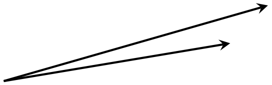
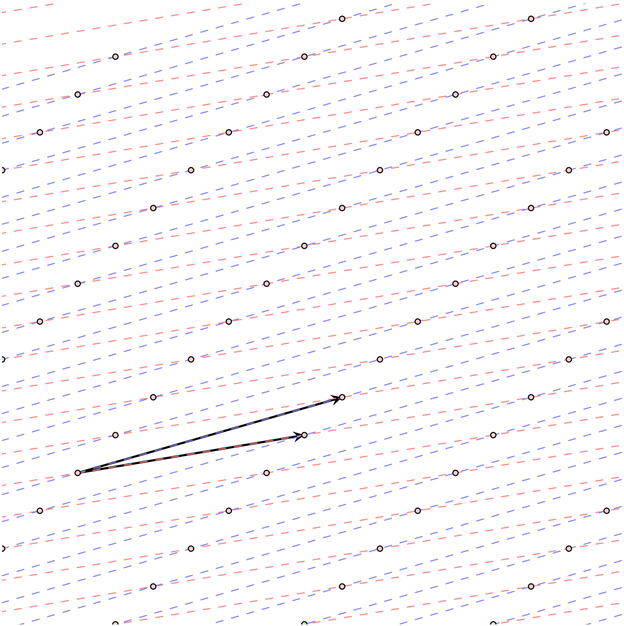
What Is a Lattice?

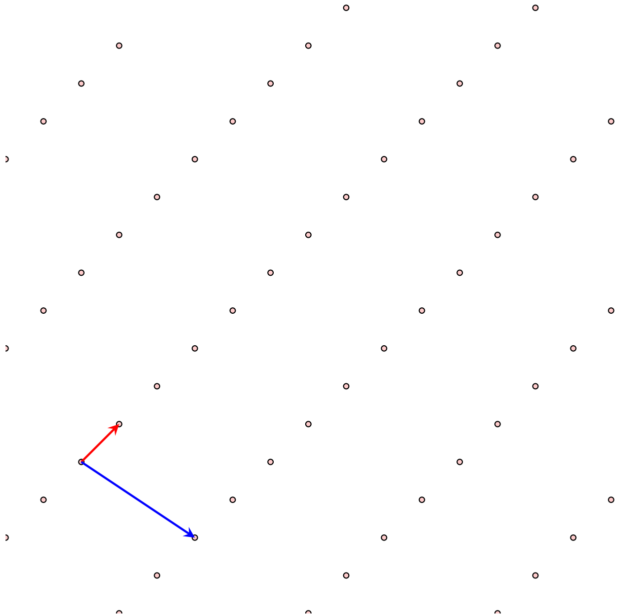
Given n linearly independent vectors $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^m$ ($n \leq m$), the lattice generated by them is the set of vectors

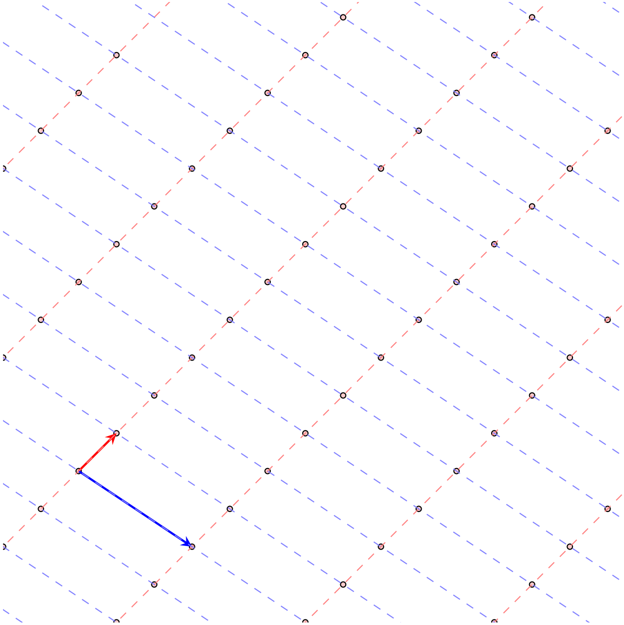
$$L(\mathbf{b_1}, \ldots, \mathbf{b_n}) = \{\sum_{i=1}^{n} x_i \mathbf{b_i} : x_i \in \mathbb{Z}\}$$

The vectors $\mathbf{b_1}, \ldots, \mathbf{b_n}$ form a basis of the lattice.



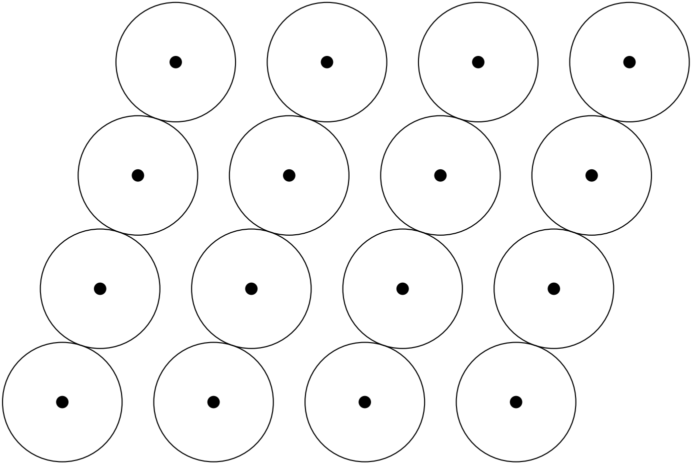






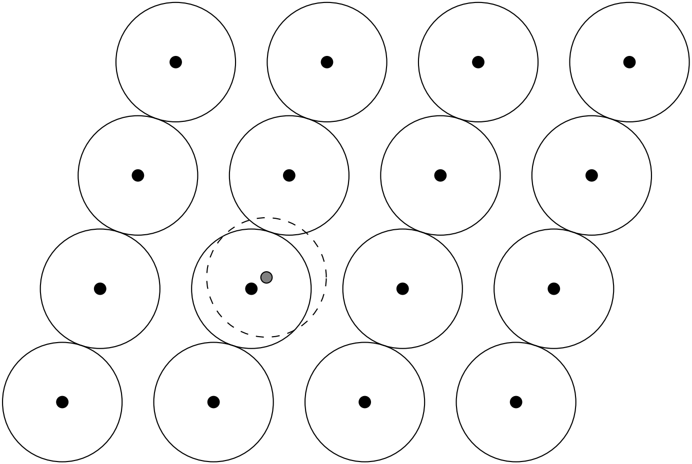
Lattices and Codes

Shortest Vector and Minimum Distance, Closet Vector and Maximum Likelyhood Decoding, Unambiguous decoding, List Decoding and BDD, Deep Holes



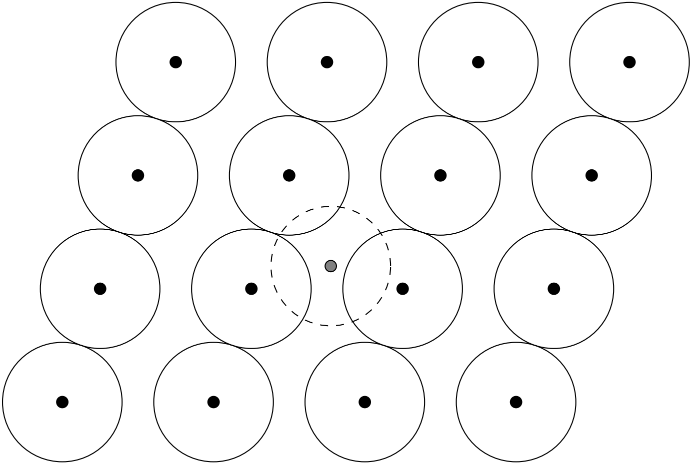
Lattices and Codes

Shortest Vector and Minimum Distance, Closet Vector and Maximum Likelyhood Decoding, Unambiguous decoding, List Decoding and BDD, Deep Holes



