Short Vectors of Planar Lattices via Continued Fractions

Friedrich Eisenbrand

Max-Planck-Institut für Informatik

Outline

Lattices

- Definition of planar integral lattices
- Shortest Vectors
- Applications
- The Gaussian algorithm

Outline

Lattices

- Definition of planar integral lattices
- Shortest Vectors
- Applications
- The Gaussian algorithm

Short vectors and best approximations

- Hermite normal form
- Shortest vectors and best approximations
- Best approximations and convergents
- A naive shortest vector algorithm based on euclid

Outline

Lattices

- Definition of planar integral lattices
- Shortest Vectors
- Applications
- The Gaussian algorithm

Short vectors and best approximations

- Hermite normal form
- Shortest vectors and best approximations
- Best approximations and convergents
- A naive shortest vector algorithm based on euclid

Fast basis reduction

- Identifying the “shortest convergent”
- Computing shortest convergent w.r.t. ℓ_∞-norm with Schönages speedup
- Reduced bases
- Fast basis reduction via (Schönhage 1971) and (Gauß 1801)

Lattices

Lattice generated by A: $\Lambda(A) = \{Ax \mid x \in \mathbf{Z}^2\}$,
where $A \in \mathbf{Z}^{2\times 2}$ nonsingular

Lattices

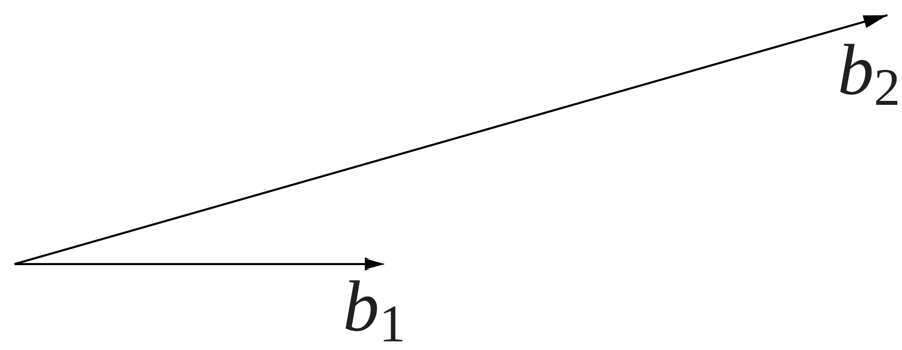
Lattice generated by A: $\Lambda(A) = \{Ax \mid x \in \mathbf{Z}^2\}$,
where $A \in \mathbf{Z}^{2\times 2}$ nonsingular

A basis of Λ

Lattices

Lattice generated by A: $\Lambda(A) = \{Ax \mid x \in \mathbf{Z}^2\}$, where $A \in \mathbf{Z}^{2\times 2}$ nonsingular

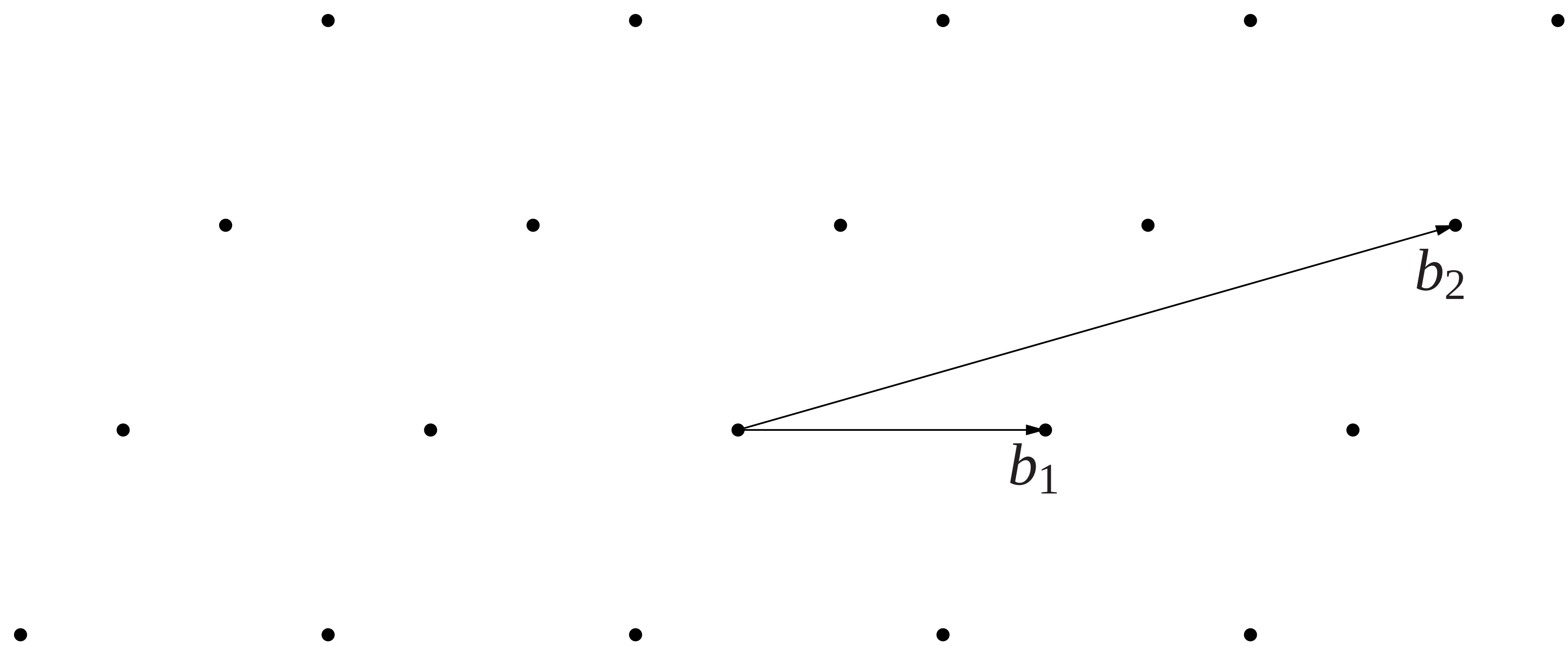
A basis of Λ



Lattices

Lattice generated by A: $\Lambda(A) = \{Ax \mid x \in \mathbf{Z}^2\}$,
where $A \in \mathbf{Z}^{2\times 2}$ nonsingular

