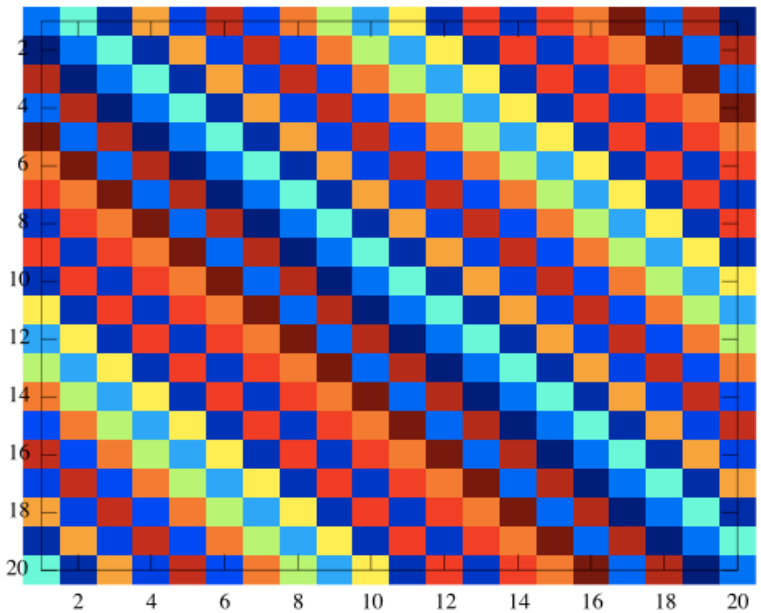
Sieving for Shortest Vectors in Ideal Lattices (work in progress)

