Lattice Basis Reduction
Part 1: Concepts

Sanzheng Qiao

Department of Computing and Software
McMaster University, Canada
qiao@mcmaster.ca
www.cas.mcmaster.ca/˜qiao

October 25, 2011, revised February 2012

Joint work with W. Zhang and Y. Wei, Fudan University

Outline

Outline

An optimization problem

Integer least squares (ILS) problem

$$\min_{x \in Z^n} \|Ax - b\|_2^2$$

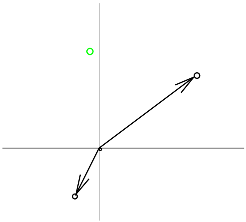
A: real, full column rank
b: real

Example

$$A = \begin{bmatrix} -1 & 4 \\ -2 & 3 \end{bmatrix}, \qquad b = \begin{bmatrix} -0.4 \\ 4 \end{bmatrix}$$

Example

$$A = \begin{bmatrix} -1 & 4 \\ -2 & 3 \end{bmatrix}, \qquad b = \begin{bmatrix} -0.4 \\ 4 \end{bmatrix}$$



A naive approach

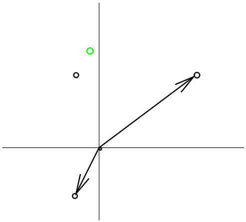
Solve for the real solution, then round it to its nearest integer.

$$A^{-1}b = \begin{bmatrix} -3.44 \\ -0.96 \end{bmatrix} \rightarrow \begin{bmatrix} -3 \\ -1 \end{bmatrix}$$

A naive approach

Solve for the real solution, then round it to its nearest integer.

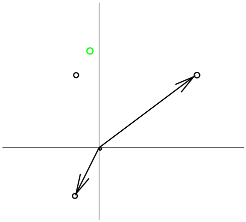
$$A^{-1}b = \begin{bmatrix} -3.44 \\ -0.96 \end{bmatrix} \rightarrow \begin{bmatrix} -3 \\ -1 \end{bmatrix}$$



A naive approach

Solve for the real solution, then round it to its nearest integer.

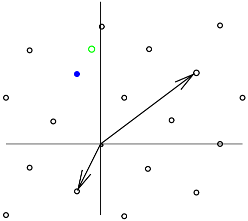
$$A^{-1}b = \begin{bmatrix} -3.44 \\ -0.96 \end{bmatrix} \rightarrow \begin{bmatrix} -3 \\ -1 \end{bmatrix}$$



Is this the ILS solution?

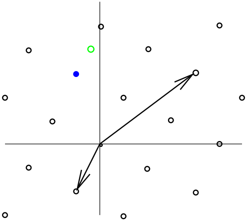
Lattices and Bases

A brute force approach:



Lattices and Bases

A brute force approach:



The set

$$L = \{Az \mid z \in Z^n\}$$

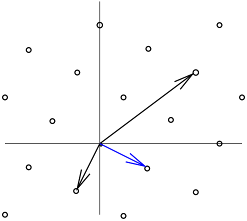
is call the lattice generated by A.

Basis: Formed by the columns of A (generator matrix).

Lattices and bases

For a given lattice, its basis is not unique.

$$B = \begin{bmatrix} -1 & 2 \\ -2 & -1 \end{bmatrix}$$



Lattices and bases

Two bases are related by $AZ = B$:

$$\begin{bmatrix} -1 & 4 \\ -2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 2 \\ -2 & -1 \end{bmatrix}$$

Z: Unimodular matrix, a nonsingular integer matrix whose inverse is also integer. (An integer matrix whose determinant is ± 1.)

Lattices and bases

Two bases are related by $AZ = B$:

$$\begin{bmatrix} -1 & 4 \\ -2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 2 \\ -2 & -1 \end{bmatrix}$$

Z: Unimodular matrix, a nonsingular integer matrix whose inverse is also integer. (An integer matrix whose determinant is ± 1.)