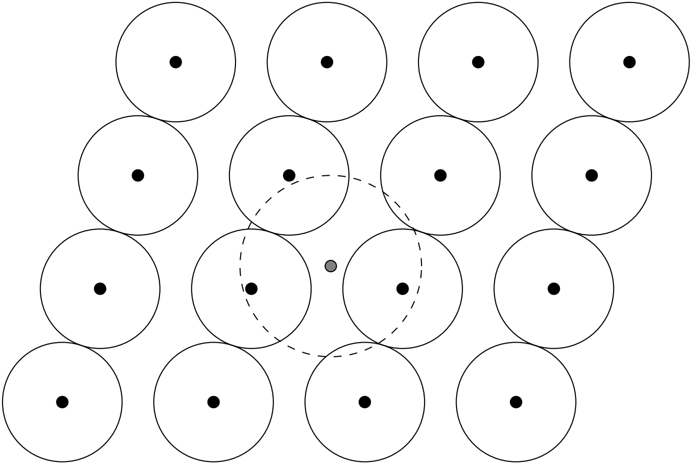
Lattices and Codes

Shortest Vector and Minimum Distance, Closet Vector and Maximum Likelyhood Decoding, Unambiguous decoding, List Decoding and BDD, Deep Holes



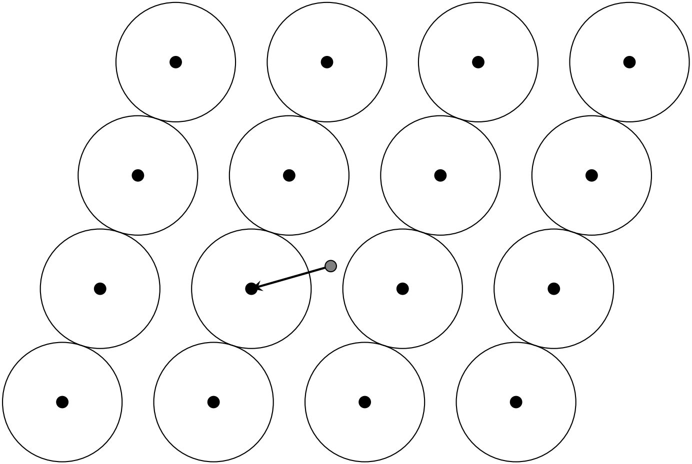
Lattices and Codes

Shortest Vector and Minimum Distance, Closet Vector and Maximum Likelyhood Decoding, Unambiguous decoding, List Decoding and BDD, Deep Holes



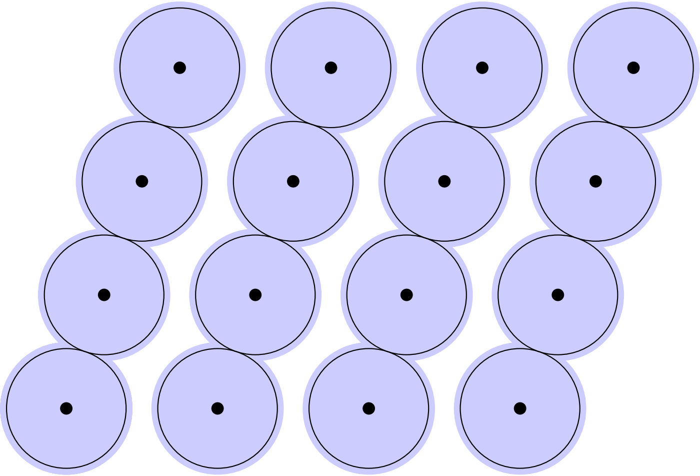
Lattices and Codes

Shortest Vector and Minimum Distance, Closet Vector and Maximum Likelyhood Decoding, Unambiguous decoding, List Decoding and BDD, Deep Holes



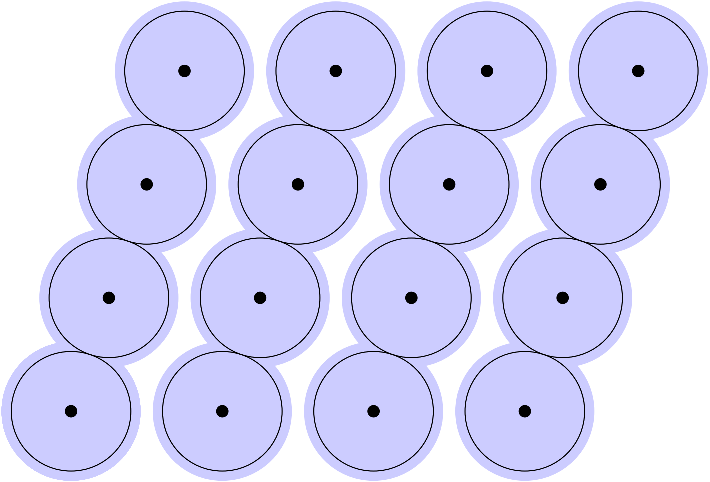
Lattices and Codes

Shortest Vector and Minimum Distance, Closet Vector and Maximum Likelyhood Decoding, Unambiguous decoding, List Decoding and BDD, Deep Holes



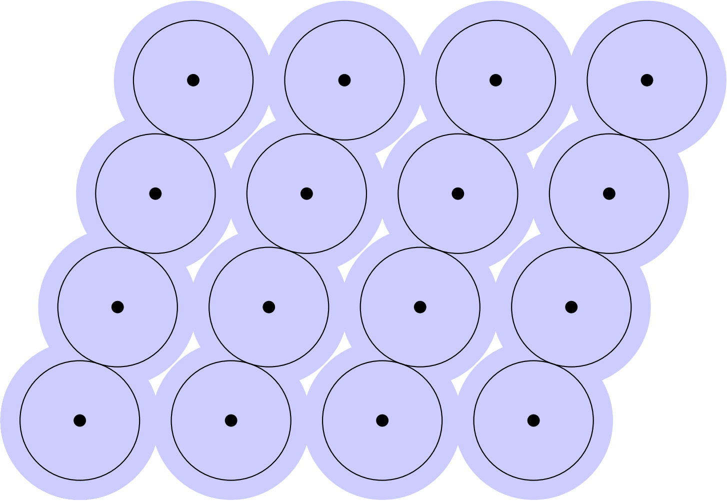
Lattices and Codes

Shortest Vector and Minimum Distance, Closet Vector and Maximum Likelyhood Decoding, Unambiguous decoding, List Decoding and BDD, Deep Holes



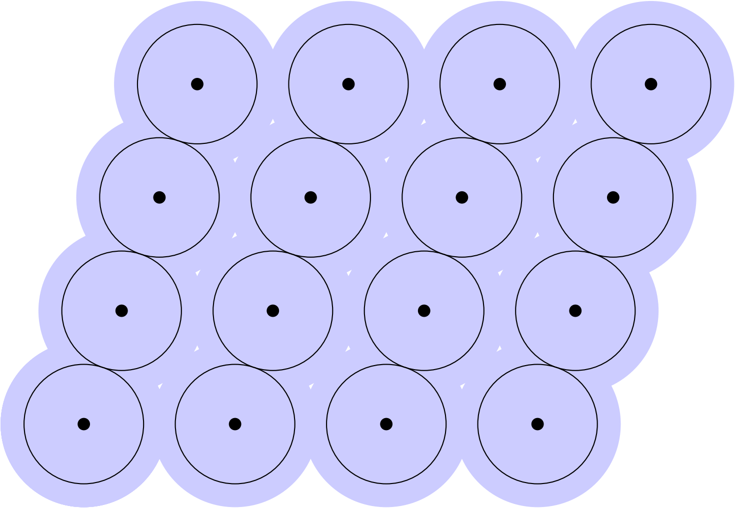
Lattices and Codes

Shortest Vector and Minimum Distance, Closet Vector and Maximum Likelyhood Decoding, Unambiguous decoding, List Decoding and BDD, Deep Holes