Michael Schneider, TU Darmstadt

mischnei@cdc.informatik.tu-darmstadt.de

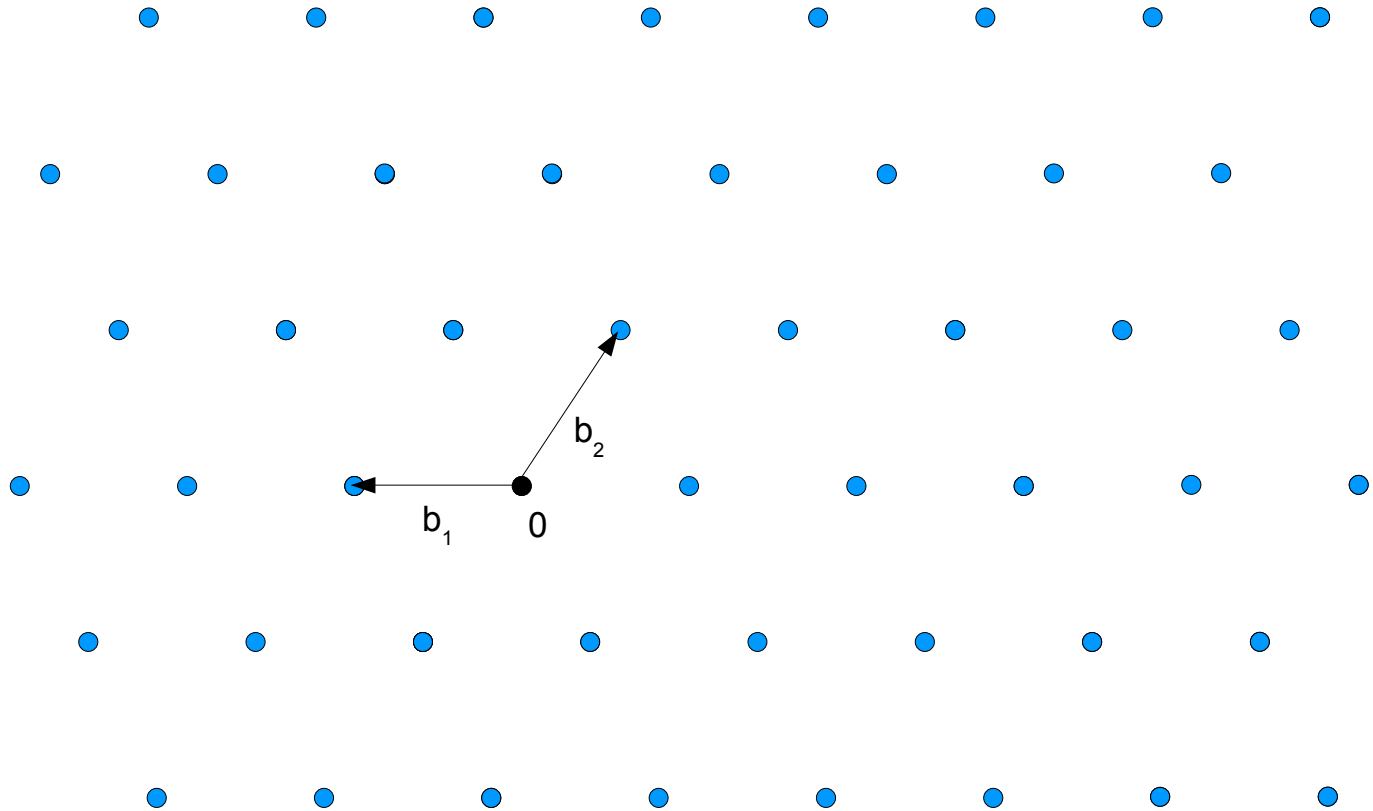
TECHNISCHE UNIVERSITÄT DARMSTADT



PQCrypto 2010 - Recent Results Section

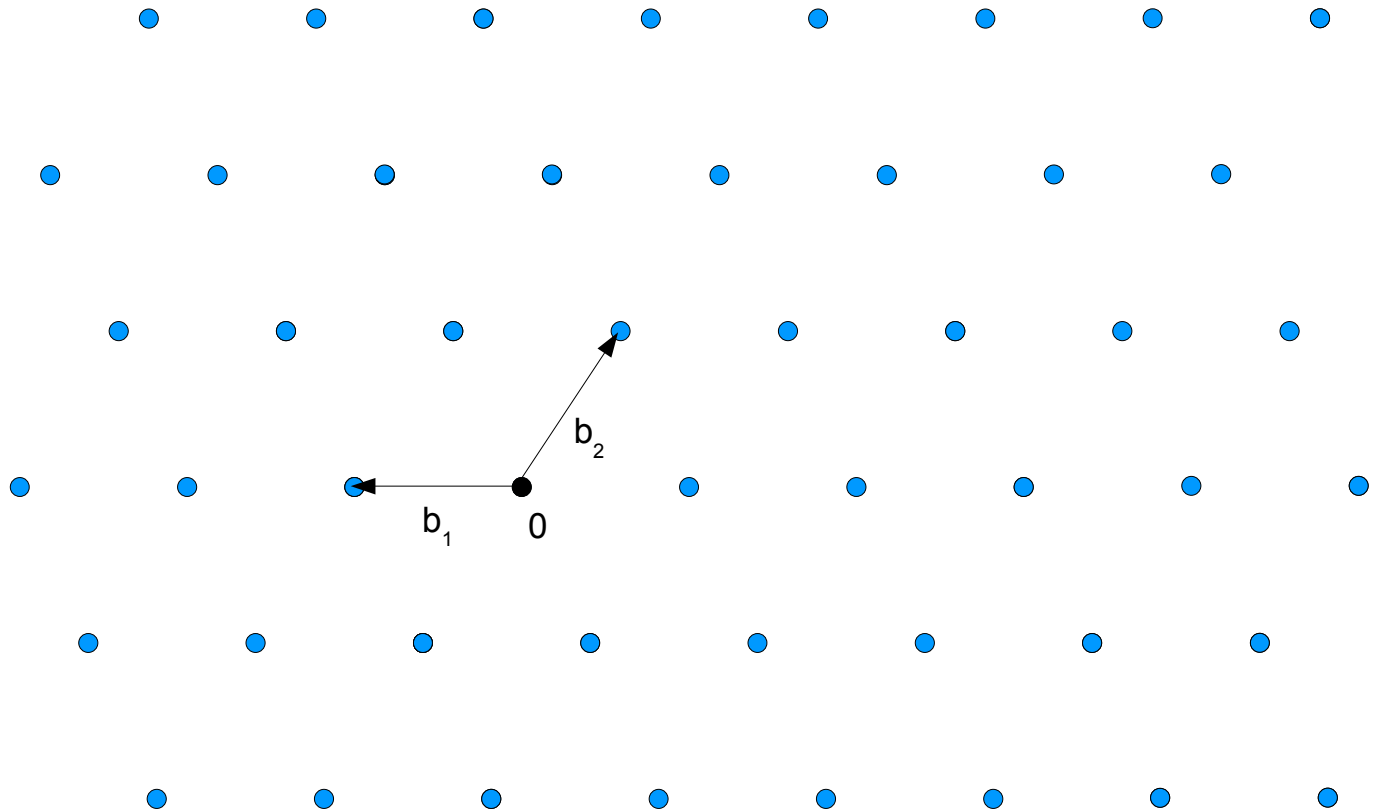
Shortest Vector Problem

TECHNISCHE UNIVERSITÄT DARMSTADT



Shortest Vector Problem

TECHNISCHE UNIVERSITÄT DARMSTADT

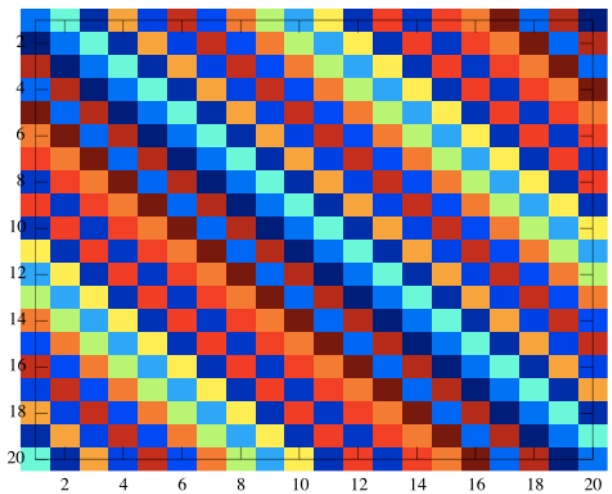


SVP: Given a basis of L, find $\mathbf{v} \in L$ with $\|\mathbf{v}\| = \min_{\mathbf{x} \in L} \|\mathbf{x}\|$

Ideal Lattices

TECHNISCHE UNIVERSITÄT DARMSTADT

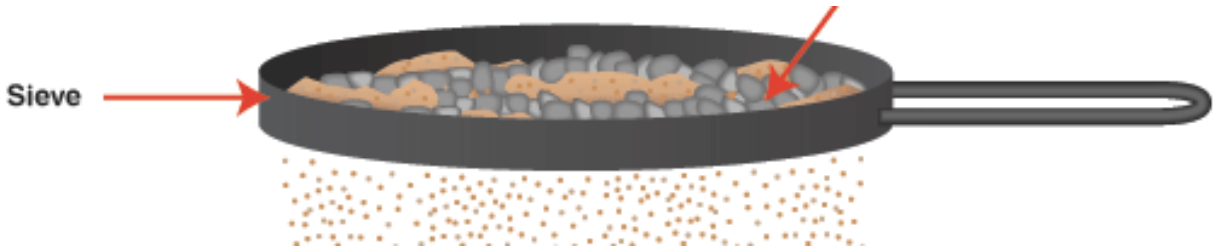
- Lattices of special form
- Used preferably for lattice crypto
- Supposed to be as hard as regular lattices
- For $\mathbf{v} \in L$, also $rot^i(\mathbf{v}) \in L \, \forall \, i = 1 \ldots n-1$



Sieving Algorithms

TECHNISCHE UNIVERSITÄT DARMSTADT

- SVP solver
- Probabilistic
- Exponential runtime $2^{\mathcal{O}(n)}$
- Exponential space $2^{\mathcal{O}(n)}$