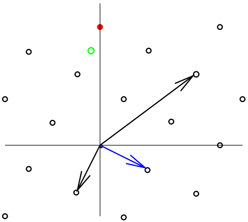
For any two generator matrices A and B of the same lattice, $|\det(A)| = |\det(B)|$, called the determinant (volume) of the lattice.

Naive approach revisited

$$B^{-1}b = \begin{bmatrix} -1.52 \\ -0.96 \end{bmatrix} \rightarrow \begin{bmatrix} -2 \\ -1 \end{bmatrix}$$

Naive approach revisited

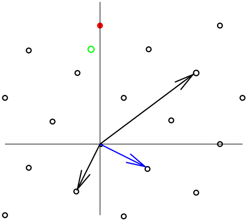
$$B^{-1}b = \begin{bmatrix} -1.52 \\ -0.96 \end{bmatrix} \to \begin{bmatrix} -2 \\ -1 \end{bmatrix}$$



A closer (closest) lattice point (1.077 vs 1.166).

Naive approach revisited

$$B^{-1}b = \begin{bmatrix} -1.52 \\ -0.96 \end{bmatrix} \rightarrow \begin{bmatrix} -2 \\ -1 \end{bmatrix}$$



A closer (closest) lattice point (1.077 vs 1.166).

Finding a closest vector (CVP) is an NP problem.

Lattice basis reduction

Lattice basis reduction problem:

Given a basis for a lattice, find a basis consisting of short vectors.

Lattice basis reduction algorithm:

Given a basis matrix A, compute a unimodular matrix Z that transforms the basis into a new basis matrix $B = AZ$ whose column vectors (basis vectors) are short.

Outline

Wireless communication

Source signal (code) s, integer vector.

Communication channel is represented by H, real/complex matrix.

Noise is represented by v, real vector.

The received signal

$$y = Hs + v$$

Given H and y, find s (decoding) using the naive approach called zero forcing (fast).

Wireless communication

Source signal (code) s, integer vector.

Communication channel is represented by H, real/complex matrix.

Noise is represented by v, real vector.

The received signal

$$y = Hs + v$$

Given H and y, find s (decoding) using the naive approach called zero forcing (fast).

When H is reduced, we have better chance of recovering s (lattice aided decoding).

Cryptography

Lattice based cryptosystems:

GGH (Goldreich, Goldwasser, Halevi) public-key cryptosystem.

Private key: A reduced basis matrix, e.g., diagonal, A.

Public key: An ill-conditioned basis matrix $B = AZ$.

Cryptography

Lattice based cryptosystems:

GGH (Goldreich, Goldwasser, Halevi) public-key cryptosystem.

Private key: A reduced basis matrix, e.g., diagonal, A.

Public key: An ill-conditioned basis matrix $B = AZ$.

Encrypt: $e = Bc + v$, c clear text, v noise.

Decrypt: $A^{-1}e \to Zc$.
($B^{-1}e$ gives wrong result.)

Cryptography

Lattice based cryptosystems:

GGH (Goldreich, Goldwasser, Halevi) public-key cryptosystem.

Private key: A reduced basis matrix, e.g., diagonal, A.

Public key: An ill-conditioned basis matrix $B = AZ$.

Encrypt: $e = Bc + v$, c clear text, v noise.

Decrypt: $A^{-1}e \rightarrow Zc$.
($B^{-1}e$ gives wrong result.)

Lattice basis reduction is an NP problem.

Outline

Matrix representation

Given a generator matrix A, compute the QRZ decomposition

$$A = QRZ^{-1}$$

Q: orthonormal columns, preserving vector length
R: upper triangular
Z: unimodular

Matrix representation

Given a generator matrix A, compute the QRZ decomposition

$$A = QRZ^{-1}$$

Q: orthonormal columns, preserving vector length
R: upper triangular
Z: unimodular

Thus QR is the QR decomposition of AZ, reduced (the columns of R or AZ are short).

Hermite reduction

Hermite-reduced, also called size-reduced.
Hermite, 1850.