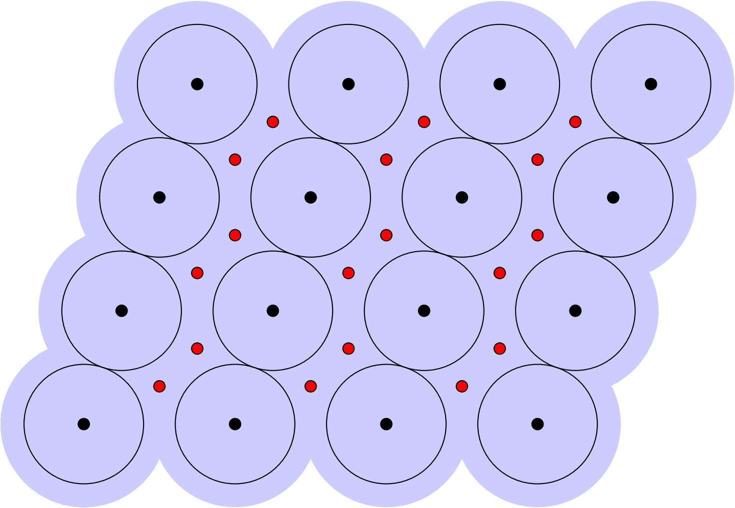
Lattices and Codes

Shortest Vector and Minimum Distance, Closet Vector and Maximum Likelyhood Decoding, Unambiguous decoding, List Decoding and BDD, Deep Holes



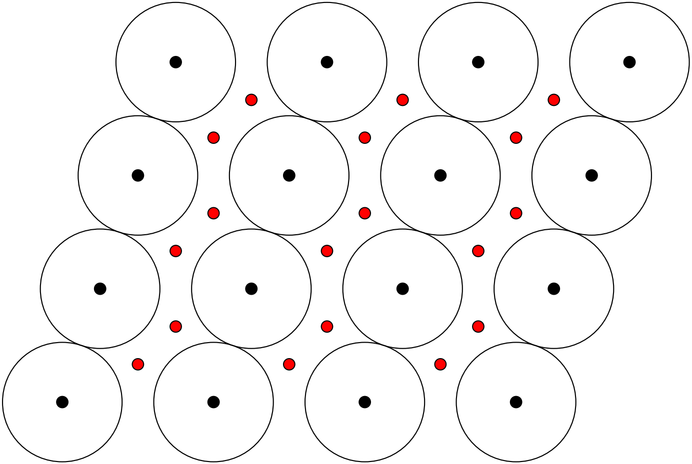
Lattices and Codes

Shortest Vector and Minimum Distance, Closet Vector and Maximum Likelyhood Decoding, Unambiguous decoding, List Decoding and BDD, Deep Holes

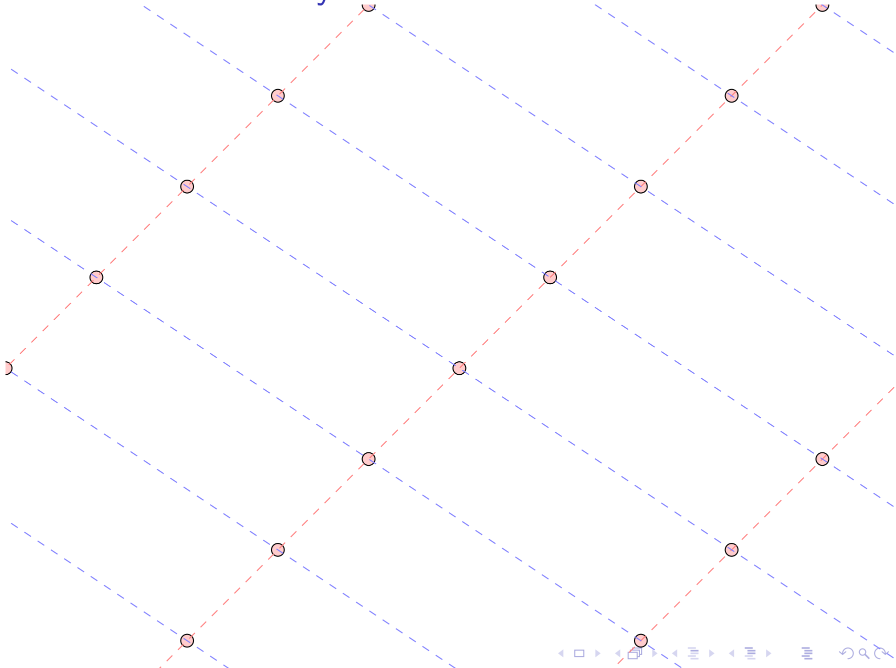


Lattices and Codes

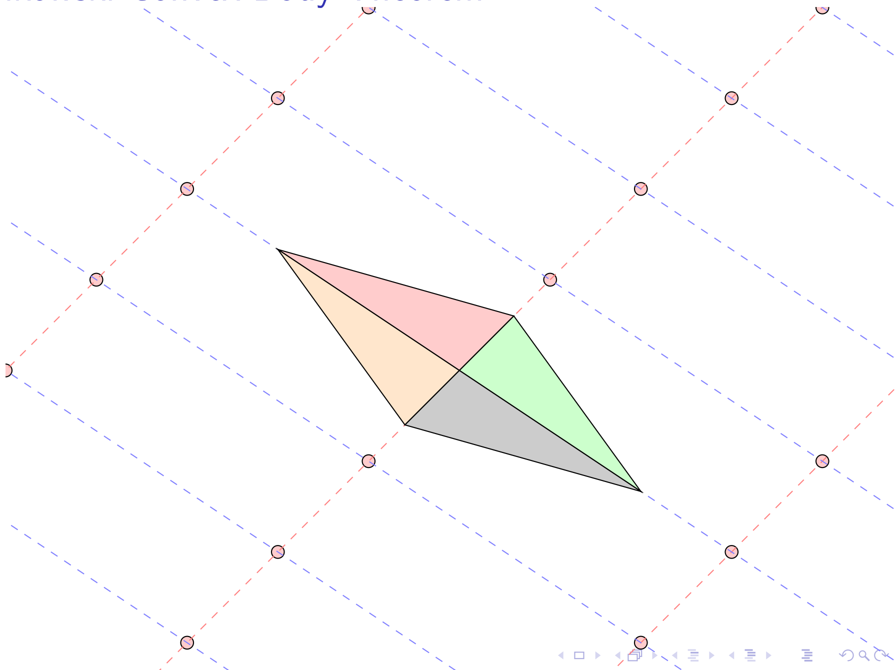
Shortest Vector and Minimum Distance, Closet Vector and Maximum Likelyhood Decoding, Unambiguous decoding, List Decoding and BDD, Deep Holes