Ideal Sieving

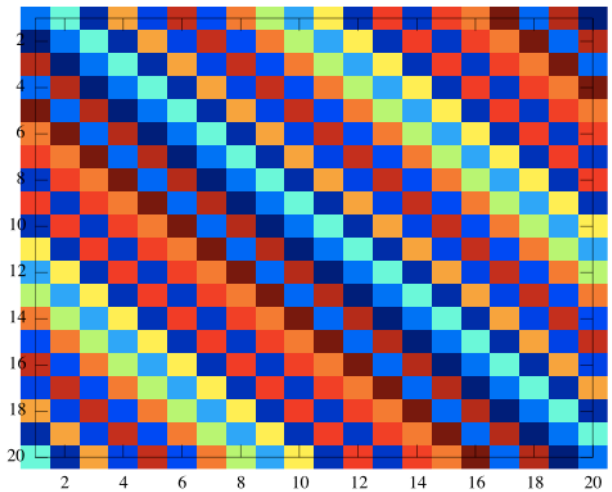
TECHNISCHE UNIVERSITÄT DARMSTADT

Use

Ideal Sieving

TECHNISCHE UNIVERSITÄT DARMSTADT

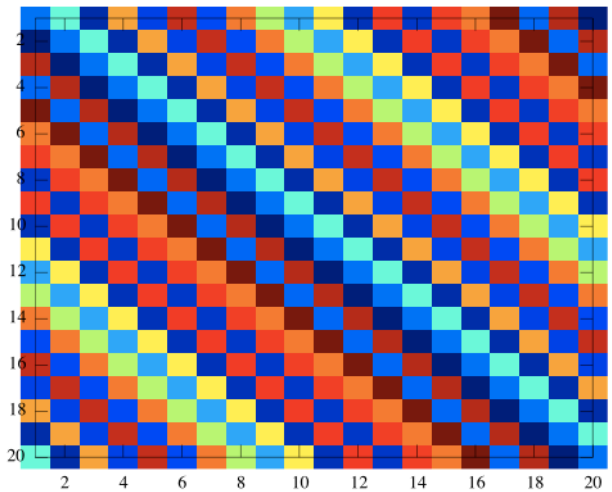
Use



Ideal Sieving

TECHNISCHE UNIVERSITÄT DARMSTADT

Use

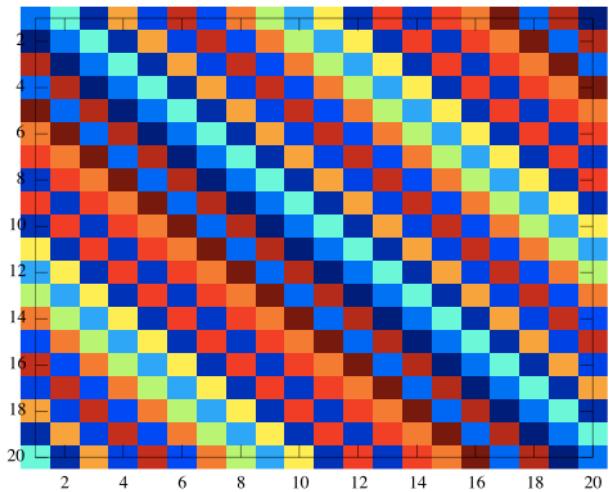


to speed up

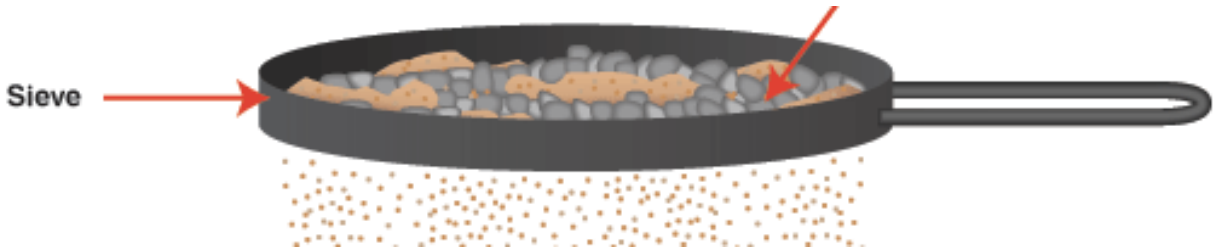
Ideal Sieving