A basis of Λ



Shortest vectors

Shortest vector of Λ: $v \in \Lambda$ with $v \neq 0$ and $\|v\| \leqslant \|u\|$ for all $u \in \Lambda$
$u \neq 0$

Shortest vectors

Shortest vector of Λ: $v \in \Lambda$ with $v \neq 0$ and $\|v\| \leqslant \|u\|$ for all $u \in \Lambda$
$u \neq 0$

Applications

- Integer programming in fixed dimension Lenstra (1983)
- Factorization of rational polynomials Lenstra, Lenstra & Lovász (1982)
- Strongly polynomial time algorithms in combinatorial optimization Frank & Tardosz (1987)

Shortest vectors

Shortest vector of Λ: $v \in \Lambda$ with $v \neq 0$ and $\|v\| \leqslant \|u\|$ for all $u \in \Lambda$
$u \neq 0$

Applications

- Integer programming in fixed dimension Lenstra (1983)
- Factorization of rational polynomials Lenstra, Lenstra & Lovász (1982)
- Strongly polynomial time algorithms in combinatorial optimization Frank & Tardosz (1987)

Shortest vectors

Shortest vector of Λ: $v \in \Lambda$ with $v \neq 0$ and $\|v\| \leqslant \|u\|$ for all $u \in \Lambda$ $u \neq 0$

Applications

- Integer programming in fixed dimension Lenstra (1983)
- Factorization of rational polynomials Lenstra, Lenstra & Lovász (1982)
- Strongly polynomial time algorithms in combinatorial optimization Frank & Tardosz (1987)

Unimodular transformations

Unimodular transformation of basis A:

$$A \cdot U,$$

where $U \in \mathbf{Z}^{2\times 2}$ with $\det(U) = \pm 1$, .i.e., U unimodular

Unimodular transformations

Unimodular transformation of basis A:

$$A \cdot U,$$

where $U \in \mathbf{Z}^{2\times 2}$ with $\det(U) = \pm 1$, .i.e., U unimodular

Matrix A basis of Λ if and only if $A \cdot U$ basis of Λ, U unimodular

Unimodular transformations

Unimodular transformation of basis A:

$$A \cdot U,$$

where $U \in \mathbf{Z}^{2\times 2}$ with $\det(U) = \pm 1$, .i.e., U unimodular

Matrix A basis of Λ if and only if $A \cdot U$ basis of Λ, U unimodular

Examples of unimodular transformations

- swapping of columns

Unimodular transformations

Unimodular transformation of basis A:

$$A \cdot U,$$

where $U \in \mathbf{Z}^{2\times 2}$ with $\det(U) = \pm 1$, .i.e., U unimodular

Matrix A basis of Λ if and only if $A \cdot U$ basis of Λ, U unimodular

Examples of unimodular transformations

- swapping of columns
- adding integral multiples of one column to another

The Gaussian reduction algorithm

GAUSS(b_1, b_2)

repeat

arrange that b_1 is the shorter vector of b_1 and b_2

find $k \in \mathbf{Z}$ such that $b_2 - kb_1$ is of minimal euclidean length

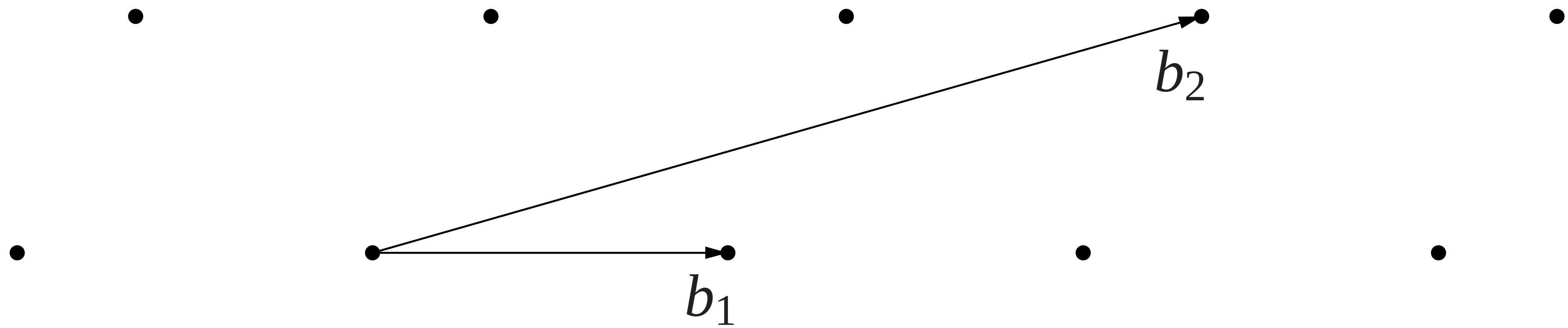
$b_2 \leftarrow (b_2 - kb_1)$ (normalization step)