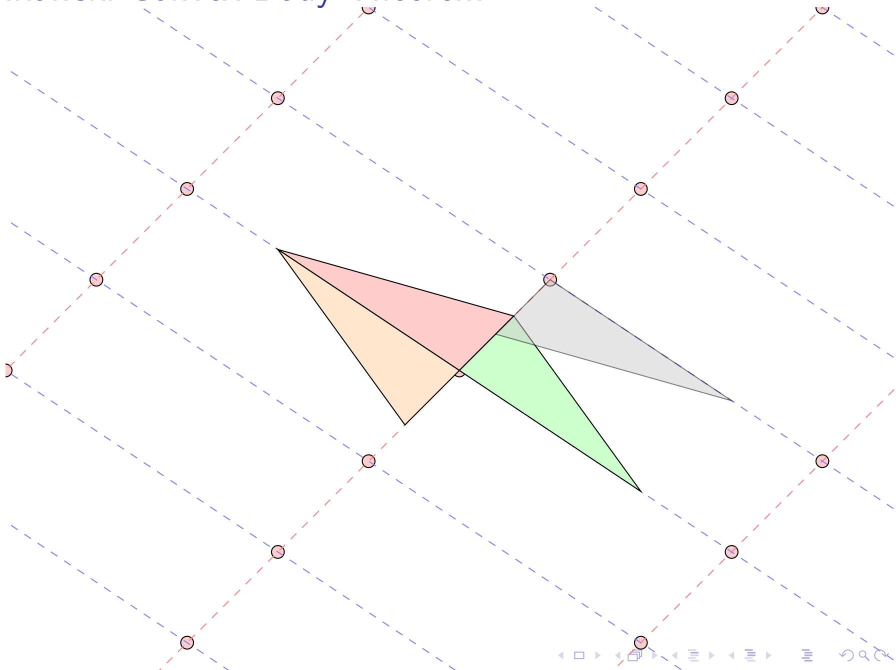
Minkowski Convex Body Theorem



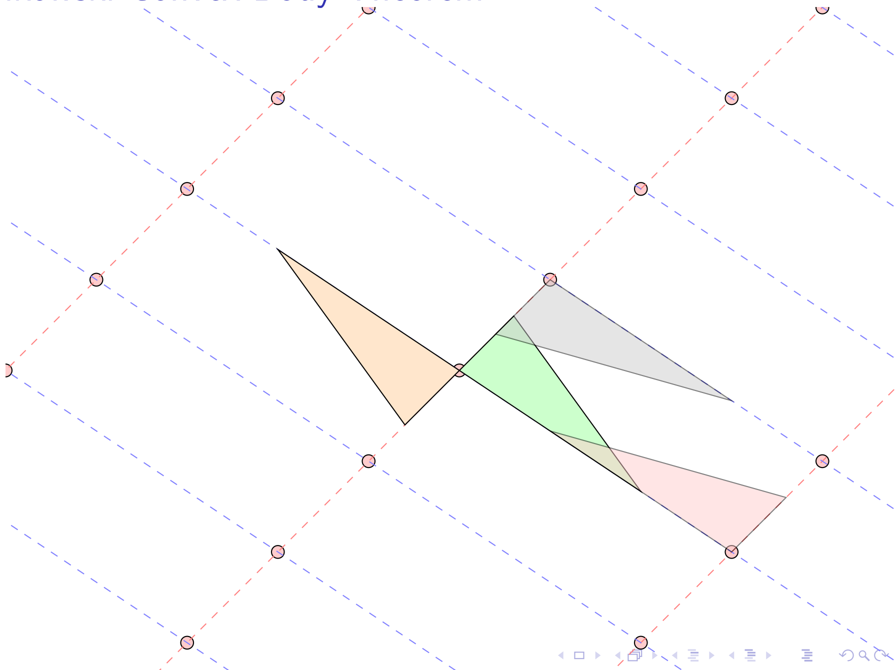
Minkowski Convex Body Theorem



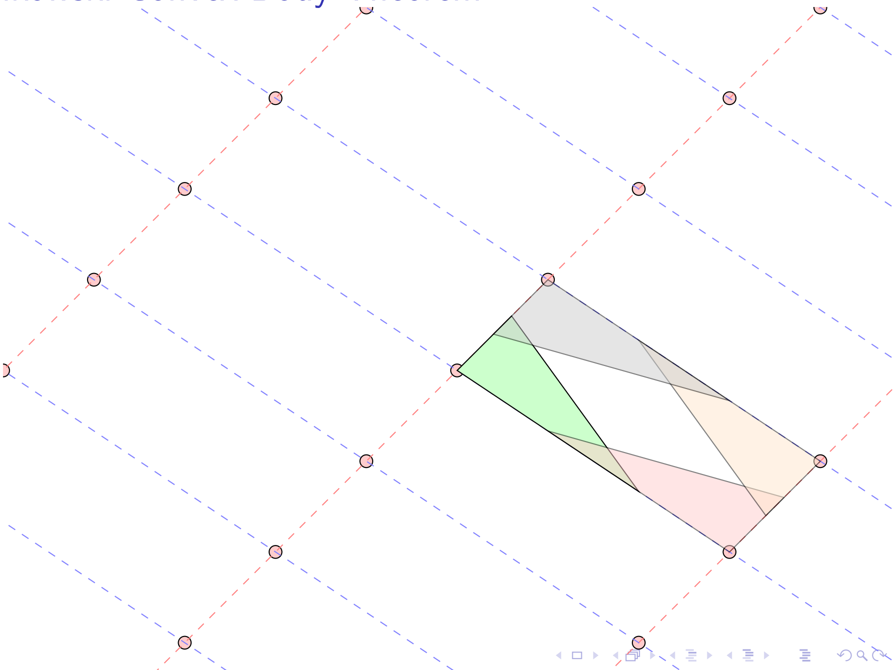
Minkowski Convex Body Theorem



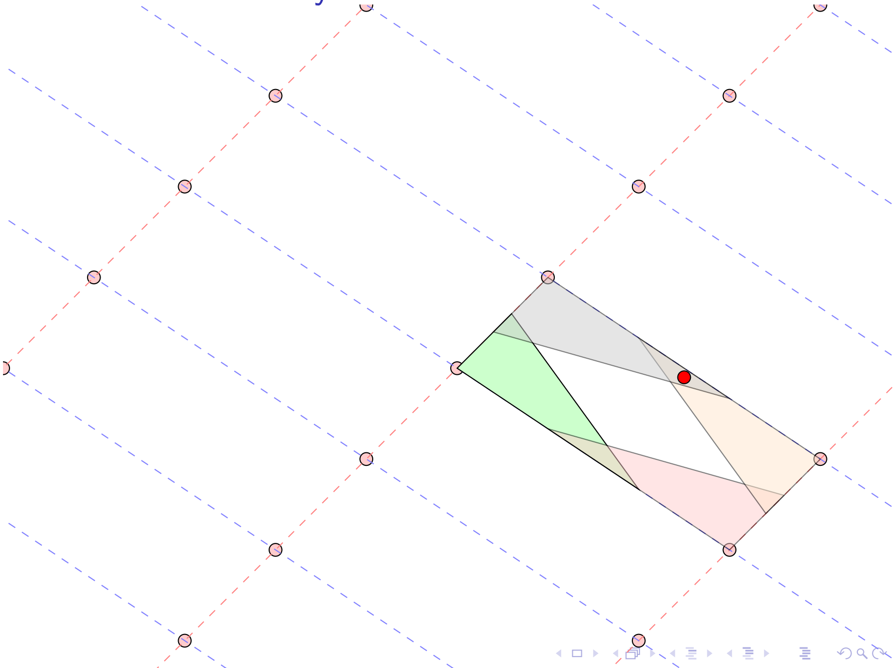
Minkowski Convex Body Theorem



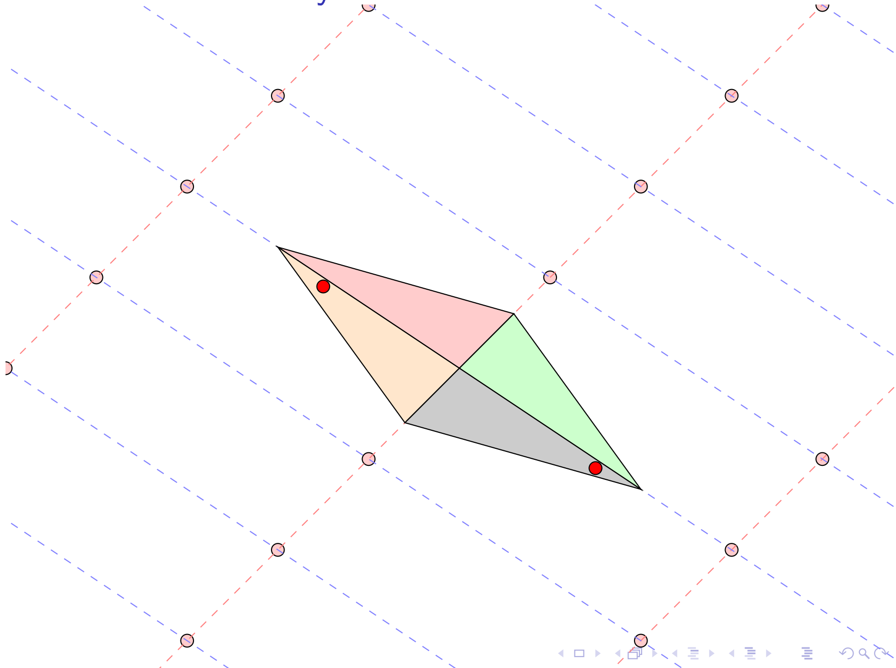
Minkowski Convex Body Theorem



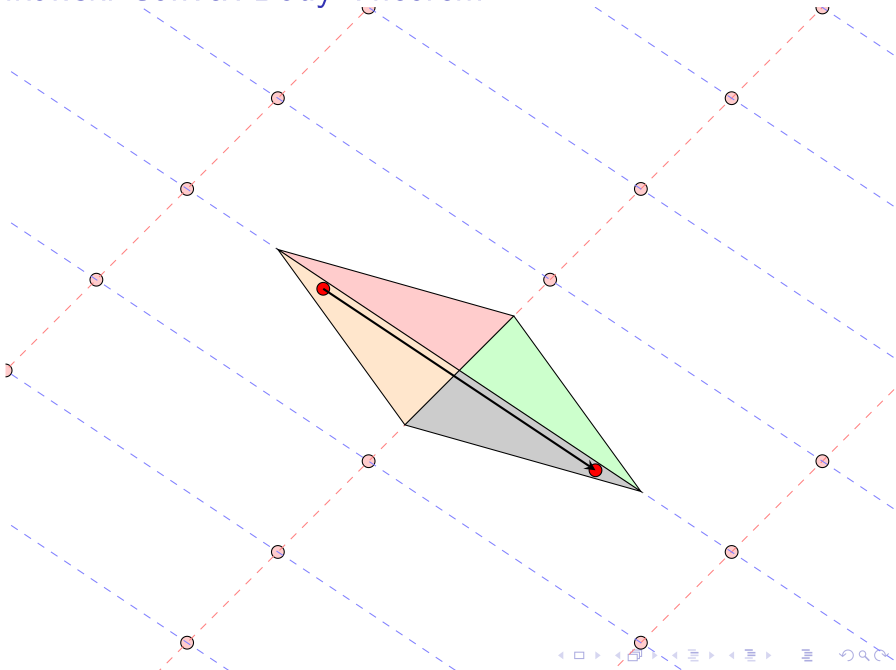
Minkowski Convex Body Theorem



