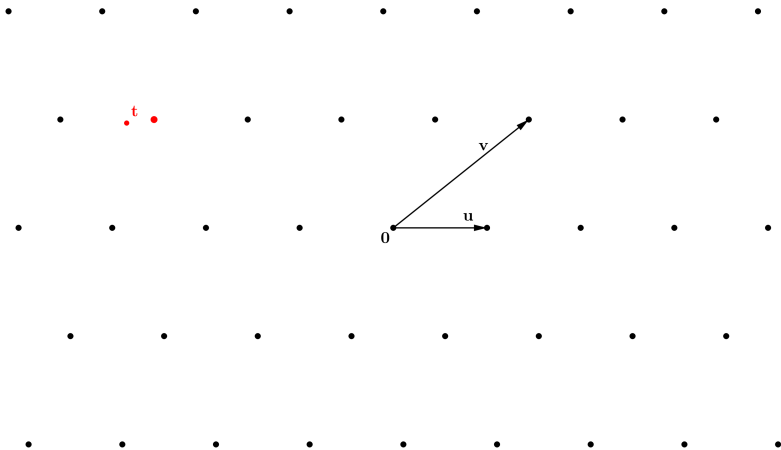
Legközelebbi vektor probléma - CVP (Closest Vector Problem)



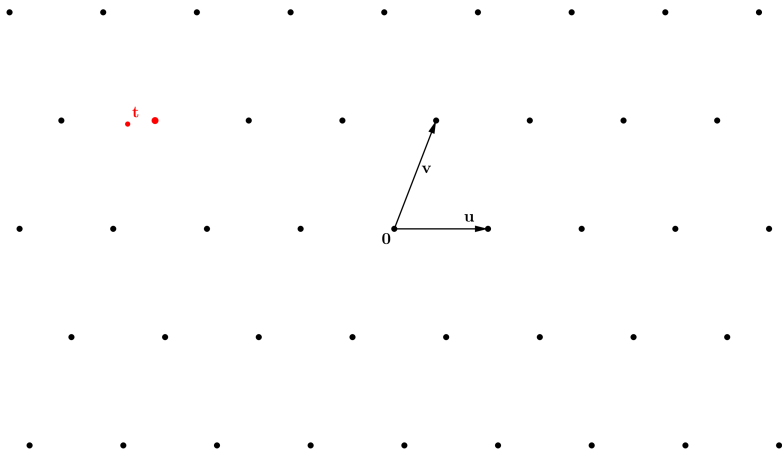
Bázis-redukció és felsoroló algoritmus



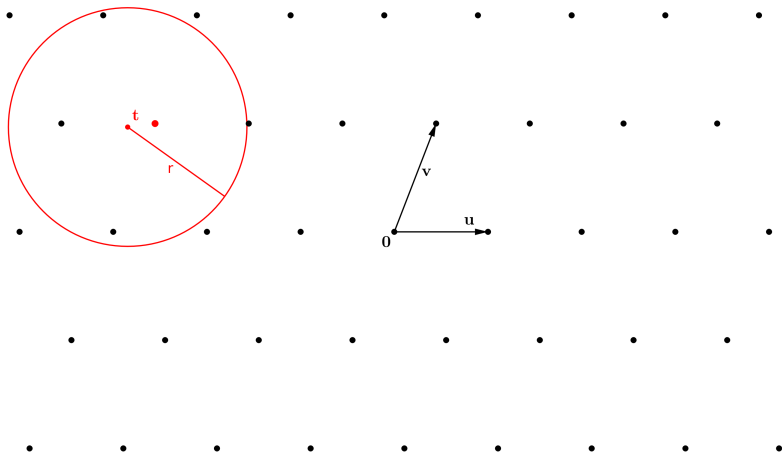
Bázis-redukció és felsoroló algoritmus



Bázis-redukció és felsoroló algoritmus



Bázis-redukció és felsoroló algoritmus



Bázis-redukció és felsorolás algoritmusok

- Bázisredukció: Lenstra, Lenstra, Lovász algoritmus (1982): polinomiális időben kellően merőleges bázis