until $k = 0$

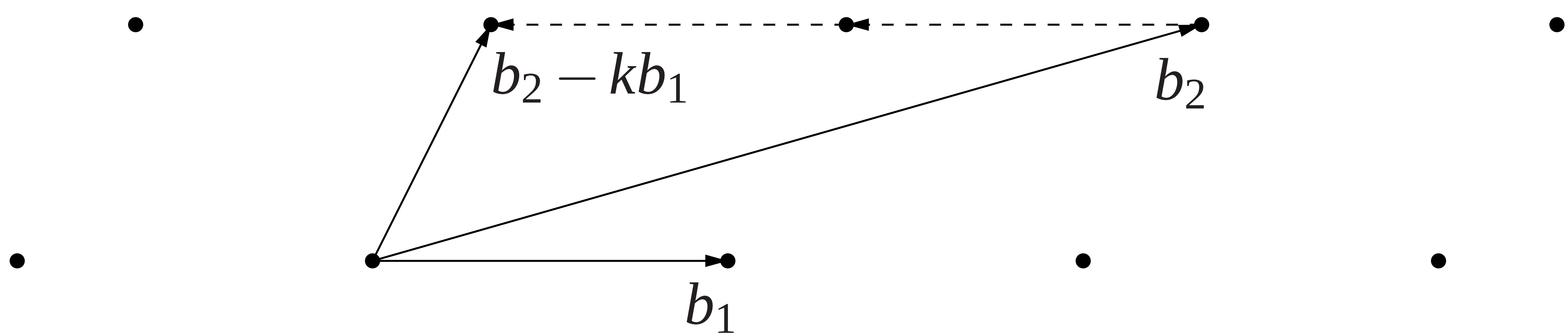
return (b_1, b_2)

k in **repeat**-loop is nearest integer to $(b_1^T b_2)/(b_1^T b_1)$

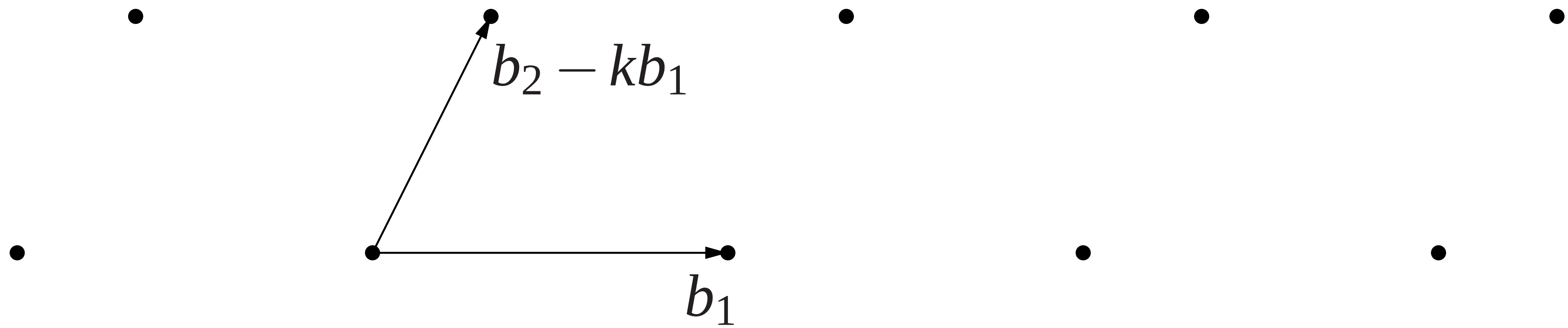
A normalization step



A normalization step



A normalization step



Complexity of GAUSS

- Lagarias (1980): Complexity of GAUSS $O(n^3)$

Complexity of GAUSS

- Lagarias (1980): Complexity of GAUSS $O(n^3)$
- Schönhage (1991) and Yap (1992) new reduction algorithm: Complexity $O(M(n)\log n)$ where $M(n)$: complexity of n-bit integer multiplication;

Complexity of GAUSS

- Lagarias (1980): Complexity of GAUSS $\mathrm{O}(n^3)$
- Schönhage (1991) and Yap (1992) new reduction algorithm: Complexity $\mathrm{O}(M(n)\log n)$ where $M(n)$: complexity of n-bit integer multiplication;

  algorithms fairly involved

Complexity of GAUSS

- Lagarias (1980): Complexity of GAUSS $O(n^3)$

- Schönhage (1991) and Yap (1992) new reduction algorithm: Complexity $O(M(n)\log n)$ where $M(n)$: complexity of n-bit integer multiplication;

  algorithms fairly involved

- This talk: Fast basis reduction via Schönhage's (1971) classical gcd-speedup and GAUSS

The Hermite Normal Form

Given lattice basis $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathbf{Z}^{2\times 2}$, compute integers x, y with $\gcd(a_3, a_4) = d = xa_3 + ya_4$

$\begin{pmatrix} a_4/d & x \\ -a_3/d & y \end{pmatrix}$ unimodular

The Hermite Normal Form

Given lattice basis $A = \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathbf{Z}^{2\times 2}$, compute integers x, y with $\gcd(a_3, a_4) = d = xa_3 + ya_4$

$\left(\begin{smallmatrix} a_4/d & x \\ -a_3/d & y \end{smallmatrix}\right)$ unimodular

Then

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} a_4/d & x \\ -a_3/d & y \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathbf{Z}^{2\times 2}$$

The Hermite Normal Form

Given lattice basis $A = \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathbf{Z}^{2\times 2}$, compute integers x, y with $\gcd(a_3, a_4) = d = xa_3 + ya_4$