Hermite-reduced

A lattice basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ is called size-reduced if its QR decomposition satisfies

$$|r_{i,i}| \geq 2|r_{i,j}|, \quad \text{for all} \quad 1 \leq i < j \leq n,$$

Hermite reduction

Hermite-reduced, also called size-reduced.
Hermite, 1850.

Hermite-reduced

A lattice basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ is called size-reduced if its QR decomposition satisfies

$$|r_{i,i}| \geq 2|r_{i,j}|, \quad \text{for all} \quad 1 \leq i < j \leq n,$$

The off-diagonal of R is small.

HKZ reduction

HKZ-reduced, strengthened Hermite-reduced.
Korkine and Zolotarev, 1873.

HKZ-reduced

A lattice basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ is called HKZ-reduced if it is size-reduced and for each trailing $(n-i+1) \times (n-i+1)$, $1 \leq i < n$, submatrix of R in the QR decomposition, its first column is a shortest nonzero vector in the lattice generated by the submatrix.

HKZ reduction

HKZ-reduced

$$
\begin{matrix}
r_{i,i} & r_{i,i+1} & \cdots & r_{i,n} \\
 & r_{i+1,i+1} & \cdots & r_{i+1,n} \\
 & & \ddots & \vdots \\
 & & & r_{n,n}
\end{matrix}
$$

LLL reduction

LLL-reduced
Lenstra, Lenstra, and Lovász, 1982

LLL-reduced

A lattice basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ is called LLL-reduced if it is size-reduced and R in the QR decomposition satisfies

$$r_{i+1,i+1}^2 + r_{i,i+1}^2 \geq \omega\, r_{i,i}^2$$

HKZ and LLL

HKZ-reduced and LLL-reduced

$$\begin{matrix} r_{i,i} & r_{i,i+1} & \cdots & r_{i,n} \\ & r_{i+1,i+1} & \cdots & r_{i+1,n} \\ & & \ddots & \vdots \\ & & & r_{n,n} \end{matrix}$$

HKZ and LLL

HKZ-reduced and LLL-reduced

$$\begin{matrix} r_{i,i} & r_{i,i+1} & \cdots & r_{i,n} \\ & r_{i+1,i+1} & \cdots & r_{i+1,n} \\ & & \ddots & \vdots \\ & & & r_{n,n} \end{matrix}$$

- LLL-reduced is weaker than HKZ-reduced, HKZ-reduced implies LLL-reduced for any ω: 0; .25 $< \omega <$ 1.0
- Easier to compute (fast).
- Practically, it produces reasonably short bases.

Minkowski minima

Minkowski, 1891
Short vectors

Minkowski minima

We say that λ_k, $1 \leq k \leq n$, is the k-th successive minimum wrt a lattice if λ_k is the lower bound of the radius λ of the sphere $||B\mathbf{z}||_2 \leq \lambda$ that contains k linearly independent lattice points.

Minkowski minima

Minkowski, 1891
Short vectors

Minkowski minima

We say that λ_k, $1 \leq k \leq n$, is the k-th successive minimum wrt a lattice if λ_k is the lower bound of the radius λ of the sphere $||B\mathbf{z}||_2 \leq \lambda$ that contains k linearly independent lattice points.

λ_1: the length of a shortest nonzero lattice vector $\mathbf{b}_1$

Minkowski minima

Minkowski, 1891
Short vectors

Minkowski minima

We say that λ_k, $1 \leq k \leq n$, is the k-th successive minimum wrt a lattice if λ_k is the lower bound of the radius λ of the sphere $||B\mathbf{z}||_2 \leq \lambda$ that contains k linearly independent lattice points.

λ_1: the length of a shortest nonzero lattice vector $\mathbf{b}_1$

Is there always a basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ so that $\|\mathbf{b}_i\| = \lambda_i$ simultaneously?

Minkowski minima

No.
Consider a lattice formed by columns of

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Minkowski minima $\lambda_1 = ... = \lambda_5 = 2$.

