15.083J/6.859J Integer Optimization

Lecture 13: Lattices II
1 Outline

- Gram-Schmidt (GS) Orthogonalization.
- Reduced bases for lattices.
- Simultaneous Diophantine approximation.

2 GS orthogonalization

- **Input:** $n$ linearly independent vectors $b^1, \ldots, b^n \in \mathbb{Q}^n$
- **Output:** $n$ linearly independent vectors $\tilde{b}^1, \ldots, \tilde{b}^n$ that are orthogonal and span the same linear space.
- **Algorithm:**
  1. (Initialization) $\tilde{b}^1 = b^1$.
  2. (Main iteration) For $i = 2, \ldots, n$, set:
     \[
     \mu_{i,j} = \frac{(b^i)' \tilde{b}^j}{||\tilde{b}^j||^2} \quad \text{for } j = 1, \ldots, i - 1,
     \]
     \[
     \tilde{b}^i = b^i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{b}^j.
     \]

2.1 Intuition

- To initialize $\tilde{b}^1 = b^1$.
- Decompose $b^2 = v + u$, such that $v = \lambda b^1$ for some $\lambda \in \mathbb{R}$ and $u$ is orthogonal to $b^1$, i.e., $u^T b^1 = 0$.
- Multiplying $b^2 = v + u$ by $b^1$, $(b^2)' b^1 = \lambda ||b^1||^2$:
  \[
  \lambda = \frac{(b^2)' b^1}{||b^1||^2},
  \]
  \[
  b^2 = u = b^2 - v = b^2 - \lambda b^1.
  \]
- Geometrically $\tilde{b}^2$ corresponds to projecting $b^2$ to the subspace that is orthogonal to $b^1$.

2.2 Properties

- $(\tilde{b}^i)' \tilde{b}^j = 0$ for all $i \neq j$.
- $\{ x \in \mathbb{R}^n \mid x = \sum_{i=1}^k \lambda_i b^i, \lambda \in \mathbb{R}^k \} = \{ x \in \mathbb{R}^n \mid x = \sum_{i=1}^k \lambda_i \tilde{b}^i, \lambda \in \mathbb{R}^k \}$ for $k = 1, \ldots, n$.
- $\det(L(b^1, \ldots, b^n)) = \prod_{j=1}^n ||\tilde{b}^j||$.
- $||\tilde{b}^j|| \leq ||b^j||$ for $j = 1, \ldots, n$. 

2.3 Example

- \( b^1 = (4, 1)' \) and \( b^2 = (1, 1)' \).
- The GS orthogonalization: \( \tilde{b}^1 = b^1 \) and \( \tilde{b}^2 = b^2 - \mu_{2,1} \tilde{b}^1 = (1, 1)' - \frac{5}{17} b^1 = \frac{1}{17} (-3, 12)' \).
- Note that \( \tilde{b}^1, \tilde{b}^2 \) do not form a basis of \( \mathcal{L} \).
- The GS orthogonalization depends on the order in which the vectors are processed.
- Consider \( b^1 = (1, 1)' \) and \( b^2 = (4, 1)' \). The GS orthogonalization \( \tilde{b}^1 = b^1, \mu_{2,1} = 5/2 \) and \( \tilde{b}^2 = (1/2)(3, -3)' \).

2.4 Nearest vector

Given \( x \in \mathbb{R} \):

\[
|x| = \begin{cases} 
|x|, & \text{if } 0 \leq x - |x| \leq \frac{1}{2}, \\
|x|, & \text{if } \frac{1}{2} < x - |x| \leq 1.
\end{cases}
\]

\([1.5] = 1, [3.7] = 4 \) and \([5.2] = 5\).

Let \( b^1, \ldots, b^n \) be a basis of the lattice \( \mathcal{L} \) with GS \( \tilde{b}^1, \ldots, \tilde{b}^n \).