$\left(\begin{smallmatrix} a_4/d & x \\ -a_3/d & y \end{smallmatrix}\right)$ unimodular

Then

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} a_4/d & x \\ -a_3/d & y \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathbf{Z}^{2\times 2}$$

We can assume that $c > 0$ and $a > b \geqslant 0$

Hermite normal form

Complexity of Hermite normal form

Given integers a and b one can compute integers x and y with

$$\gcd(a,b) = xa + yb$$

in time $O(M(n)\log n)$ (Schönhage 1971)

Complexity of HNF: $O(M(n)\log n)$

Complexity of Hermite normal form

Given integers a and b one can compute integers x and y with

$$\gcd(a,b) = xa + yb$$

in time $\mathrm{O}(M(n)\log n)$ (Schönhage 1971)

Complexity of HNF: $\mathrm{O}(M(n)\log n)$

Assuming: Lattice is given by its Hermite normal form

Best approximations

For $\alpha \in Q$, fraction x/y is best approximation if all other fractions x'/y' with $y' \leqslant y$ satisfy

$$|y'\alpha - x'| > |y\alpha - x|$$

Shortest vectors and best approximations

$$\Lambda = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \;\middle|\; x, y \in \mathbf{Z} \right\}$$

Theorem. *There exists a shortest vector* $\binom{-xa+yb}{yc}$, $x \in \mathbf{N}_0$, $y \in \mathbf{N}_+$ *of* Λ *such that at least one of the following conditions is satisfied.*

Shortest vectors and best approximations

$$\Lambda = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mid x, y \in \mathbf{Z} \right\}$$

Theorem. *There exists a shortest vector* $\binom{-xa+yb}{yc}$, $x \in \mathbf{N}_0$, $y \in \mathbf{N}_+$ *of* Λ *such that at least one of the following conditions is satisfied.*

- *The fraction* x/y *is a best approximation to the number* b/a.

Shortest vectors and best approximations

$$\Lambda = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mid x, y \in \mathbf{Z} \right\}$$

Theorem. *There exists a shortest vector* $\left(\begin{smallmatrix} -xa+yb \\ yc \end{smallmatrix}\right)$, $x \in \mathbf{N}_0$, $y \in \mathbf{N}_+$ *of* Λ *such that at least one of the following conditions is satisfied.*

- *The fraction* x/y *is a best approximation to the number* b/a.
- *If the fraction* p/q *is the reduced representation of* b/a*, then* p *is odd,* q *is even,* $x \in \{\lfloor p/2 \rfloor, \lceil p/2 \rceil\}$ *and* $y = q/2$.

Best approximations via euclidean algorithm

x/y best approximation of b/a, then x/y is a convergent of b/a

Best approximations via euclidean algorithm

x/y best approximation of b/a, then x/y is a convergent of b/a

Convergents of $\alpha \in \mathbf{Q}$ inductively defined

Best approximations via euclidean algorithm

x/y best approximation of b/a, then x/y is a convergent of b/a

Convergents of $\alpha \in \mathbf{Q}$ inductively defined

- $\lfloor \alpha \rfloor$

Best approximations via euclidean algorithm

x/y best approximation of b/a, then x/y is a convergent of b/a

Convergents of $\alpha \in \mathbf{Q}$ inductively defined

- $\lfloor \alpha \rfloor$
- $\lfloor \alpha \rfloor + 1/c$, where c convergent of $1/(\alpha - \lfloor \alpha \rfloor)$

The Gregorian calendar

The earth turns around the sun in $365 + 104\,629/432\,000$ days.

First convergent is 365

The Gregorian calendar

The earth turns around the sun in $365 + 104\,629/432\,000$ days.

First convergent is 365

Second convergent: $365 + 1/4$, since 4 is first convergent of $432\,000/104\,629 = 4 + 13\,484/104\,629$

The Gregorian calendar

The earth turns around the sun in $365 + 104\,629/432\,000$ days.

First convergent is 365

Second convergent: $365 + 1/4$, since 4 is first convergent of $432\,000/104\,629 = 4 + 13\,484/104\,629$

Leap year all 4 years

The Gregorian calendar

Pope Gregor XIII (1582) used fifth convergent

$$365 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{6}}}}} = 365 + 194/801$$

The Gregorian calendar

Pope Gregor XIII (1582) used fifth convergent

$$365 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{6}}}}} = 365 + 194/801$$

Every 800 years skip 6 leap years; every year divisible by 100 but not by 400

The Gregorian calendar

Pope Gregor XIII (1582) used fifth convergent

$$365 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{6}}}}} = 365 + 194/801$$

Every 800 years skip 6 leap years; every year divisible by 100 but not by 400

The first year the in which calendar is 1 day ahead is 4915

Computing convergents

Euclidean algorithm

$\textsc{ExGCD}(a,b)$

$M \leftarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$n \leftarrow 0$

while $(b \neq 0)$ **do**

$\quad q \leftarrow \lfloor a/b \rfloor$

$\quad M \leftarrow M \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}$

$\quad (a,b) \leftarrow (b, a-qb)$

$\quad n \leftarrow n+1$

return $(d = a, x = (-1)^n M_{2,2}, y = (-1)^{n+1} M_{1,2})$

Computing convergents

Let $M^{(k)}$, $k \geqslant 0$, denote M after k-th iteration of while-loop

Computing convergents

Let $M^{(k)}$, $k \geqslant 0$, denote M after k-th iteration of while-loop

Well known fact:

k-th convergent of a/b is $M^{(k)}_{1,1}/M^{(k)}_{2,1}$

Naive shortest vector algorithm

- Compute Hermite normal form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ of A