TECHNISCHE UNIVERSITÄT DARMSTADT

Use

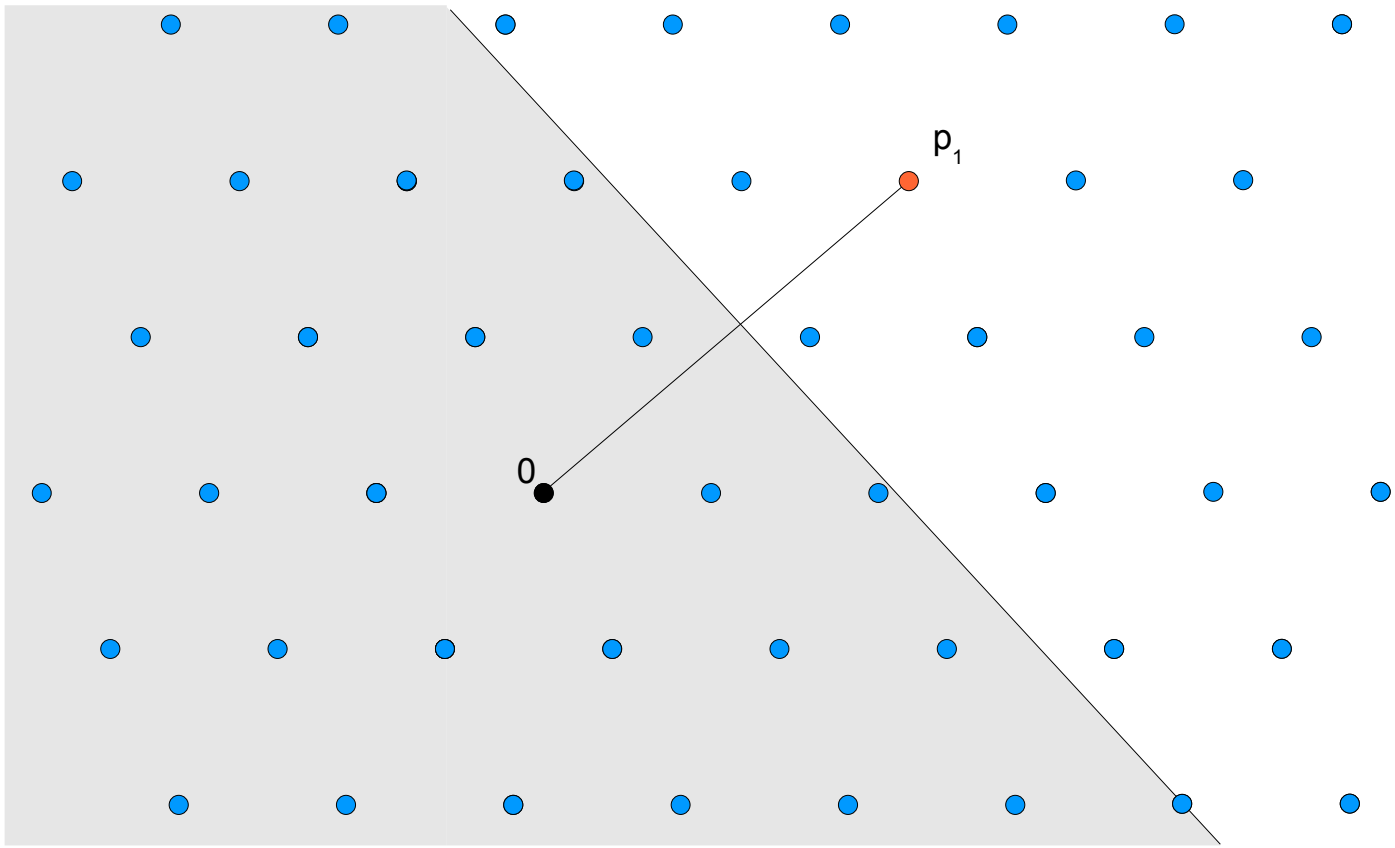


to speed up



Sieving Algorithms

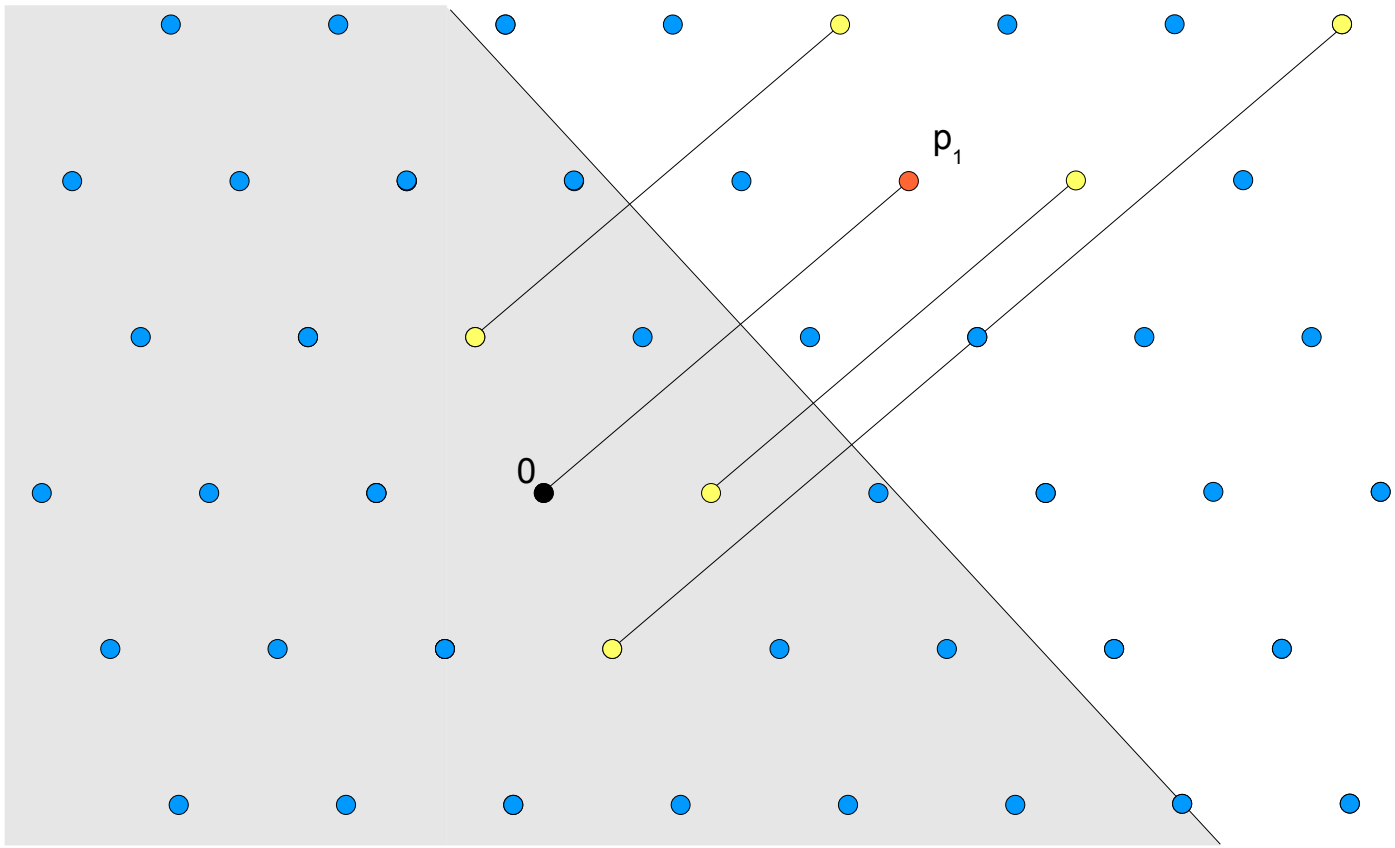
TECHNISCHE UNIVERSITÄT DARMSTADT



$$\cdot = \{\mathbf{x} : \|\mathbf{x} - \mathbf{p_1}\| \geq \|\mathbf{x}\|\}$$

Sieving Algorithms

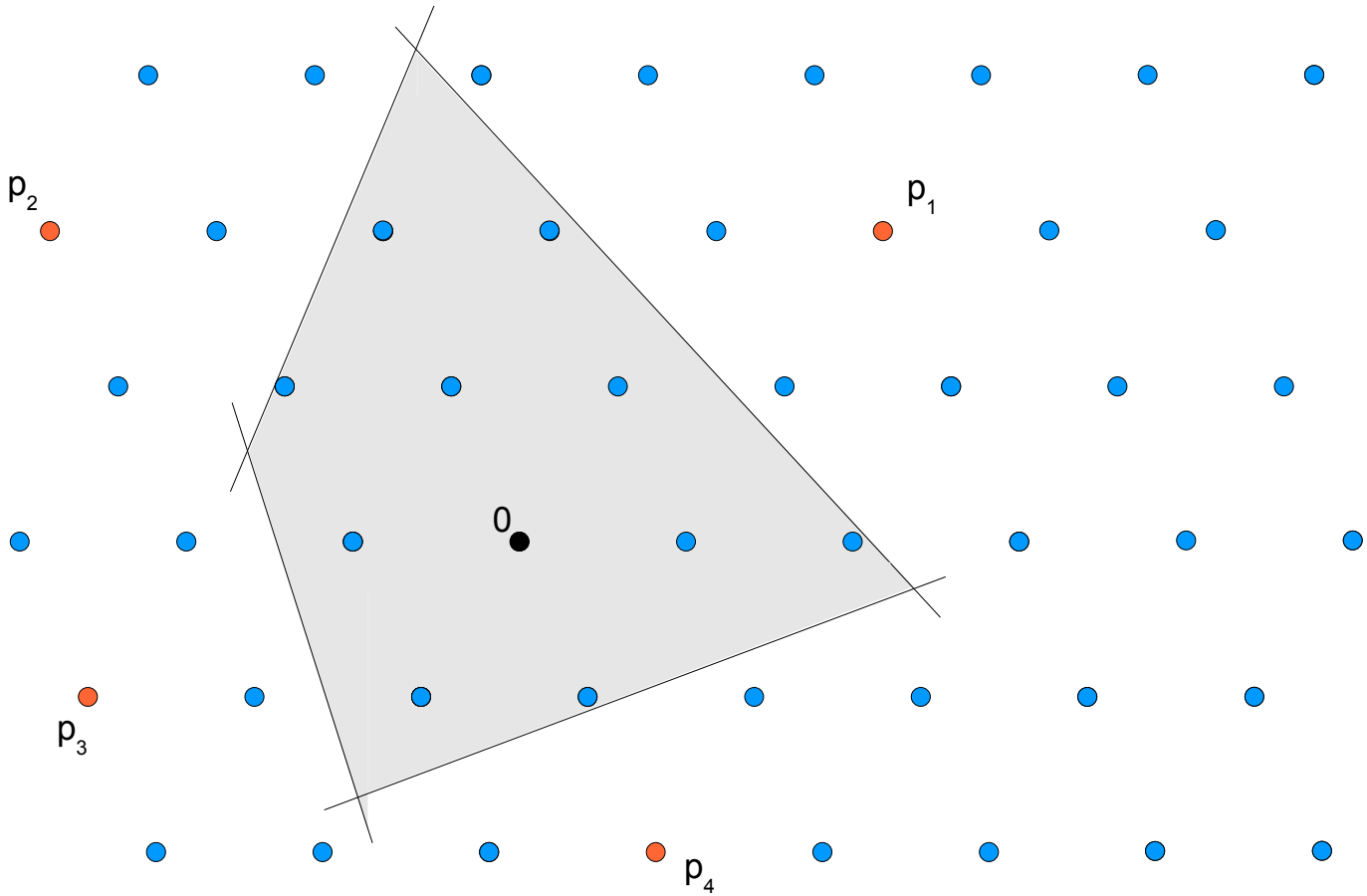
TECHNISCHE UNIVERSITÄT DARMSTADT