- For every \( z \in \mathcal{L} \setminus \{0\} \),
  \[
  ||z|| \geq \min\{|||\tilde{b}^1|||, \ldots, ||\tilde{b}^n|||\}.
  \]

- If \( \tilde{b}^1, \ldots, \tilde{b}^n \) is a basis of \( \mathcal{L} \), then the nearest vector in \( \mathcal{L} \) to the vector \( x = \sum_{j=1}^{n} \lambda_j \tilde{b}^j \), \( \lambda \in \mathbb{R}^n \) is given by:
  \[
  b^* = \sum_{j=1}^{n} \mu_j \tilde{b}^j, \quad \text{where } \mu_j = [\lambda_j].
  \]

2.5 Proof

- \( 0 \neq z = \sum_{i=1}^{n} \sigma_i b^i \) with \( \sigma_i \in \mathbb{Z}, i = 1, \ldots, n \).
- Let \( k \) be the largest index such that \( \sigma_k \neq 0 \), i.e., \( |\sigma_k| \geq 1 \).

\[
\begin{align*}
  z &= \sum_{i=1}^{k} \sigma_i \left( \tilde{b}^i + \sum_{j=1}^{k-1} \mu_{i,j} \tilde{b}^j \right) \\
  &= \sum_{j=1}^{k-1} \left( \sigma_j + \sum_{i=j+1}^{k} \sigma_i \mu_{i,j} \right) \tilde{b}^j \\
  &= \sum_{j=1}^{k} \lambda_j \tilde{b}^j,
\end{align*}
\]

where \( \lambda_j = \sigma_j + \sum_{i=j+1}^{k} \sigma_i \mu_{i,j} \).
• Since \((b^i)'b^i = 0\),
\[
\|z\|^2 = z'z = \sum_{j=1}^{k-1} \lambda_j^2||\tilde{b}^j||^2 + \sigma_k^2||\tilde{b}^k||^2 \geq \sigma_k^2||\tilde{b}^k||^2 \geq ||\tilde{b}^k||^2.
\]

• \(||z|| \geq ||\tilde{b}^k|| \geq \min\{||\tilde{b}^1||, \ldots, ||\tilde{b}^n||\}\).

• \(b = \sum_{j=1}^{n} \nu_j\tilde{b}^j\) with \(\nu_j \in \mathbb{Z}\), be an arbitrary vector of the lattice \(\mathcal{L}\).

• Let \(x = \sum_{i=1}^{n} \lambda_i\tilde{b}^i\), \(\lambda \in \mathbb{R}^n\). Then,
\[
||b - x||^2 = \sum_{j=1}^{n} (\nu_j - \lambda_j)^2||\tilde{b}^j||^2 \geq \sum_{j=1}^{n} (\mu_j - \lambda_j)^2||\tilde{b}^j||^2 = ||b^* - x||^2.
\]

• For all \(b \in \mathcal{L}\), \(||b - x|| \geq ||b^* - x||\).
• Importance of orthogonality.

3 Reduced Bases

3.1 Definition

Let \(\mathcal{L} = \mathcal{L}(b^1, \ldots, b^n)\) with \(b^1, \ldots, b^n \in \mathbb{Q}^n\) and with GS: \(\tilde{b}^1, \ldots, \tilde{b}^n\). The basis \(\{b^1, \ldots, b^n\}\) is called reduced if the following conditions hold:

• (a) \(|\mu_{i,j}| \leq \frac{1}{2}\) for all \(i, j\) with \(1 \leq j < i \leq n\),

• (b) \(||\tilde{b}^{i+1} + \mu_{i+1,i}\tilde{b}^i||^2 \geq \frac{3}{4}||\tilde{b}^i||^2\), for all \(i = 1, \ldots, n - 1\).

3.2 Intuition

• Conditions (a) and (b) jointly imply that a reduced basis consists of nearly orthogonal vectors.

• \(\tilde{b}^i = b^i\), condition (a) for \(i = 2\) implies that
\[
\mu_{2,1} = \frac{(b^2)'b^1}{||b^1||^2} \leq \frac{1}{2}.
\]

• From GS \(b^2 = \tilde{b}^2 + \mu_{2,1}\tilde{b}^1\), and thus (b) for \(i = 1\) \(||b^2||^2 \geq \frac{3}{4}||b^1||^2\).