Naive shortest vector algorithm

- Compute Hermite normal form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ of A
- Compute reduced fraction p/q of b/a and vectors $(-\lfloor p/2 \rfloor a + \lfloor q/2 \rfloor b, \lfloor q/2 \rfloor c)^T$ and $(a,0)^T$ store shortest one in MIN

Naive shortest vector algorithm

- Compute Hermite normal form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ of A
- Compute reduced fraction p/q of b/a and vectors $(-\lfloor p/2 \rfloor a + \lfloor q/2 \rfloor b, \lfloor q/2 \rfloor c)^T$ and $(a,0)^T$ store shortest one in MIN
- Compute convergents g_k/h_k of b/a with $\text{EXGCD}(b,a)$ and compare the length of the induced vector $(-g_k a + h_k b, h_k c)^T$ with MIN. If shorter, replace MIN

Naive shortest vector algorithm

- Compute Hermite normal form $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ of A
- Compute reduced fraction p/q of b/a and vectors $(-\lfloor p/2 \rfloor a + \lfloor q/2 \rfloor b, \lfloor q/2 \rfloor c)^T$ and $(a, 0)^T$ store shortest one in MIN
- Compute convergents g_k/h_k of b/a with EXGCD(b, a) and compare the length of the induced vector $(-g_k a + h_k b, h_k c)^T$ with MIN. If shorter, replace MIN

  In the end MIN contains a shortest vector

Naive shortest vector algorithm

- Compute Hermite normal form $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ of A
- Compute reduced fraction p/q of b/a and vectors $(-\lfloor p/2 \rfloor a + \lfloor q/2 \rfloor b, \lfloor q/2 \rfloor c)^T$ and $(a,0)^T$ store shortest one in MIN
- Compute convergents g_k/h_k of b/a with $\textsc{exgcd}(b,a)$ and compare the length of the induced vector $(-g_k a + h_k b, h_k c)^T$ with MIN. If shorter, replace MIN

  In the end MIN contains a shortest vector

  Linear search through all convergents of b/a

Finding shortest vector w.r.t ℓ_∞-norm

Consider set of vectors

$$\left\{ \begin{pmatrix} -g_k a + h_k b \\ h_k c \end{pmatrix} \mid k = 0, \ldots, t \right\}, \tag{1}$$

where $\beta_k = g_k / h_k$, $0 \leqslant k \leqslant t$ are the convergents of b/a.

Proposition. *Shortest vector in* (1) *w.r.t.* ℓ_∞ *is last convergent of* b/a *outside the interval* $[(b-c)/a, (b+c)/a]$ *or first convergent of* b/a *inside* $[(b-c)/a, (b+c)/a]$.

Finding shortest vector w.r.t ℓ_∞-norm

Common convergent of interval $[\alpha_1, \alpha_2]$: Convergent β_k of α_1 and α_2 where k maximal

Finding shortest vector w.r.t ℓ_∞-norm

Common convergent of interval $[\alpha_1, \alpha_2]$: Convergent β_k of α_1 and α_2 where k maximal

Schönhage (1971): One can compute common convergent β_k and corresponding matrix $M^{(k)}$ of two rationals $\alpha_1, \alpha_2 \in \mathbf{Q}$ in time $O(M(n) \log n)$

Finding shortest vector w.r.t ℓ_∞-norm

Common convergent of interval $[\alpha_1, \alpha_2]$: Convergent β_k of α_1 and α_2 where k maximal

Schönhage (1971): One can compute common convergent β_k and corresponding matrix $M^{(k)}$ of two rationals $\alpha_1, \alpha_2 \in \mathbf{Q}$ in time $O(M(n)\log n)$

Proposition. *Let $\beta_k = g_k/h_k$ common convergent of $[(b-c)/a, (b+c)/a]$. Then k-th, $k+1$-st or $k+2$-nd convergent of b/a is shortest vector in (1) w.r.t. the ℓ_∞-norm.*

Fast shortest vector algorithm

- Compute HNF $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ of A

Fast shortest vector algorithm

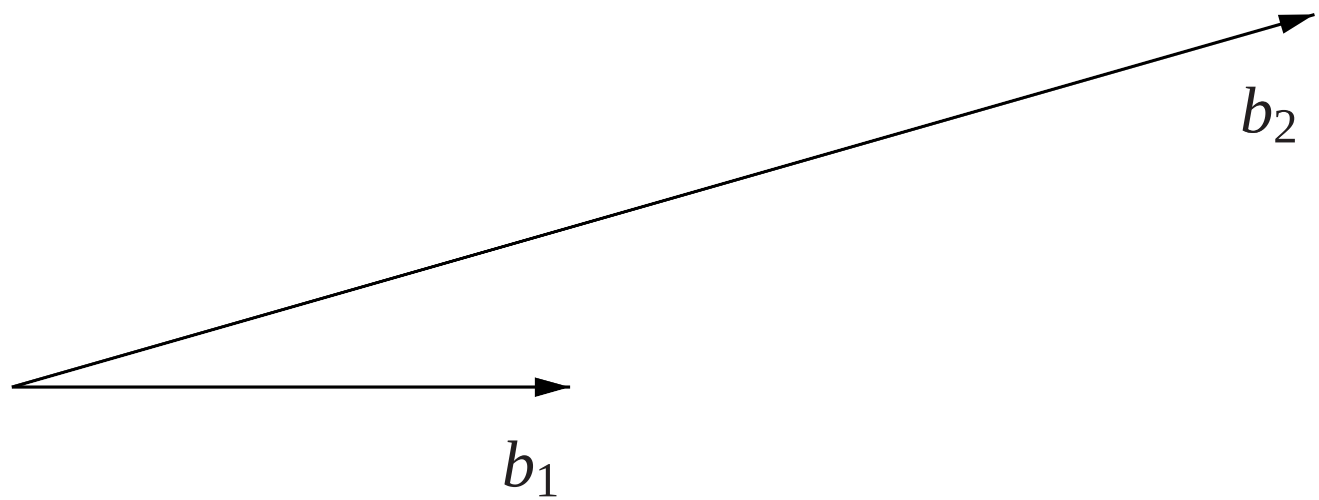
- Compute HNF $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ of A
- Compute reduced representation p/q of b/a and vectors $(a,0)^T$, $(-\lfloor p/2 \rfloor a + \lfloor q/2 \rfloor b, \lfloor q/2 \rfloor c)^T$; store shortest nonzero one in a container MIN