Minkowski Convex Body Theorem



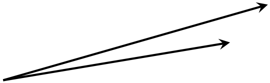
Minkowski Convex Body Theorem



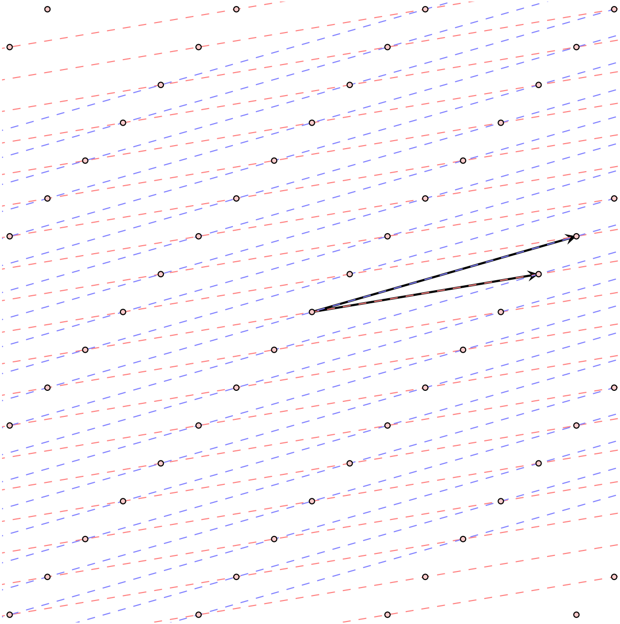
The shortest vector

- Hermite bound: $\sqrt{n} det(L)^{1/n}$ (uniform)
- On average has length $(1+o(1))\sqrt{\frac{n}{2e\pi}} det(L)^{1/n}$ (Gauss Heuristic)
- Must have length less than $(1+o(1))\sqrt{\frac{2n}{e\pi}} det(L)^{1/n}$. (The Minkowski Convex Body Theorem)