reduce points

Sieving Algorithms

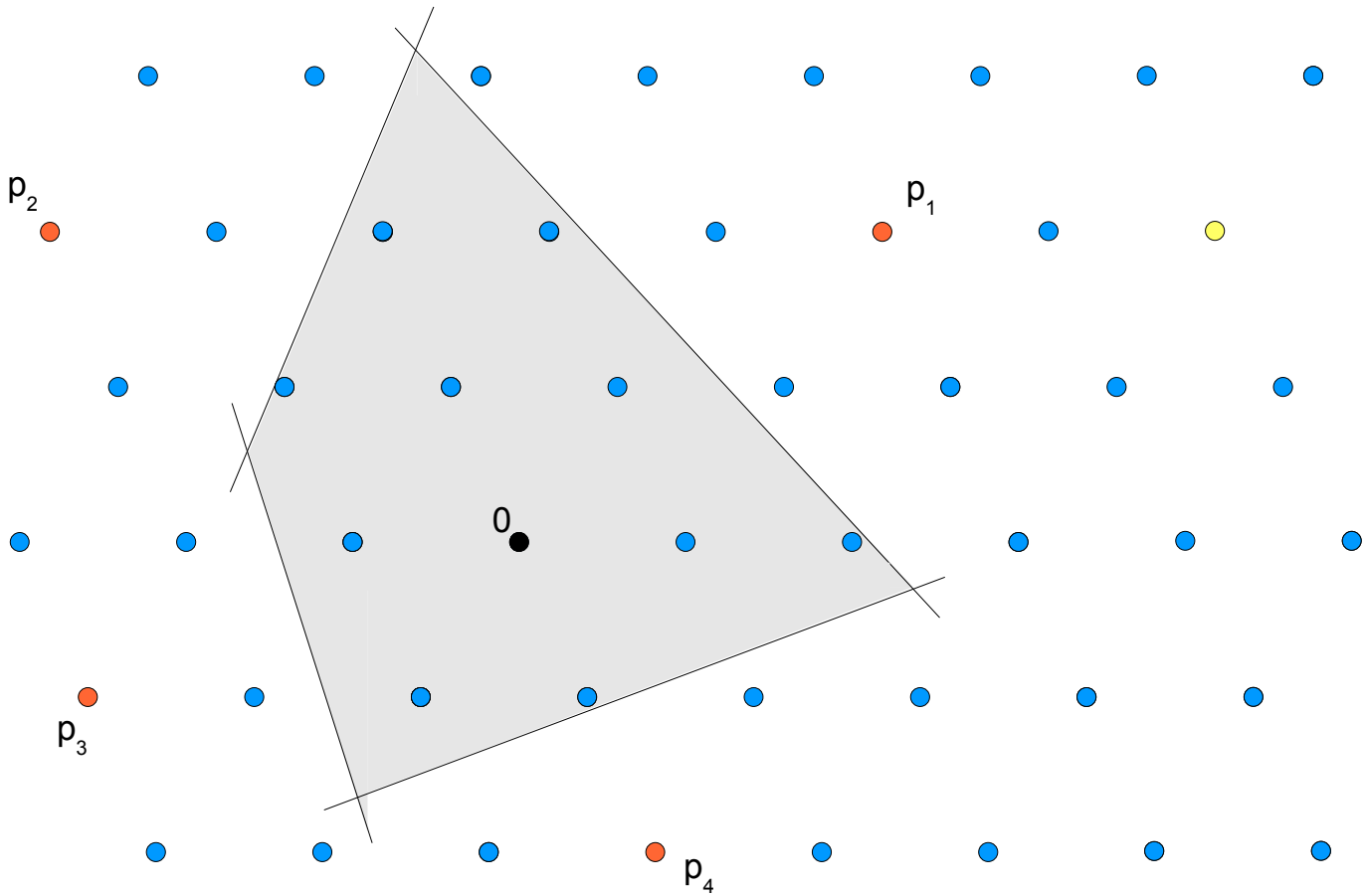
TECHNISCHE UNIVERSITÄT DARMSTADT



intersection of halfspaces

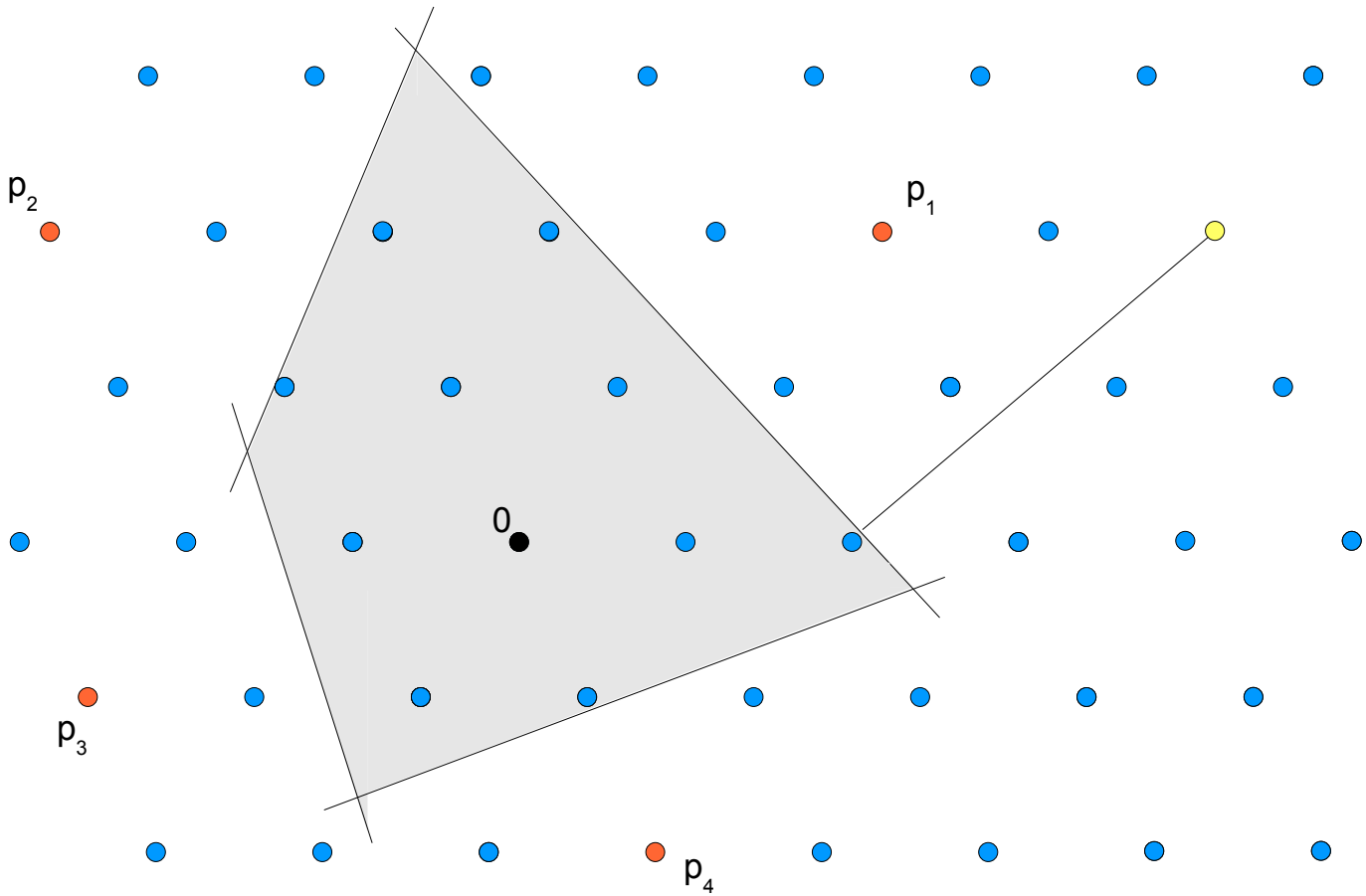
Sieving Algorithms

TECHNISCHE UNIVERSITÄT DARMSTADT



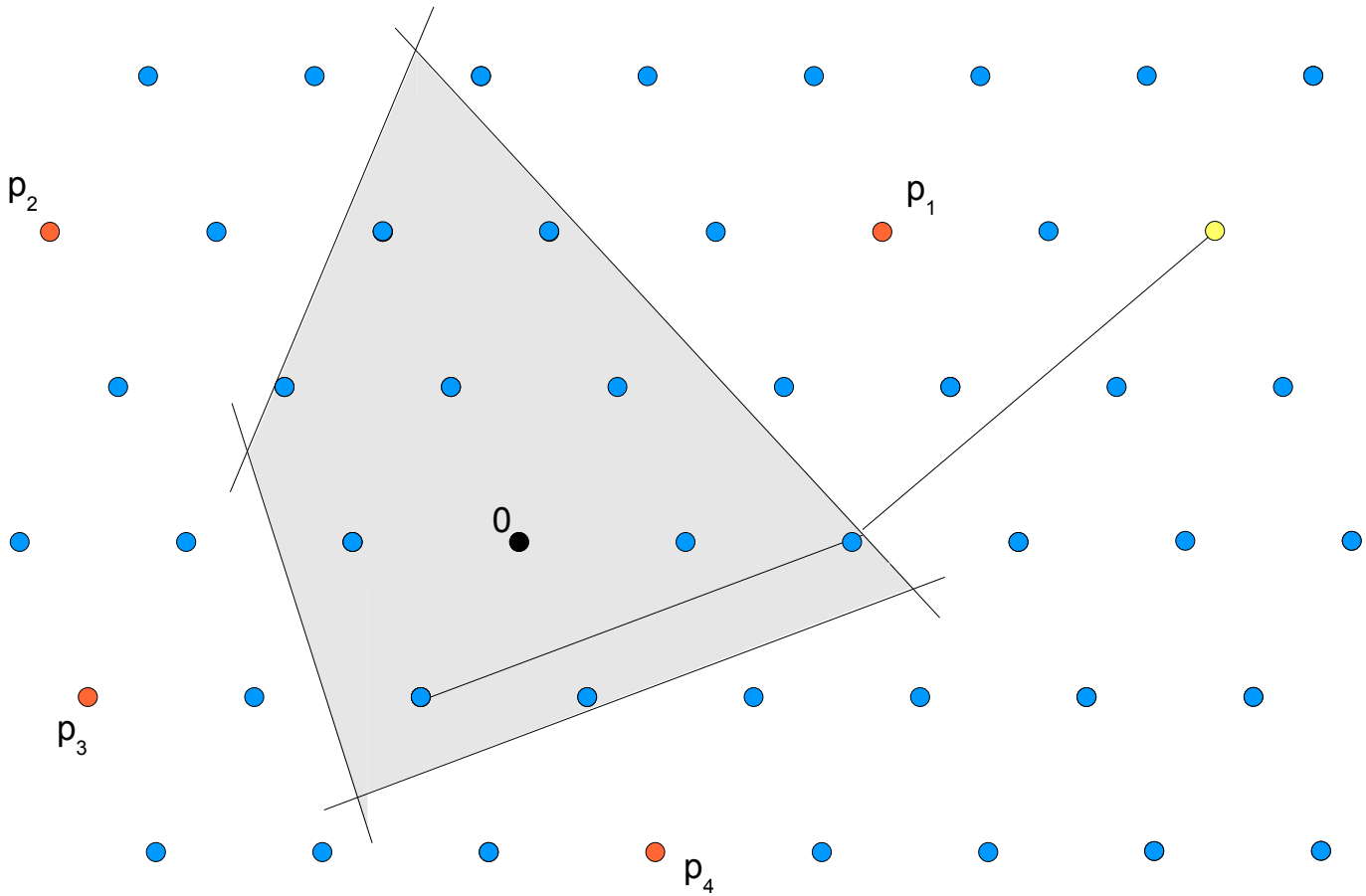
Sieving Algorithms

TECHNISCHE UNIVERSITÄT DARMSTADT



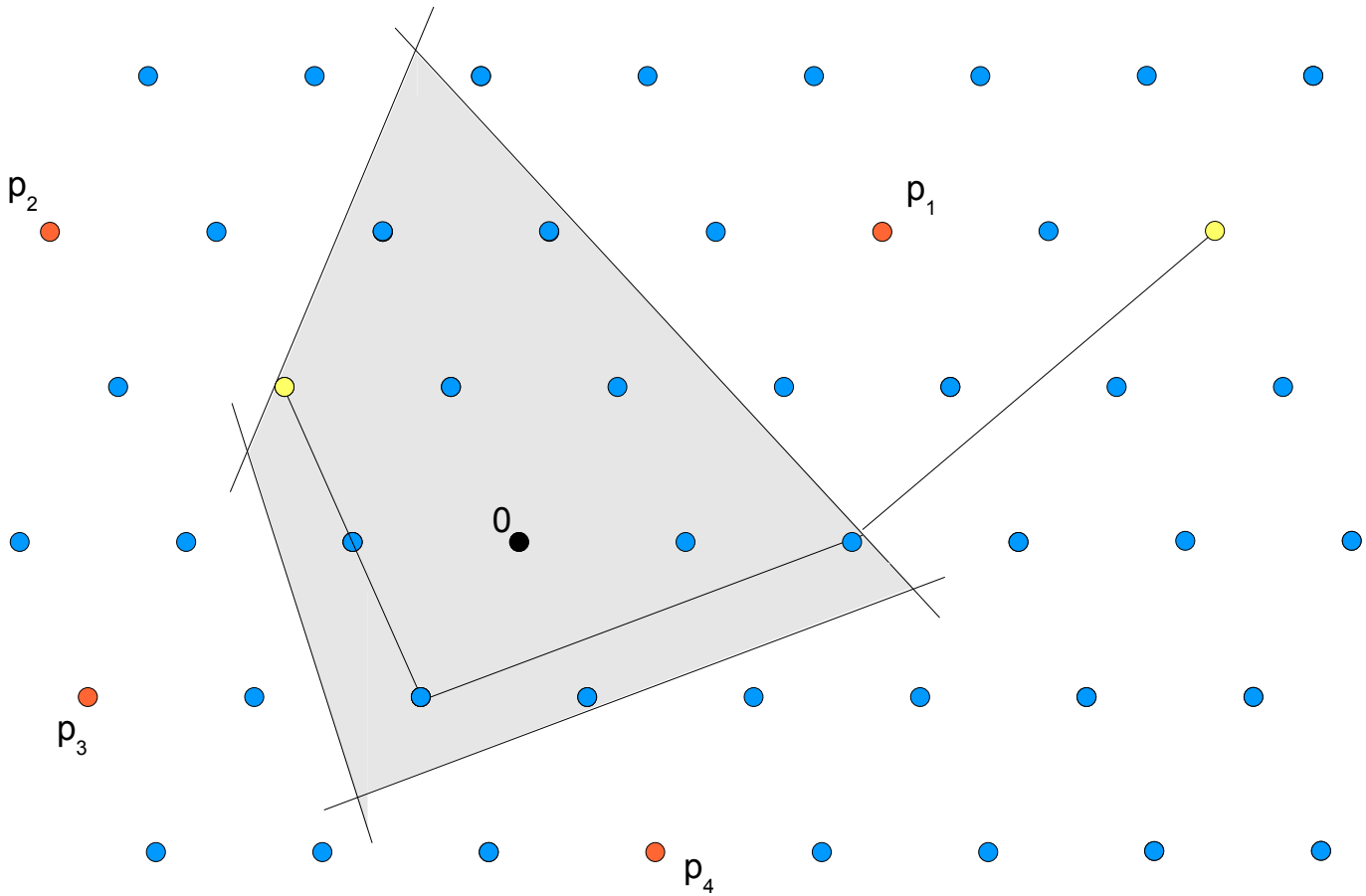