Fast shortest vector algorithm

- Compute HNF $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ of A
- Compute reduced representation p/q of b/a and vectors $(a,0)^T$, $(-\lfloor p/2 \rfloor a + \lfloor q/2 \rfloor b, \lfloor q/2 \rfloor c)^T$; store shortest nonzero one in a container MIN
- Compute common convergent β_k of $[(b-c)/a, (b+c)/a]$ and corresponding matrix $M^{(k)}$. Compute next two convergents of b/a with EXGCD; Replace MIN if one of convergents yields shorter vector

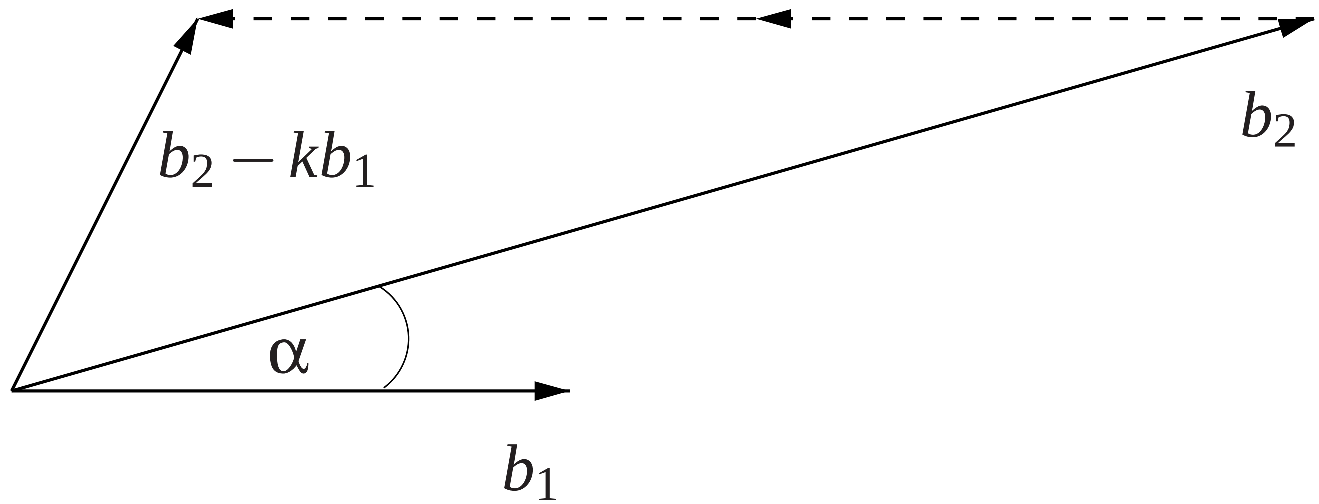
Reduced bases

Lattice basis (b_1, b_2) is reduced if enclosed angle in range $90^\circ \pm 30^\circ$