Bázis-redukció és felsorolás algoritmusok

- Bázisredukció: Lenstra, Lenstra, Lovász algoritmus (1982): polinomiális időben kellően merőleges bázis
- A CVP probléma NP-nehéz

Bázis-redukció és felsorolás algoritmusok

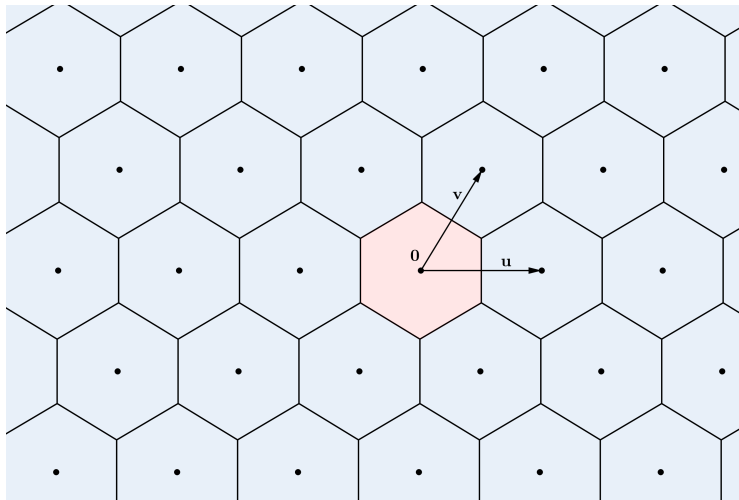
- Bázisredukció: Lenstra, Lenstra, Lovász algoritmus (1982): polinomiális időben kellően merőleges bázis
- A CVP probléma NP-nehéz
- Felsorolás algoritmus megoldja a problémát $n^{O(n)}$ időben és polinomiális térben (Kannan 1983)

Bázis-redukció és felsorolás algoritmusok

- Bázisredukció: Lenstra, Lenstra, Lovász algoritmus (1982): polinomiális időben kellően merőleges bázis
- A CVP probléma NP-nehéz
- Felsorolás algoritmus megoldja a problémát $n^{O(n)}$ időben és polinomiális térben (Kannan 1983)
- Van szimplán exponenciális algoritmus ($2^{O(n)}$)?

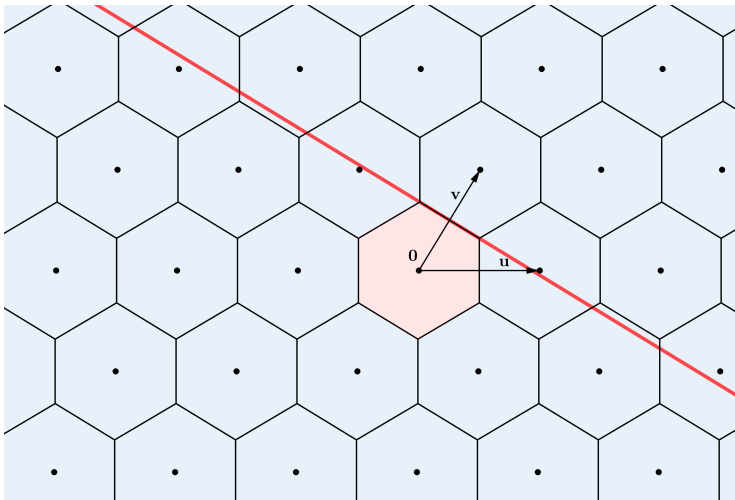
Voronoi-cella

- Definíció: $\text{vor } L = \{v \in \mathbb{R}^n \mid \forall b \in L: d(v, 0) \leq d(v, b)\}$