Sieving Algorithms

TECHNISCHE UNIVERSITÄT DARMSTADT



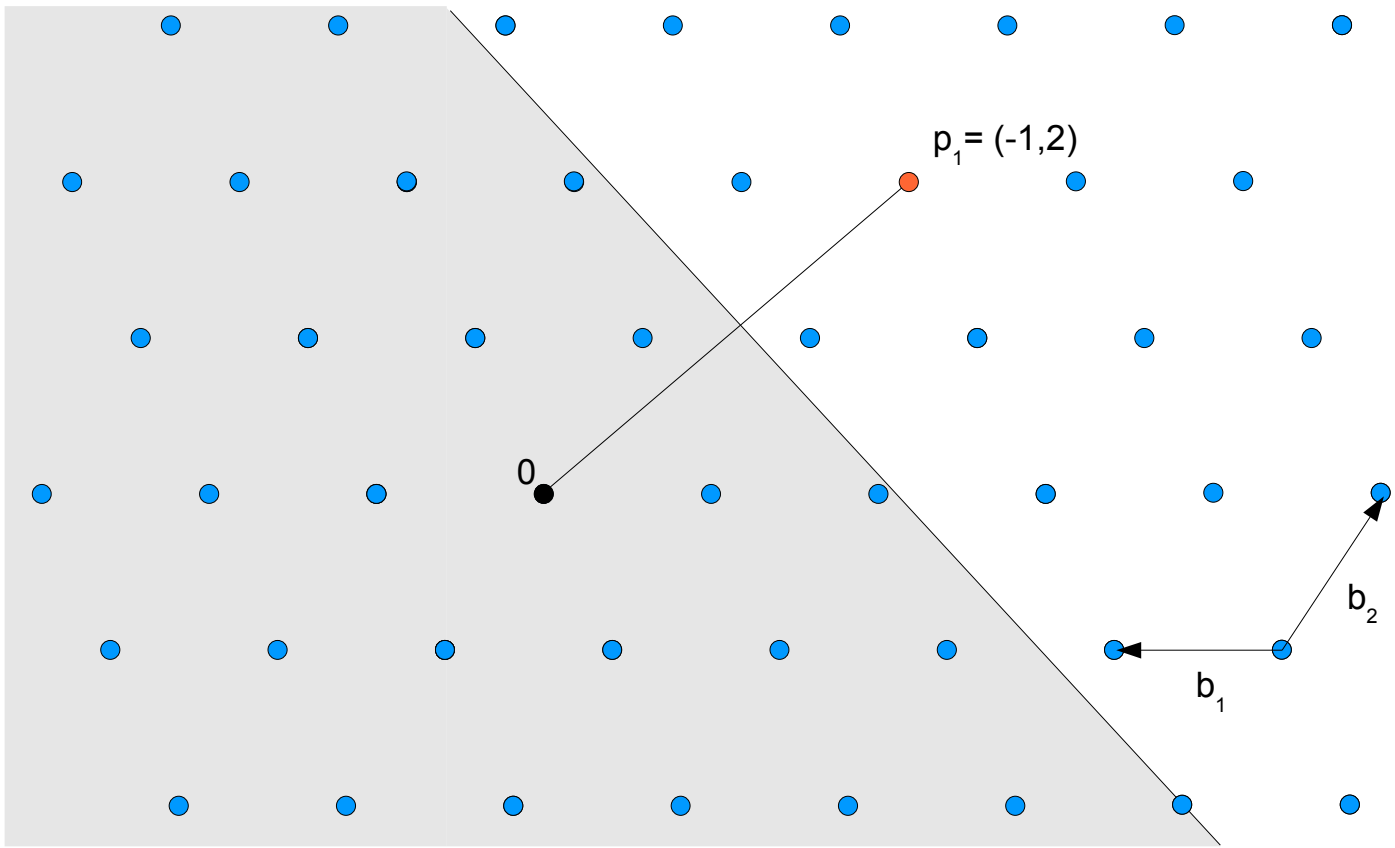
Sieving Algorithms

TECHNISCHE UNIVERSITÄT DARMSTADT



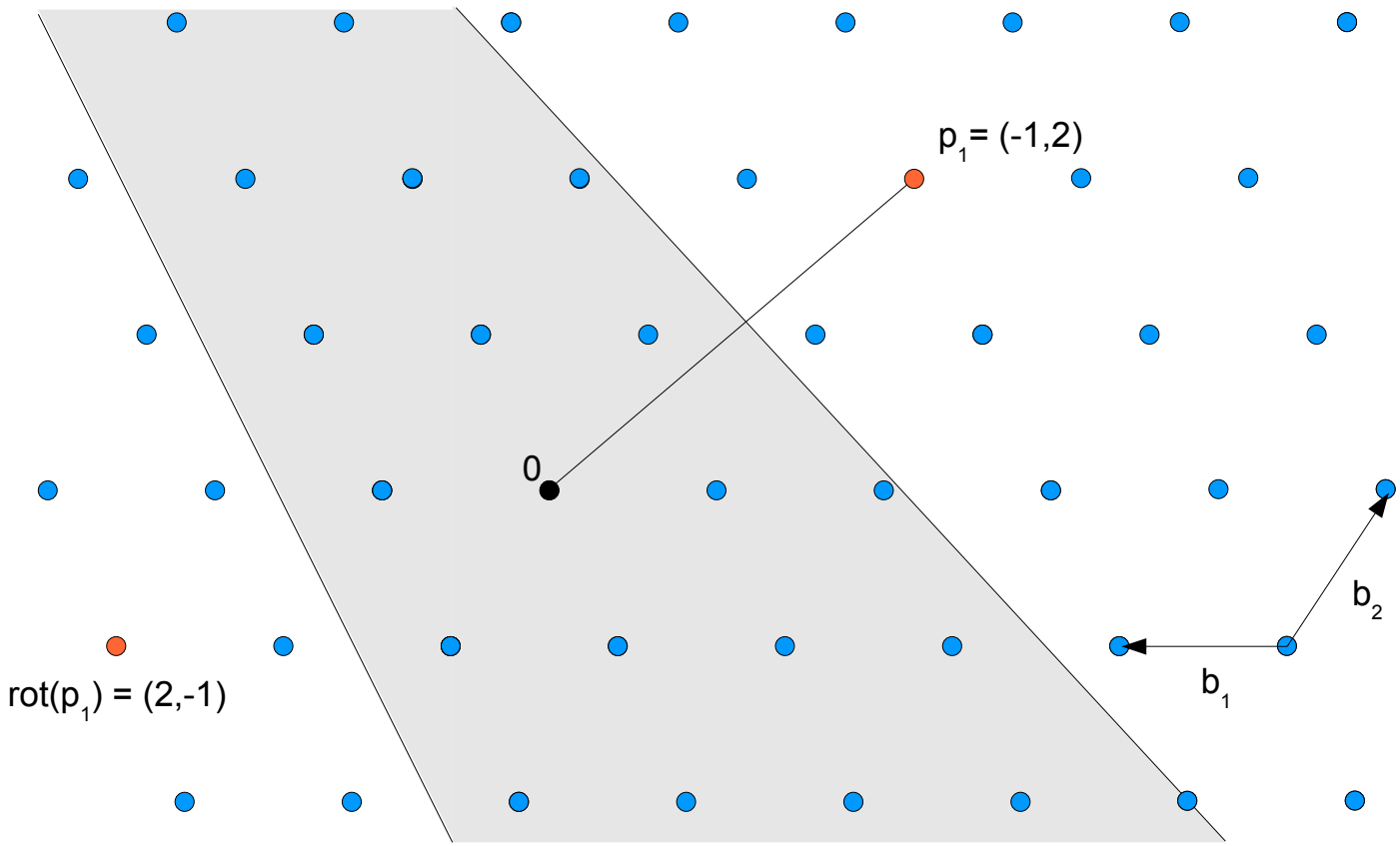
Idea of Ideal Sieving

TECHNISCHE UNIVERSITÄT DARMSTADT



Idea of Ideal Sieving

TECHNISCHE UNIVERSITÄT DARMSTADT



Sieving Algorithms