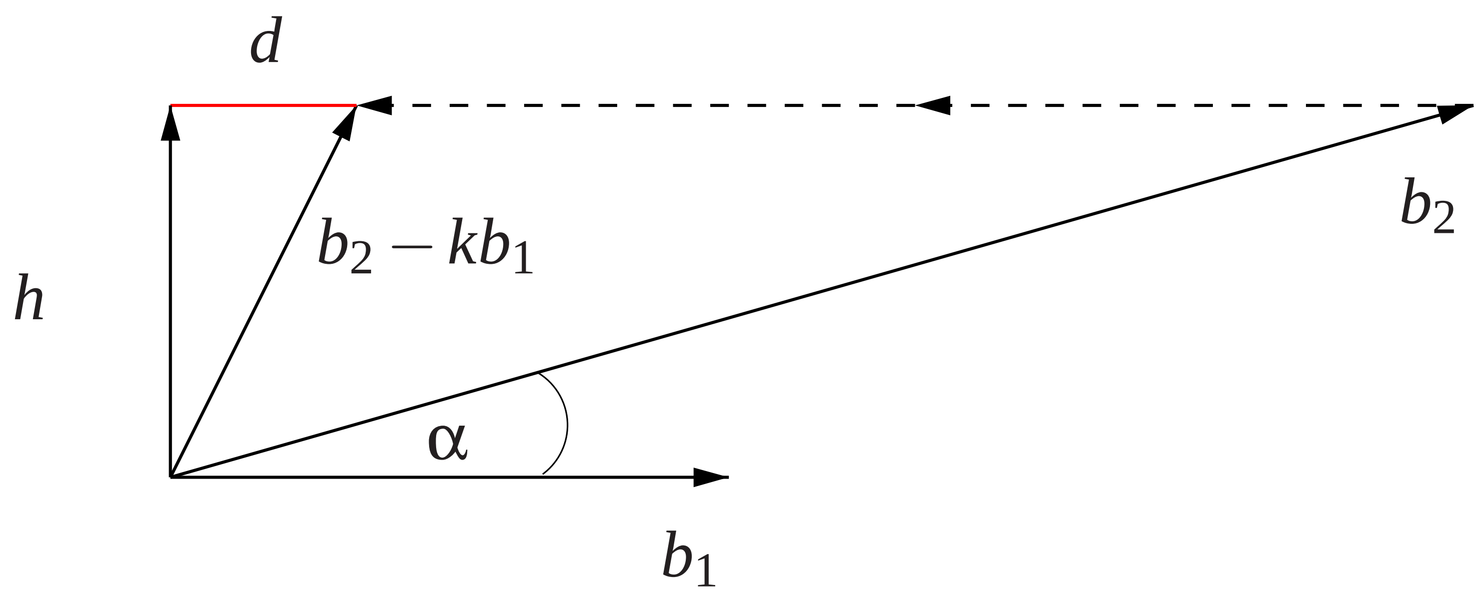
Reduced bases

Lattice basis (b_1, b_2) is reduced if enclosed angle in range $90^\circ \pm 30^\circ$



Reduced bases

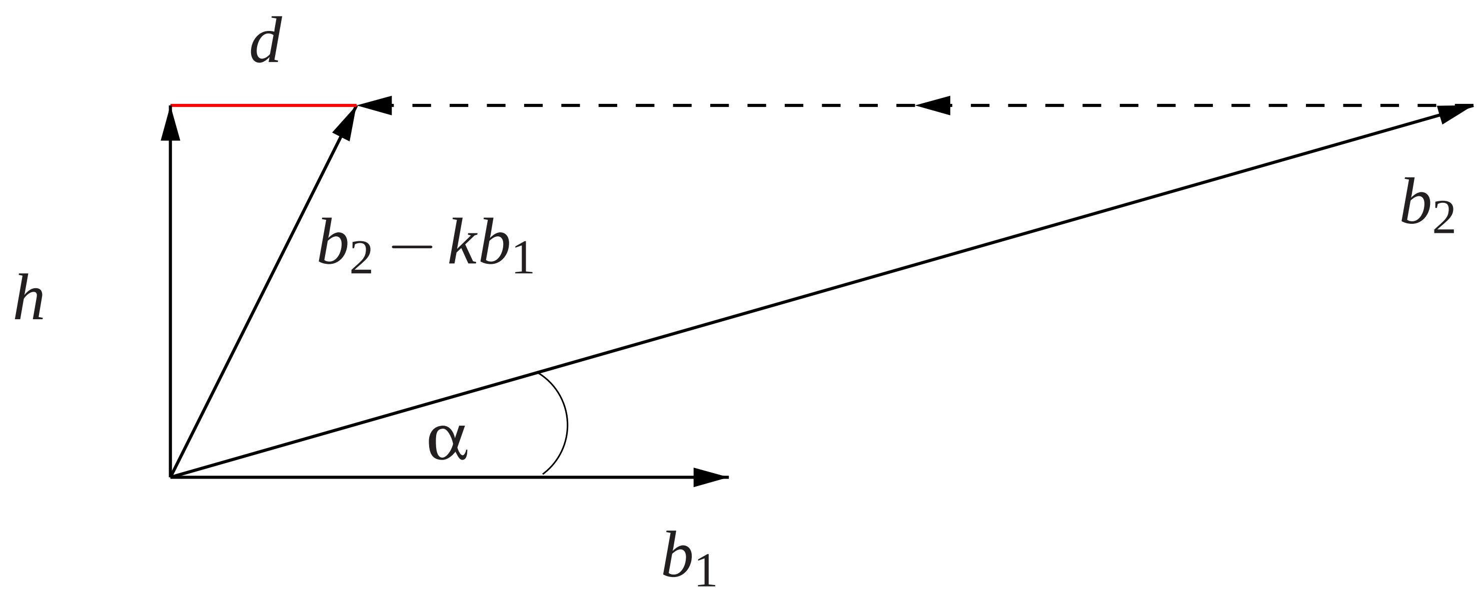
Lattice basis (b_1, b_2) is reduced if enclosed angle in range $90^\circ \pm 30^\circ$



$\|d\| \leqslant 1/2\,\|b_1\|$ and $\|h\| = \sin\alpha \|b_2\|$ suppose $\alpha < 60^\circ$

Reduced bases

Lattice basis (b_1, b_2) is reduced if enclosed angle in range $90^\circ \pm 30^\circ$