• Let \(\theta\) be the angle between the two vectors \(b^i\) and \(\tilde{b}^2\). Then
\[
\cos \theta = \frac{(b^2)'b^i}{||b^2|| \cdot ||b^i||} = \frac{(b^2)'b^1}{||b^1||} \cdot \frac{||b^1||}{||b^2||} \leq \frac{1}{2} \frac{2}{\sqrt{3}} = \frac{1}{\sqrt{3}}.
\]

This implies that \(\theta \geq \cos^{-1}(1/\sqrt{3}) = 54.7^\circ\),

• For the purpose of achieving a bigger angle between the two vectors, that is, bringing the vectors closer to orthogonality, we would like to have as high a constant \(c\) as possible. For \(c = 1\), conditions (a) and (b) imply that an angle \(\theta\) would be at least \(\cos^{-1}(1/2) = 60^\circ\).
3.3 Properties

For a reduced basis \(b^1, \ldots, b^n\) of a lattice \(\mathcal{L}\) and its GS \(\tilde{b}^1, \ldots, \tilde{b}^n\):

- (a) \(\|\tilde{b}^i\|^2 \geq 2^{i-j} \|\tilde{b}^j\|^2\) for all \(1 \leq i < j \leq n\).
- (b) \(\|b^1\| \leq 2^{(n-1)/4} \det(\mathcal{L})^{1/n}\).
- (c) \(\|b^1\| \leq 2^{(n-1)/2} \min\{|\|b\| : b \in \mathcal{L} \setminus \{0\}\}\).
- (d) \(\|b^1\| \ldots \|b^n\| \leq 2^{(n-1)/4} \det(\mathcal{L})\).

3.4 Proof

- For all \(i = 1, \ldots, n - 1\):
  \[
  \frac{3}{4} \|\tilde{b}^i\|^2 \leq \|\tilde{b}^{i+1} + \mu_{i+1,i} \tilde{b}^i\|^2
  = \|\tilde{b}^{i+1}\|^2 + \mu_{i+1,i}^2 \|\tilde{b}^i\|^2
  \leq \|\tilde{b}^{i+1}\|^2 + \frac{1}{4} \|\tilde{b}^i\|^2.
  \]
  This gives
  \[
  \|\tilde{b}^{i+1}\|^2 \geq \frac{1}{2} \|\tilde{b}^i\|^2,
  \]
  leading to
  \[
  \|\tilde{b}^j\|^2 \geq 2^{i-j} \|\tilde{b}^i\|^2,
  \]
  for all \(1 \leq i < j \leq n\).

- Applying part (a) for \(i = 1\) we obtain
  \[
  \|\tilde{b}^{i+1}\|^2 \geq 2^{1-j} \|\tilde{b}^1\|^2 = 2^{1-j} \|\tilde{b}^i\|^2,
  \]
  for all \(1 \leq j \leq n\).

From Proposition 6.2(c), we have
\[
\det(\mathcal{L})^2 = \prod_{j=1}^n \|\tilde{b}^j\|^2 \geq \left(\prod_{j=1}^n 2^{1-j}\right) \|\tilde{b}^1\|^2 2^n = \left(\frac{1}{2}\right)^{(n(n-1))/2} \|\tilde{b}^1\|^2 2^n,
\]
proving part (b).

- From Proposition 6.3, we have that for every \(b \in \mathcal{L} \setminus \{0\}\),
  \[
  \|b\|^2 \geq \min\{|\|\tilde{b}^j\|^2 : j = 1, \ldots, n\} \geq 2^{1-n} \|\tilde{b}^1\|^2,
  \]
  proving part (c).