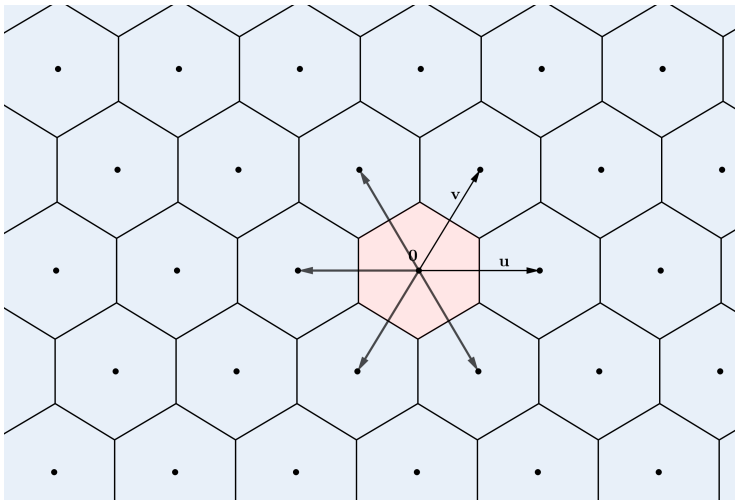
Voronoi-vektorok

- $H_v = \{w \in \mathbb{R}^n \mid v \cdot w \leq v^2/2\}$



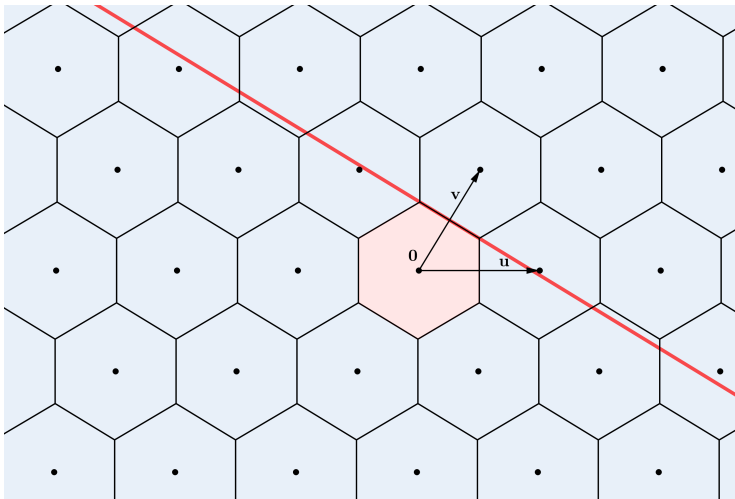
Voronoi-vektorok

- $H_v = \{w \in \mathbb{R}^n \mid v \cdot w \leq v^2/2\}$



Voronoi-vektorok

- Szigorú: metszete a Voronoi-cellával $n - 1$ dimenziós



Voronoi-vektorok

- Tétel (Voronoi 1908): $0 \neq b \in L$ pontosan akkor Voronoi-vektor ha minimális hosszúságú az $b + 2L$ osztály vektorai között, és akkor szigorú ha ezen osztály legrövidebb vektorai pont $\pm b$

Voronoi-vektorok

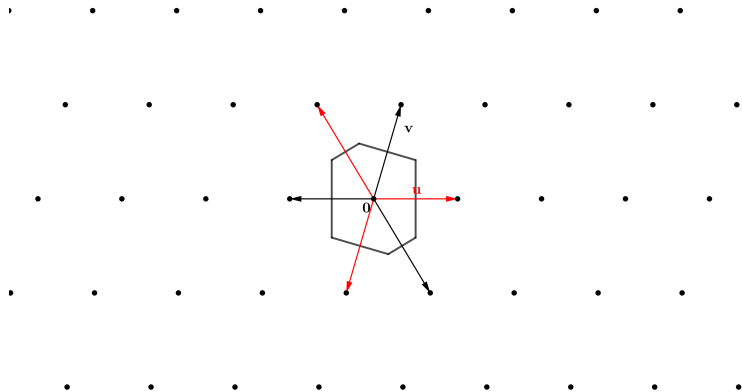
- Tétel (Voronoi 1908): $0 \neq b \in L$ pontosan akkor Voronoi-vektor ha minimális hosszúságú az $b + 2L$ osztály vektorai között, és akkor szigorú ha ezen osztály legrövidebb vektorai pont $\pm b$
- szigorú Voronoi vektorok száma $\leq 2(2^n - 1)$