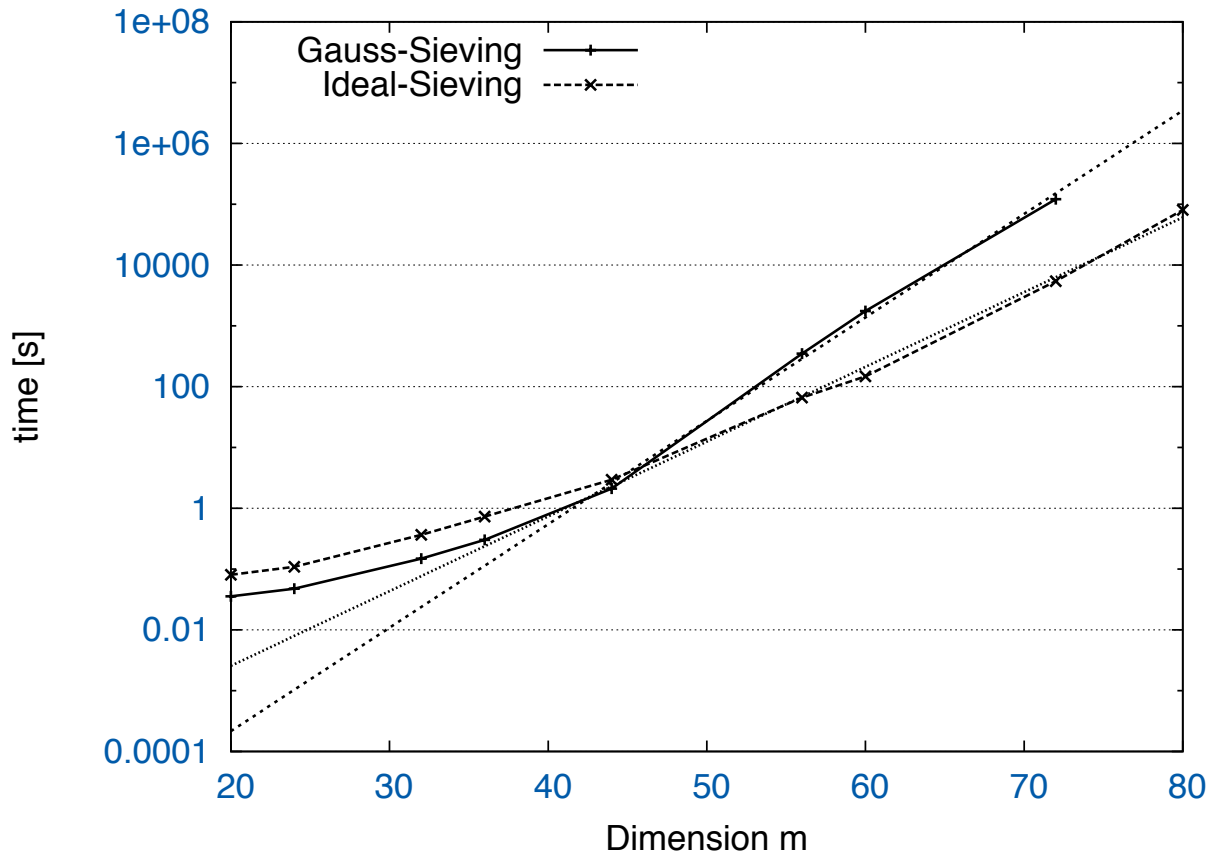
TECHNISCHE UNIVERSITÄT DARMSTADT

Algorithm	Time	Space	Comment
[AKS01]	$2^{\mathcal{O}(m)}$	$2^{\mathcal{O}(m)}$	
[NV08]	$2^{5.9m}$	$2^{2.95m}$	practical
[MV10]	$2^{3.2m}$	$2^{1.33m}$	
[PS10]	$2^{2.46m}$	$2^{1.23m}$	best in theory
[MV10]	$2^{0.52m}$	$2^{0.2m}$	not provable
this work	$2^{0.41m}$	$2^{0.16m}$	only ideal lattices