- From GS, Proposition 6.2 and the definition of a reduced basis we obtain
  \[
  \|\tilde{b}^i\|^2 = \|\tilde{b}^1\|^2 + \sum_{j=2}^{i-1} \mu_{i,j}^2 \|\tilde{b}^j\|^2 \leq \|\tilde{b}^1\|^2 + \frac{1}{4} \sum_{j=1}^{i-1} \|\tilde{b}^j\|^2
  \leq \|\tilde{b}^1\|^2 + \frac{1}{4} \sum_{j=1}^{i-1} 2^{i-j} \|\tilde{b}^i\|^2
  \leq \|\tilde{b}^1\|^2 \left(1 + \frac{1}{4} (2 + \ldots + 2^{i-1})\right)
  = \|\tilde{b}^i\|^2 \left(1 + \frac{1}{4} (2^i - 2)\right)
  \leq \|\tilde{b}^i\|^2 2^{i-1}.
  \]
Using Proposition 6.2(c) we obtain
\[ \prod_{i=1}^{n} \|b^i\|^2 \leq 2^{(n(n-1))/2} \prod_{i=1}^{n} \|\tilde{b}^i\|^2 = 2^{(n(n-1))/2} \det(L)^2, \]
proving part (d).

- From Minkowski, \( L \) there exist a vector \( u \in L \) such that \( \|u\|_\infty \leq \det(L)^{1/n} \).
In contrast, \( \|b^1\|_\infty \leq \|b^1\|_2 \leq 2^{(n-1)/4} \det(L)^{1/n} \) is weaker. The key difference is that we can find the vector \( b^1 \) in polynomial time.

### 3.5 Algorithm 6.2

- **Input:** A basis \( b^1, \ldots, b^n \in \mathbb{Z}^n \) of a lattice \( L \).
- **Output:** A basis of \( L \) satisfying condition (a)
- **Algorithm:**
  1. For \( i = 2, \ldots, n \)
     For \( j = i - 1, \ldots, 1 \)
     (a) If \( |\mu_{i,j}| > 1/2 \), then set \( b^i = b^i - |\mu_{i,j}| b^j \).
     (b) Compute the GS of \( b^1, \ldots, b^n \) and the corresponding multipliers \( \mu_{i,j} \).
  2. Return \( b^1, \ldots, b^n \).

### 3.6 Correctness

- The basis returned by Algorithm 6.2 satisfies condition (a).
- Algorithm 6.2 requires \( O(n^4) \) arithmetic operations.
- Algorithm 6.2 has the invariance property that after each iteration the GS of the initial basis of \( L \) remains unchanged, i.e.,
  \[ \tilde{b}^i = q^i \text{ for all } i = 1, \ldots, n. \]

### 3.7 Basis Reduction

- **Input:** A basis \( b^1, \ldots, b^n \in \mathbb{Z}^n \) of a lattice \( L \).
- **Output:** A basis of \( L \) satisfying conditions (a) and (b).
- **Algorithm:**
  1. Compute the Gram-Schmidt orthogonalization \( \tilde{b}^1, \ldots, \tilde{b}^n \) of the vectors \( b^1, \ldots, b^n \).
  2. Apply Algorithm 6.2.
  3. For \( i = 1, \ldots, n \)
     If \( \|\tilde{b}^{i+1} + \mu_{i+1,i} \tilde{b}^i\|^2 < 3/4 \|\tilde{b}^i\|^2 \), then interchange \( b^i \) and \( b^{i+1} \) and return to Step 1.
  4. Return \( b^1, \ldots, b^n \).
3.8 Polynominality

Let \( b^1, \ldots, b^n \in \mathbb{Z}^n \) be a basis of the lattice \( \mathcal{L} \). The basis reduction algorithm returns a reduced basis of \( \mathcal{L} \) by performing \( O(n^5 \log_2 b_{\max}) \) arithmetic operations, where \( b_{\max} \) is the largest integer (in absolute value) among the entries in \( b^1, \ldots, b^n \).