Voronoi-vektorok

- Tétel (Voronoi 1908): $0 \neq b \in L$ pontosan akkor Voronoi-vektor ha minimális hosszúságú az $b + 2L$ osztály vektorai között, és akkor szigorú ha ezen osztály legrövidebb vektorai pont $\pm b$
- szigorú Voronoi vektorok száma $\leq 2(2^n - 1)$
- Nyitott kérdés: Van-e minden rácsnak Voronoi-vektorokból álló bázisa? (első 4 dimenzióban igen)

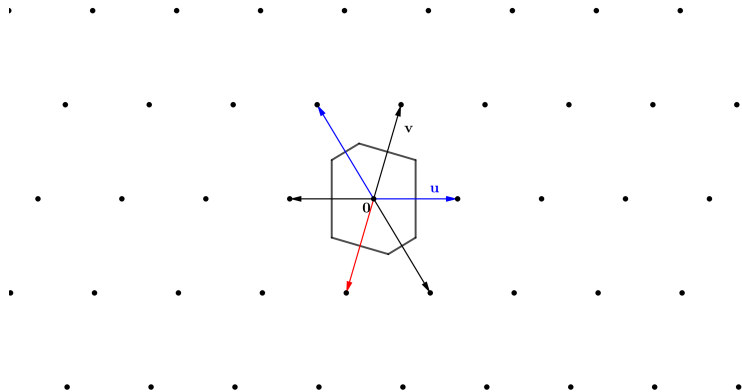
Voronoi-első típusú rácok

- Def: rács Voronoi-első típusú ha van tompa superbázisa



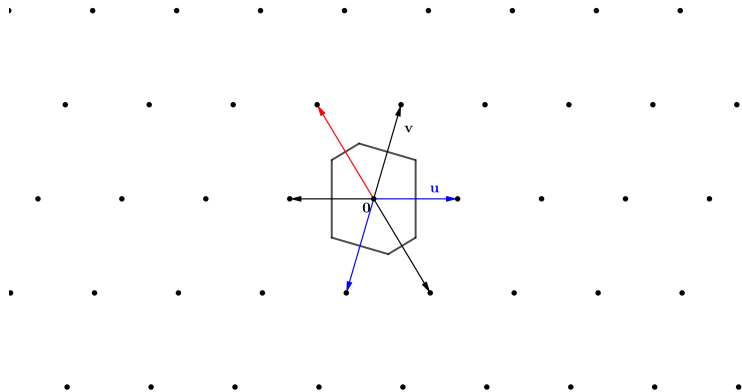
Voronoi-első típusú rácok

- Def: rác Voronoi-első típusú ha van tompa superbázisa



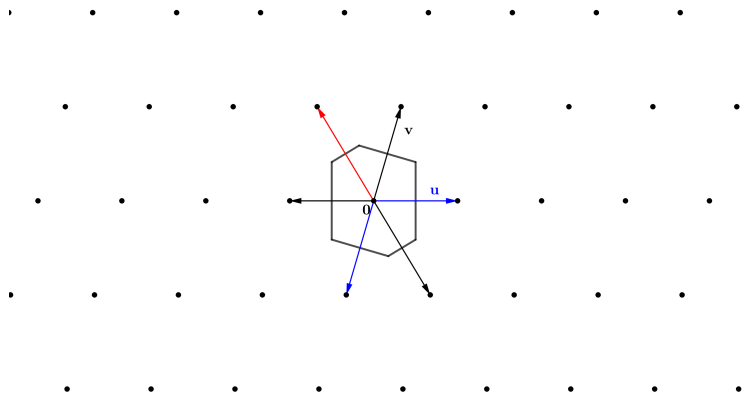
Voronoi-első típusú rácok

- Def: rác Voronoi-első típusú ha van tompa superbázisa

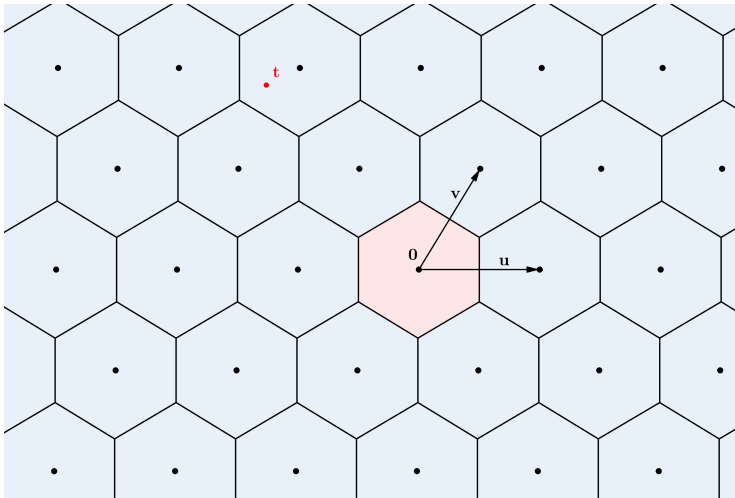


Voronoi-első típusú rácok

- Def: rács Voronoi-első típusú ha van tompa superbázisa
- Tétel: Első 3 dimenzióban minden rács első típusú



Algoritmus Voronoi-cella számítással



Algoritmus Voronoi-cella számítással

Algoritmus (Micciancio-Voulgaris 2010):

- Voronoi-cella számítás: $2^n - 1$ CVP megoldása (előző tétel szerint)

Algoritmus Voronoi-cella számítással

Algoritmus (Micciancio-Voulgaris 2010):

- Voronoi-cella számítás: $2^n - 1$ CVP megoldása (előző tétel szerint)
- Bázis-redukció: n dimenziós CVP visszavezetése $2^{n/2}$ darab $n - 1$ dimenziós CVP megoldására