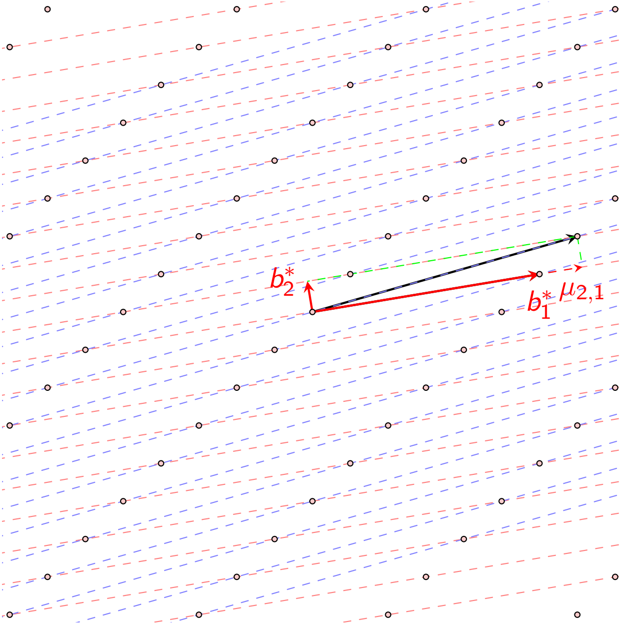
Lattice reduction at dimension 2



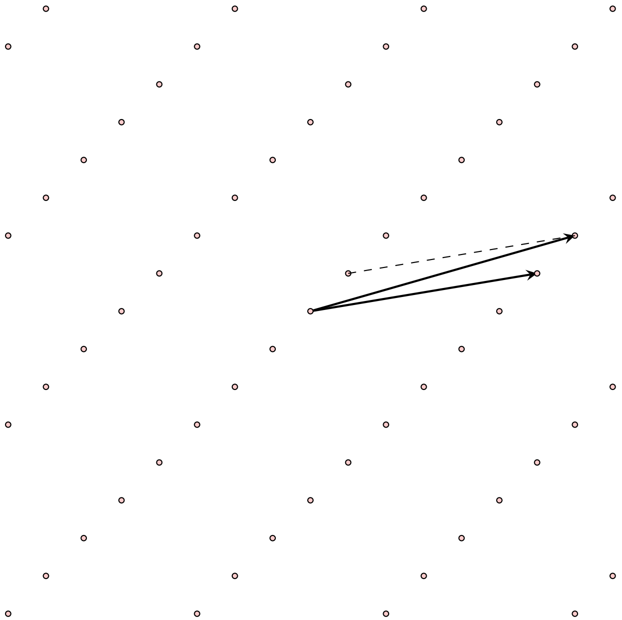
Lattice reduction at dimension 2



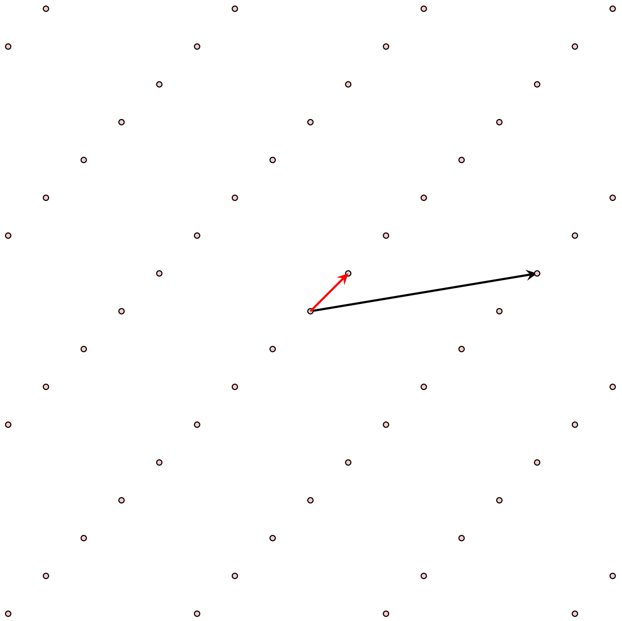
Lattice reduction at dimension 2



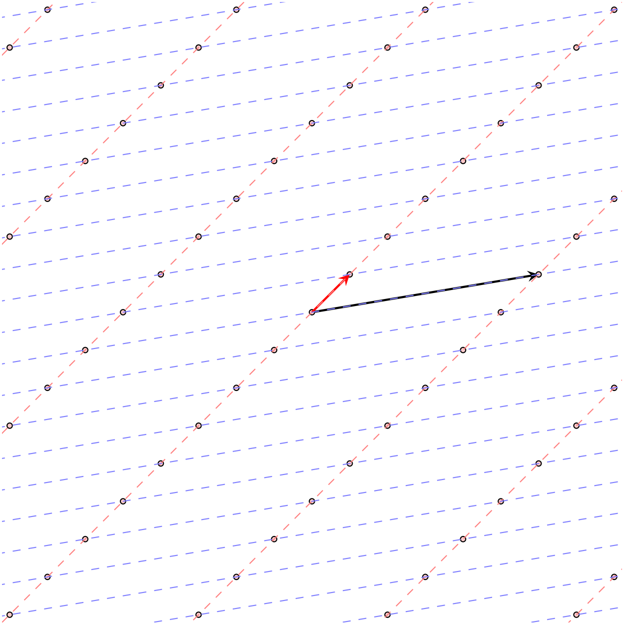
Lattice reduction at dimension 2



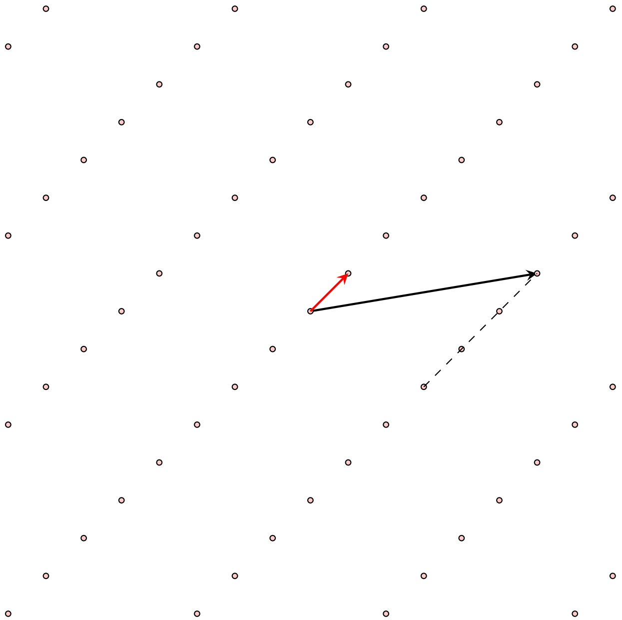
Lattice reduction at dimension 2



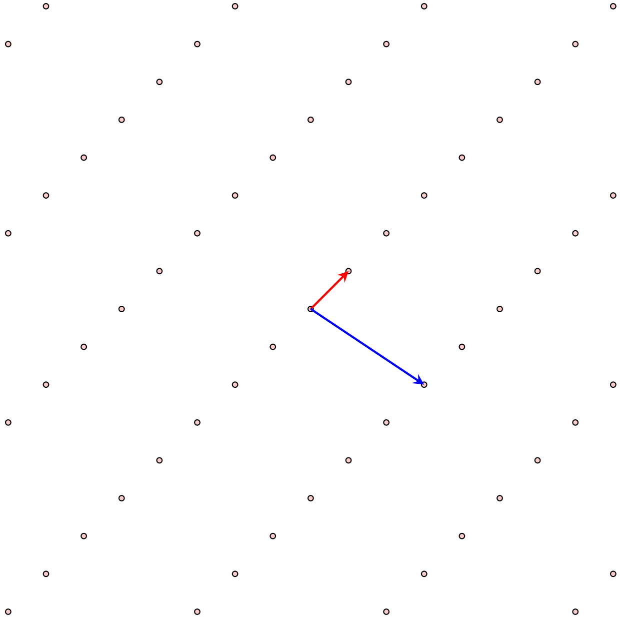
Lattice reduction at dimension 2



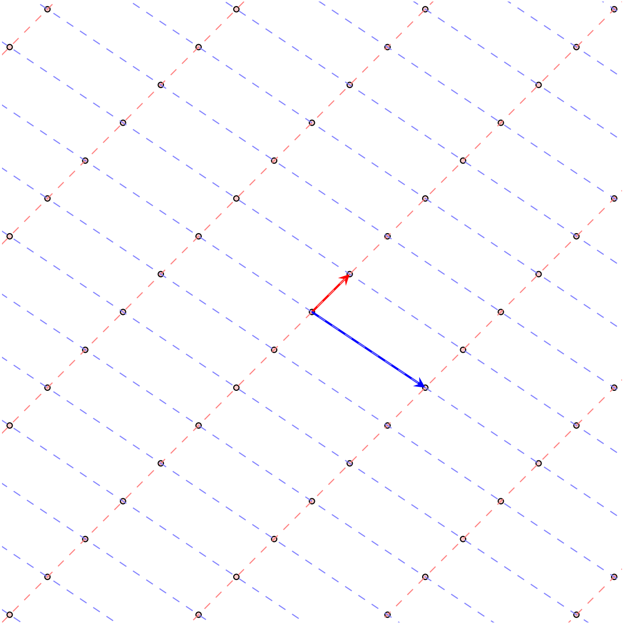
Lattice reduction at dimension 2



Lattice reduction at dimension 2



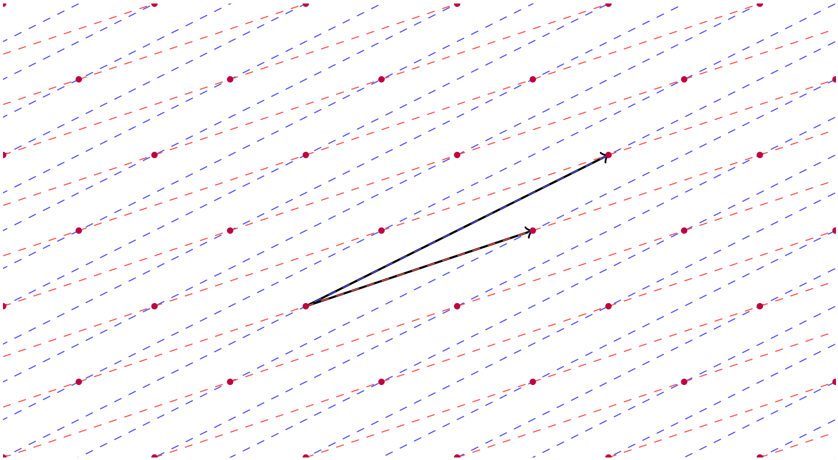
Lattice reduction at dimension 2



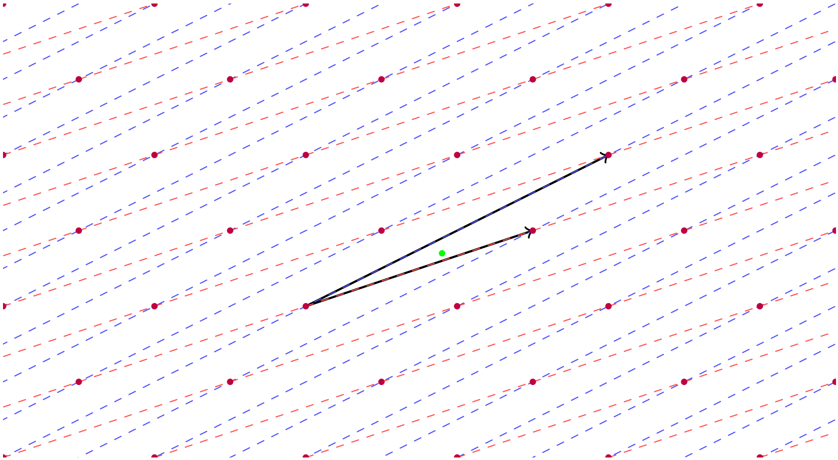
Closest Vector Problem

For one dimensional lattices, rounding works.