4 Simultaneous diophantine approximation

- For given numbers \( \alpha_1, \ldots, \alpha_n \in \mathbb{Q} \), \( 0 < \epsilon < 1 \) and a given integer number \( N > 1 \), find \( p_1, \ldots, p_n \in \mathbb{Z} \) and \( q \in \mathbb{Z}^+ \) with \( 0 < q \leq N \) satisfying:
  \[
  \left| \alpha_i - \frac{p_i}{q} \right| < \frac{\epsilon}{q} \quad \text{for } i \in \{1, \ldots, n\}. \quad (*)
  \]

- If \( N \geq \epsilon^{-n} \), then there exist \( p_1, \ldots, p_n \in \mathbb{Z} \) and \( q \in \mathbb{Z}^+ \) with \( 0 < q \leq N \) satisfying (*)

- Proof We define a lattice \( \mathcal{L} = \mathcal{L}(b^1, \ldots, b^n) \subset \mathbb{Q}^{n+1} \) where
  \[ b^0 = (\alpha_1, \ldots, \alpha_n, \delta)^t, \quad b^i = -e_i, \quad i = 1, \ldots, n, \]
  \[ \delta = \epsilon^{n+1}. \]

  Since \( \det(\mathcal{L}) = \delta = \epsilon^{n+1} \) and \( \dim(\mathcal{L}) = n + 1 \), from Convex body theorem we obtain that there exists an \( a \in \mathcal{L} \), \( a \neq 0 \) with \( \|a\|_{\infty} \leq (\det(\mathcal{L}))^{1/(n+1)} = \epsilon \).

  Hence, there exist \( q, p_1, \ldots, p_n \in \mathbb{Z} \) such that
  \[ a = q b^0 + \sum_{i=1}^{n} p_i b^i, \]
  with \( |a_i| \leq \epsilon \), or equivalently
  \[ |a_i| = |q \alpha_i - p_i| \leq \epsilon, \quad \text{for } i = 1, \ldots, n \]
  \[ a_n = q \delta \leq \epsilon, \quad \text{i.e., } q \leq \epsilon^{-n}. \]

  • To complete the proof we need to check that \( q > 0 \). Note that we assume without loss of generality that \( q \geq 0 \), since we can always take \(-a\) instead of \( a \).

  If \( q = 0 \), then \( |p_i| \leq \epsilon \) for all \( i \). Since \( p_i \in \mathbb{Z} \) and \( 0 < \epsilon < 1 \), we have \( p_i = 0 \). This leads to \( a = 0 \), which is a contradiction since \( a \neq 0 \).

4.1 Using Basis Reduction

- Theorem If \( N \geq 2^{n(n+1)/4} \epsilon^{-n} \), we can find in polynomial time \( p_1, \ldots, p_n \in \mathbb{Z} \) and \( q \in \mathbb{Z}^+ \) with \( 0 < q \leq N \) satisfying Eq. (*)

- \( \delta = 2^{-n(n+1)/4} \epsilon^{n+1} \) in the basis for the lattice \( \mathcal{L} \) defined earlier.

- Applying Basis Reduction we find in polynomial time a reduced basis of \( \mathcal{L} \). The first vector \( c \in \mathcal{L} \) in the reduced basis satisfies (recall that we use \( n+1 \) instead of \( n \), since \( \dim(\mathcal{L}) = n + 1 \))
  \[ \|c\|_{\infty} \leq \|c\|_2 \leq 2^{n/4} \det(\mathcal{L})^{1/(n+1)} = 2^{n/4} \delta^{1/(n+1)} = \epsilon. \]
Hence, we can find $p_1, \ldots, p_n \in \mathbb{Z}$ and $q \in \mathbb{Z}_+$ such that
\[ c = qb^0 + \sum_{i=1}^{n} p_i b^i, \]
with $|c_i| \leq \epsilon$, or equivalently
\[ |c_i| = |q\alpha_i - p_i| \leq \epsilon, \quad i = 1, \ldots, n \]
$c_n = q \delta \leq \epsilon$, i.e., $q \leq 2^{n(n+1)/4} \epsilon^{-n}$. 

7