Minkowski minima

No.
Consider a lattice formed by columns of

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Minkowski minima $\lambda_1 = ... = \lambda_5 = 2$.

The columns of $2I_5$ do not form a basis for the lattice (determinants do not equal).

Minkowski reduction

Minkowski-reduced

A lattice basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ is called Minkowski-reduced if for each $\mathbf{b}_k$, $k = 1, ..., n$, $||\mathbf{b}_k||_2$ is the lower bound of the radius ρ of the sphere $||B\mathbf{z}||_2 \leq \rho$ that contains k lattice vectors that can be extended to a basis for the lattice.

Minkowski reduction

Minkowski-reduced

A lattice basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ is called Minkowski-reduced if for each $\mathbf{b}_k$, $k = 1, ..., n$, $||\mathbf{b}_k||_2$ is the lower bound of the radius ρ of the sphere $||B\mathbf{z}||_2 \leq \rho$ that contains k lattice vectors that can be extended to a basis for the lattice.

Properties

- $\mathbf{b}_i$ is a shortest nonzero vector in the sublattice generated by $\{\mathbf{b}_i, \mathbf{b}_{i+1}, \ldots, \mathbf{b}_n\}$;
- $\lambda_1 = ||\mathbf{b}_1||_2 \leq ||\mathbf{b}_2||_2 \leq \cdots \leq ||\mathbf{b}_n||_2$;
- $||\mathbf{b}_i||_2 \geq \lambda_i$ for $1 \leq i \leq n$.

Minkowski reduction

Another (weaker or equivalent?) notion

Minkowski-reduced

A lattice basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ is called Minkowski-reduced if for each $\mathbf{b}_i$, $i = 1, 2, \ldots, n$, its length

$$||\mathbf{b}_i||_2 = \min(||\hat{\mathbf{b}}_i||_2, ||\hat{\mathbf{b}}_{i+1}||_2, \ldots, ||\hat{\mathbf{b}}_n||_2)$$

over all sets $\{\hat{\mathbf{b}}_i, \hat{\mathbf{b}}_{i+1}, \ldots, \hat{\mathbf{b}}_n\}$ of lattice points such that $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}, \hat{\mathbf{b}}_i, \hat{\mathbf{b}}_{i+1}, \ldots, \hat{\mathbf{b}}_n\}$ form a basis for the lattice.

Minkowski reduction

Another (weaker or equivalent?) notion

Minkowski-reduced

A lattice basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ is called Minkowski-reduced if for each $\mathbf{b}_i$, $i = 1, 2, \ldots, n$, its length

$$||\mathbf{b}_i||_2 = \min(||\hat{\mathbf{b}}_i||_2, ||\hat{\mathbf{b}}_{i+1}||_2, \ldots, ||\hat{\mathbf{b}}_n||_2)$$

over all sets $\{\hat{\mathbf{b}}_i, \hat{\mathbf{b}}_{i+1}, \ldots, \hat{\mathbf{b}}_n\}$ of lattice points such that $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}, \hat{\mathbf{b}}_i, \hat{\mathbf{b}}_{i+1}, \ldots, \hat{\mathbf{b}}_n\}$ form a basis for the lattice.

In words, each $\mathbf{b}_i$, for $i = 1, 2, \ldots, n-1$, is a shortest nonzero lattice vector such that $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i\}$ can be extended to a basis for the lattice.

Outline

Examples

$$\begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 1 \end{bmatrix}$$

HKZ, thus LLL, reduced, but not Minkowski-reduced.

Examples

$$\begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 1 \end{bmatrix}$$

HKZ, thus LLL, reduced, but not Minkowski-reduced.

$$B = \begin{bmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & 1 & \frac{1}{2} \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Minkowski-reduced, also HKZ-reduced.

Examples

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Minkowski-reduced, but not LLL-reduced for $\omega > 0.5$, thus not HKZ-reduced.

Next talk

Preview

Algorithms for computing reduced bases.

Thank you!

Thank you!

Questions?