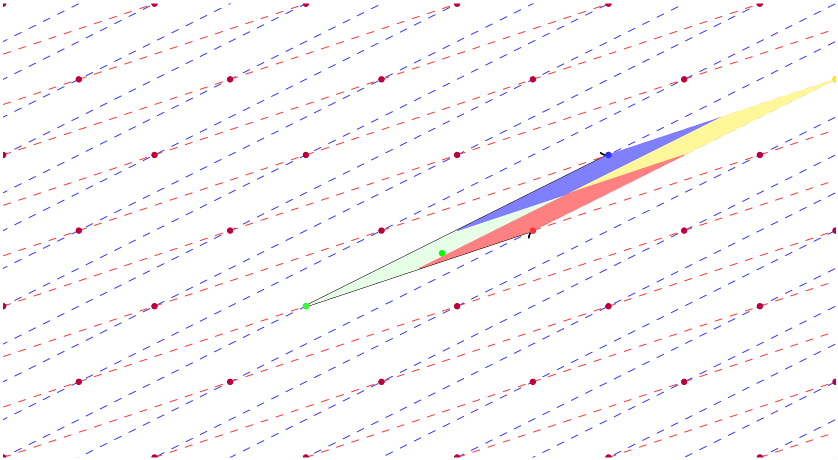
Closest Vector Problem–Dimension two



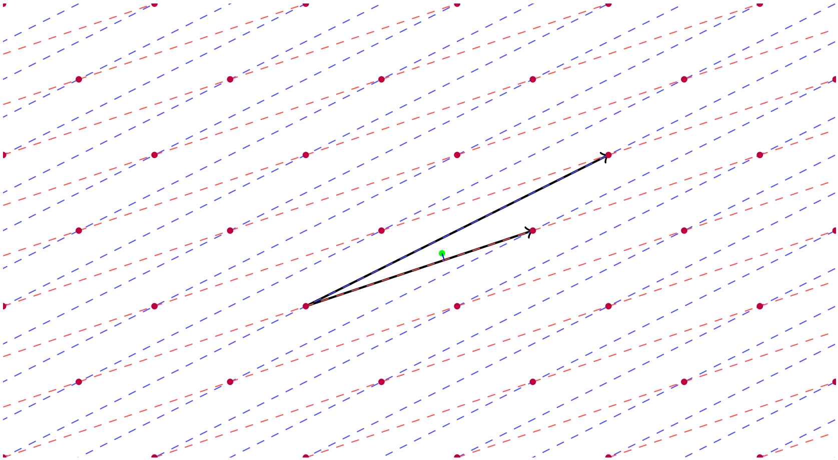
Closest Vector Problem–Dimension two



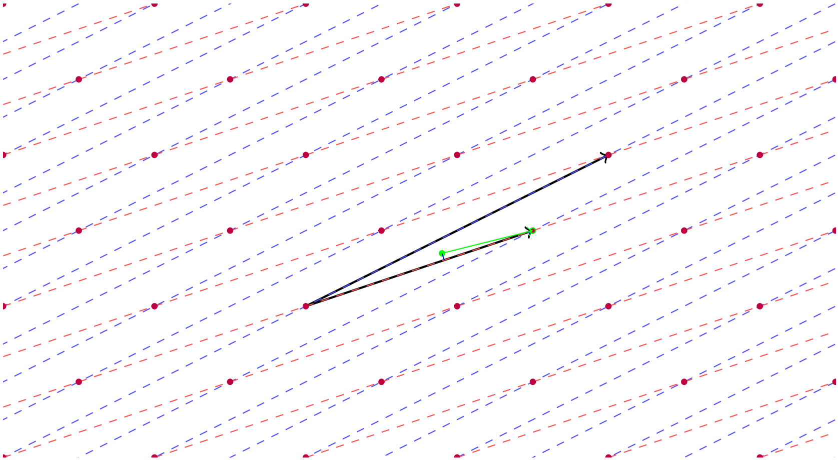
Closest Vector Problem–Dimension two



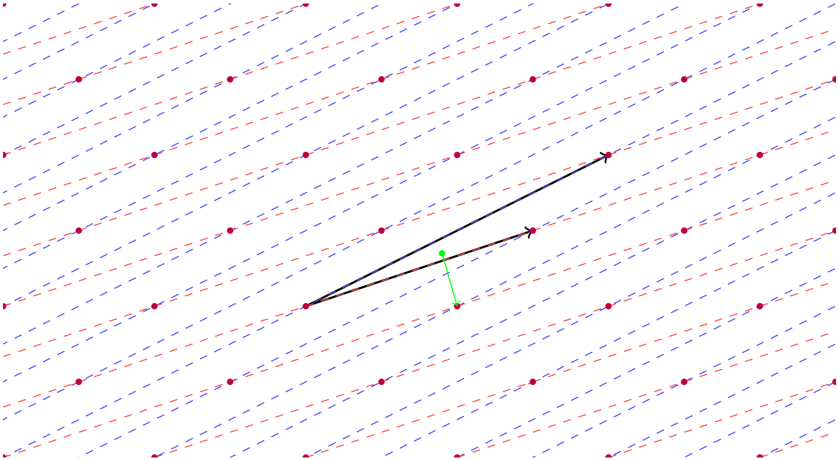
Closest Vector Problem–Dimension two



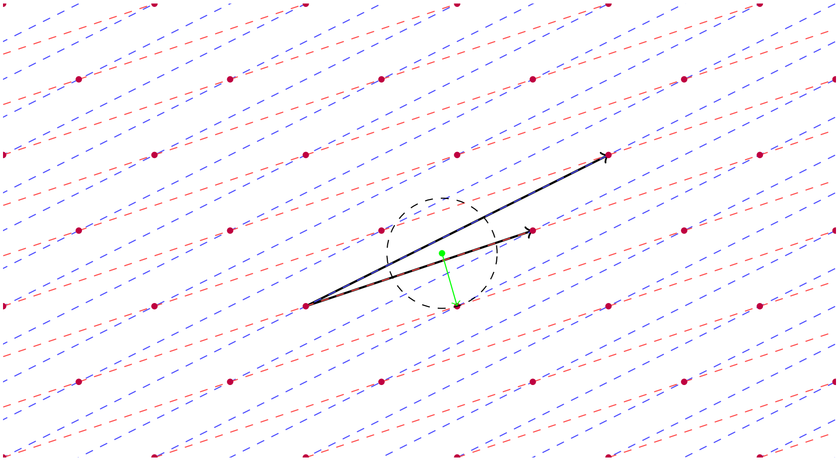
Closest Vector Problem–Dimension two



Closest Vector Problem–Dimension two



Closest Vector Problem–Dimension two



The LLL reduction

There is a polynomial time algorithm to find a vector b_1 in the lattice such that $|b_1| \leq (2/\sqrt{3})^n \lambda_1$, where λ_1 denotes the length of the shortest vector.

LLL explained

$$b_1 = b_1^*$$

$$b_2 = \mu_{2,1} b_1^* + b_2^*$$

$$b_3 = \mu_{3,1} b_1^* + \mu_{3,2} b_2^* + b_3^*$$

$$b_4 = \mu_{4,1} b_1^* + \mu_{4,2} b_2^* + \mu_{4,3} b_3^* + b_4^*$$

LLL explained

$$b_1 = b_1^*$$

$$b_2 = \mu_{2,1} b_1^* + b_2^*$$

$$b_3 = \mu_{3,1} b_1^* + \mu_{3,2} b_2^* + b_3^*$$

$$b_4 = \mu_{4,1} b_1^* + \mu_{4,2} b_2^* + \mu_{4,3} b_3^* + b_4^*$$

LLL explained

$$b_1 = b_1^*$$

$$b_2 = \mu_{2,1} b_1^* + b_2^*$$

$$b_3 = \mu_{3,1} b_1^* + \mu_{3,2} b_2^* + b_3^*$$

$$b_4 = \mu_{4,1} b_1^* + \mu_{4,2} b_2^* + \mu_{4,3} b_3^* + b_4^*$$

LLL explained

$$b_1 = b_1^*$$

$$b_2 = \mu_{2,1} b_1^* + b_2^*$$

$$b_3 = \mu_{3,1} b_1^* + \mu_{3,2} b_2^* + b_3^*$$

$$b_4 = \mu_{4,1} b_1^* + \mu_{4,2} b_2^* + \mu_{4,3} b_3^* + b_4^*$$