Experimental Results

TECHNISCHE UNIVERSITÄT DARMSTADT

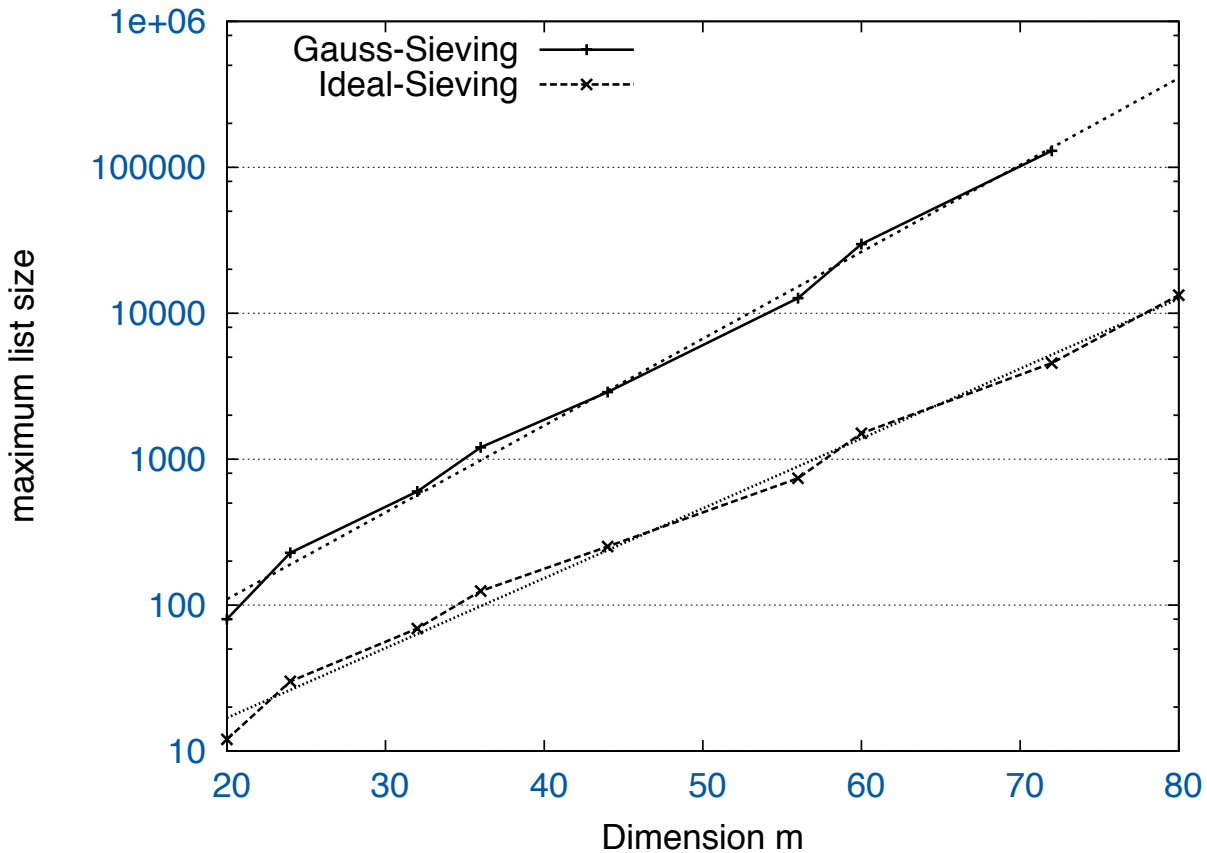
Measured Runtime



Experimental Results

TECHNISCHE UNIVERSITÄT DARMSTADT

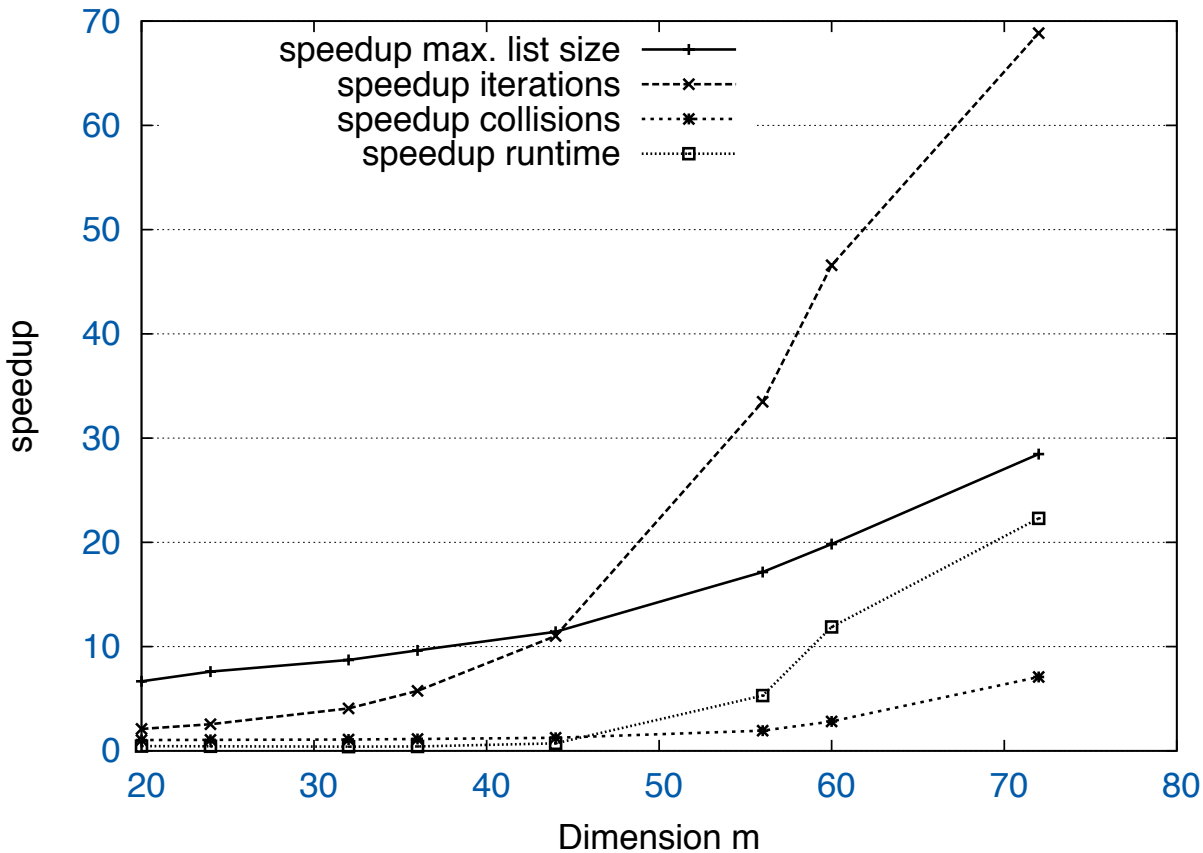
Maximum List Size



Experimental Results

TECHNISCHE UNIVERSITÄT DARMSTADT

Speedups



Future Work

TECHNISCHE UNIVERSITÄT DARMSTADT

- Adapt runtime proof
- ...

Future Work

TECHNISCHE UNIVERSITÄT DARMSTADT

- Adapt runtime proof
- ...

Thank you for your attention!

Bibliography I

TECHNISCHE UNIVERSITÄT DARMSTADT

Miklos Ajtai, Ravi Kumar, and D. Sivakumar.

A sieve algorithm for the shortest lattice vector problem.
In *STOC 2001*, pages 601–610. ACM, 2001.

Daniele Micciancio and Panagiotis Voulgaris.

Faster exponential time algorithms for the shortest vector problem.
In *SODA 2010*, pages 1468–1480, 2010.

Phong Q. Nguyen and Thomas Vidick.

Sieve algorithms for the shortest vector problem are practical.
J. of Mathematical Cryptology, 2(2), 2008.

Xavier Pujol and Damien Stehlé.

Solving the shortest lattice vector problem in time $2^{2.465n}$, 2010.
submitted.