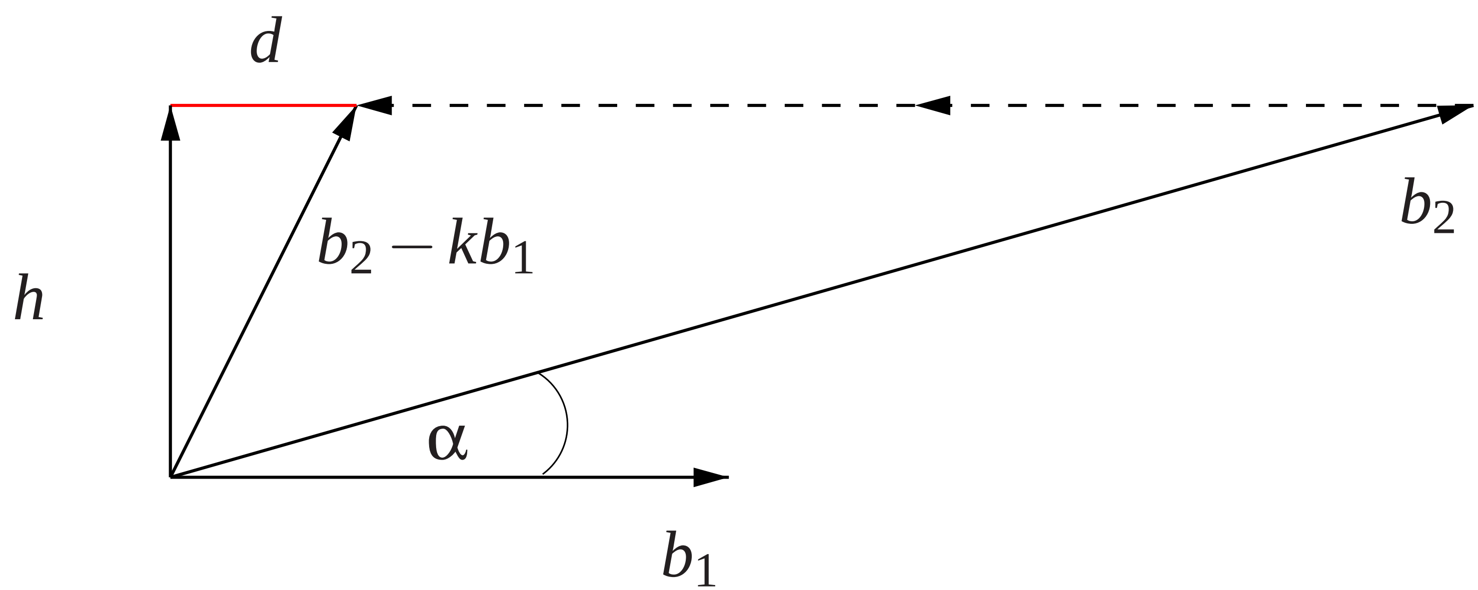


$\|d\| \leqslant 1/2\,\|b_1\|$ and $\|h\| = \sin\alpha \|b_2\|$ suppose $\alpha < 60^\circ$

$$\begin{aligned}\|b_2 - kb_1\|^2 &= \|h\|^2 + \|d\|^2 = 1/4\|b_1\|^2 + (\sin\alpha)^2\|b_2\|^2 \\ &\leqslant (1/4 + (\sin\alpha)^2)\,\|b_2\|^2\end{aligned}$$

Reduced bases

Lattice basis (b_1, b_2) is reduced if enclosed angle in range $90^\circ \pm 30^\circ$



$\|d\| \leqslant 1/2\,\|b_1\|$ and $\|h\| = \sin\alpha\|b_2\|$ suppose $\alpha < 60^\circ$

$$
\begin{aligned}
\|b_2 - kb_1\|^2 &= \|h\|^2 + \|d\|^2 = 1/4\|b_1\|^2 + (\sin\alpha)^2\|b_2\|^2 \\
&\leqslant (1/4 + (\sin\alpha)^2)\,\|b_2\|^2 < \|b_2\|^2
\end{aligned}
$$

Almost reduced basis

Proposition. *There exists* $\mathrm{O}(M(n)\log n)$ *time algorithm that computes basis* B *of* Λ *defined by* $A \in \mathbf{Z}^{2\times 2}$*, with property that the first column of* B *is shortest vector w.r.t.* ℓ_∞*-norm.*

Almost reduced basis

Proposition. *There exists* $\mathrm{O}(M(n)\log n)$ *time algorithm that computes basis* B *of* Λ *defined by* $A \in \mathbf{Z}^{2\times 2}$, *with property that the first column of* B *is shortest vector w.r.t.* ℓ_∞*-norm.*

Analysis of Gaussian algorithm (Lagarias 1980) reveals this basis almost reduced

Almost reduced basis

Proposition. *There exists* $\mathrm{O}(M(n)\log n)$ *time algorithm that computes basis* B *of* Λ *defined by* $A \in \mathbf{Z}^{2\times 2}$, *with property that the first column of* B *is shortest vector w.r.t.* ℓ_∞*-norm.*

Analysis of Gaussian algorithm (Lagarias 1980) reveals this basis almost reduced

Corollary. *There exists* $\mathrm{O}(M(n)\log n)$ *time algorithm that computes reduced basis* B *of* Λ *defined by* $A \in \mathbf{Z}^{2\times 2}$

Summary of results

- Shortest vector corresponds to best approximation of a rational defined by the lattice
- Shortest vectors can be found with the euclidean algorithm
- Fast basis reduction can be solely based on Schönhage's (1971) result and reduction algorithm of Gauss (1801)

Summary of results

- Shortest vector corresponds to best approximation of a rational defined by the lattice
- Shortest vectors can be found with the euclidean algorithm
- Fast basis reduction can be solely based on Schönhage’s (1971) result and reduction algorithm of Gauss (1801)

Summary of results

- Shortest vector corresponds to best approximation of a rational defined by the lattice
- Shortest vectors can be found with the euclidean algorithm
- Fast basis reduction can be solely based on Schönhage's (1971) result and reduction algorithm of Gauss (1801)

Open Problem

What about shortest vector problem in arbitrary fixed dimension?

Open Problem

What about shortest vector problem in arbitrary fixed dimension?

Fastest known algorithm of Kannan (1987) runs in time $O(M(n)n)$

Open Problem

What about shortest vector problem in arbitrary fixed dimension?

Fastest known algorithm of Kannan (1987) runs in time $O(M(n)n)$

Challenge:

Prove that shortest vector problem in arbitrary fixed dimension can be solved in time $O(M(n)\log n)$