Algoritmus Voronoi-cella számítással

Algoritmus (Micciancio-Voulgaris 2010):

- Voronoi-cella számítás: $2^n - 1$ CVP megoldása (előző tétel szerint)
- Bázis-redukció: n dimenziós CVP visszavezetése $2^{n/2}$ darab $n - 1$ dimenziós CVP megoldására
- CVP megoldása a szigorú Voronoi-vektorok ismeretében

Összefoglaló, nyitott kérdések

- Előző algoritmus: $2^{O(n)}$ idő és tár.

Összefoglaló, nyitott kérdések

- Előző algoritmus: $2^{O(n)}$ idő és tár.
- Felsorolás (korábbi) algoritmus: $n^{O(n)}$ idő és polinomiális tár

Összefoglaló, nyitott kérdések

- Előző algoritmus: $2^{O(n)}$ idő és tár.
- Felsorolás (korábbi) algoritmus: $n^{O(n)}$ idő és polinomiális tár
- $2^{O(n)}$ idő és poli tár?

Összefoglaló, nyitott kérdések

- Előző algoritmus: $2^{O(n)}$ idő és tár.
- Felsorolás (korábbi) algoritmus: $n^{O(n)}$ idő és polinomiális tár
- $2^{O(n)}$ idő és poli tár?
- Más normákban meg lehet csinálni?

Összefoglaló, nyitott kérdések

- Előző algoritmus: $2^{O(n)}$ idő és tár.
- Felsorolás (korábbi) algoritmus: $n^{O(n)}$ idő és polinomiális tár
- $2^{O(n)}$ idő és poli tár?
- Más normákban meg lehet csinálni?
- Rácsok speciális családján?

Összefoglaló, nyitott kérdések

- Előző algoritmus: $2^{O(n)}$ idő és tár.
- Felsorolás (korábbi) algoritmus: $n^{O(n)}$ idő és polinomiális tár
- $2^{O(n)}$ idő és poli tár?
- Más normákban meg lehet csinálni?
- Rácsok speciális családján?
- ...