LLL explained

$$b_1 = b_1^*$$

$$b_2 = \mu_{2,1} b_1^* + b_2^*$$

$$b_3 = \mu_{3,1} b_1^* + \mu_{3,2} b_2^* + b_3^*$$

$$b_4 = \mu_{4,1} b_1^* + \mu_{4,2} b_2^* + \mu_{4,3} b_3^* + b_4^*$$

Do

1. Calculate b_i^*
2. Apply integral linear operations so $|\mu_{ij}| \leq 1/2$
3. Swap if $\delta |b_i^*| > |\mu_{i+1,i} b_i^* + b_{i+1}^*|$

Until no swapping in the last step

LLL explained

$$b_1 = b_1^*$$

$$b_2 = \mu_{2,1} b_1^* + b_2^*$$

$$b_3 = \mu_{3,1} b_1^* + \mu_{3,2} b_2^* + b_3^*$$

$$b_4 = \mu_{4,1} b_1^* + \mu_{4,2} b_2^* + \mu_{4,3} b_3^* + b_4^*$$

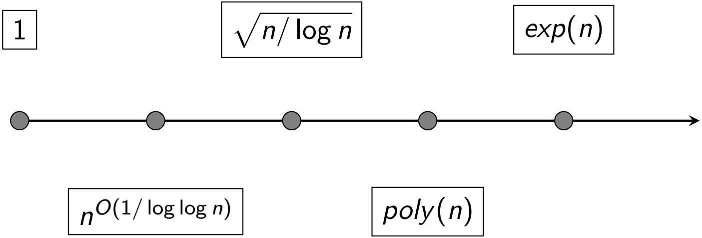
It is δLLL-reduced $(1/4 < \delta < 1)$ if $|\mu_{i,j}| \leq 1/2$ and

$$\begin{aligned}
\delta|b_1^*| &\leq |\mu_{2,1} b_1^* + b_2^*| \\
\delta|b_2^*| &\leq |\mu_{3,2} b_2^* + b_3^*| \\
\delta|b_3^*| &\leq |\mu_{4,3} b_3^* + b_4^*| \\
&\cdots
\end{aligned}$$

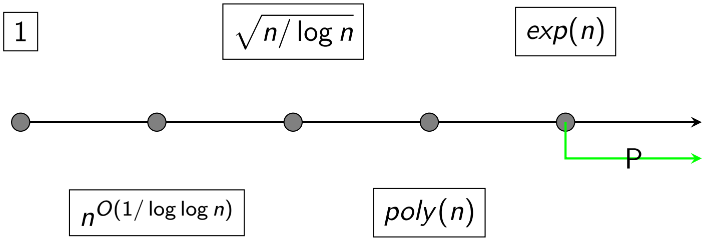
More algorithms for SVP

- Can be found in $4^{n+o(1)}$ arithmetic operations deterministically. (Micciancio-Voulgaris 2010),
- or random $2^{(1+\epsilon)n}$ time (Divesh Aggarwal, Daniel Dadush, Oded Regev, Noah Stephens-Davidowitz 2015).
- For approximation factor 2^k, need time $2^{O(n/k)}$.

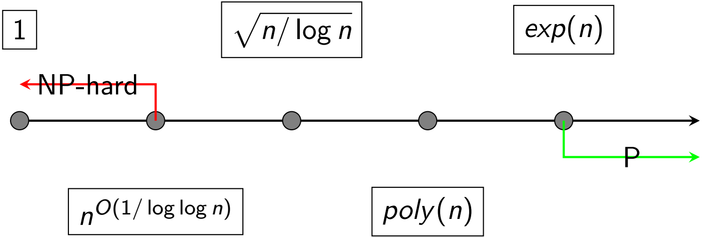
Complexity of approx-SVP



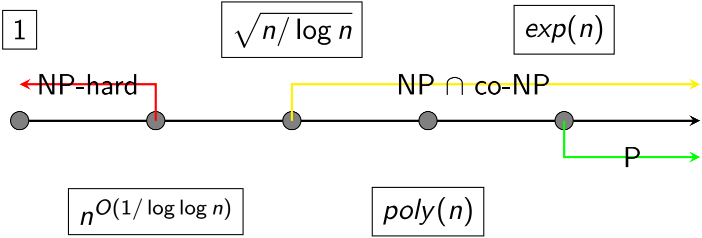
Complexity of approx-SVP



Complexity of approx-SVP



Complexity of approx-SVP



Complexity of approx-SVP