15.083J/6.859J Integer Optimization

Lecture 13: Lattices II

1 Outline

Slide 1

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

2 GS orthogonalization

Slide 2

- **Input**: n linearly independent vectors $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n \in \mathcal{Q}^n$
- **Output**: n linearly independent vectors $\tilde{\boldsymbol{b}}^1, \ldots, \tilde{\boldsymbol{b}}^n$ that are orthogonal and span the same linear space.
- **Algorithm**:
  1. **(Initialization)** $\tilde{\boldsymbol{b}}^1 = \boldsymbol{b}^1$.
  2. **(Main iteration)** For $i = 2, \ldots, n$, set:

$$
\begin{aligned}
\mu_{i,j} &= \frac{(\boldsymbol{b}^i)' \tilde{\boldsymbol{b}}^j}{||\tilde{\boldsymbol{b}}^j||^2} \text{ for } j = 1, \ldots, i-1, \\
\tilde{\boldsymbol{b}}^i &= \boldsymbol{b}^i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{\boldsymbol{b}}^j.
\end{aligned}
$$

2.1 Intuition

Slide 3

- To initialize $\tilde{\boldsymbol{b}}^1 = \boldsymbol{b}^1$.
- Decompose $\boldsymbol{b}^2 = \boldsymbol{v} + \boldsymbol{u}$, such that $\boldsymbol{v} = \lambda \boldsymbol{b}^1$ for some $\lambda \in \mathcal{R}$ and $\boldsymbol{u}$ is orthogonal to $\boldsymbol{b}^1$, i.e., $\boldsymbol{u}'\boldsymbol{b}^1 = 0$.
- Multiplying $\boldsymbol{b}^2 = \boldsymbol{v} + \boldsymbol{u}$ by $\boldsymbol{b}^1$, $(\boldsymbol{b}^2)'\boldsymbol{b}^1 = \lambda ||\boldsymbol{b}^1||^2$:

$$\lambda = \frac{(\boldsymbol{b}^2)'\boldsymbol{b}^1}{||\boldsymbol{b}^1||^2},$$

$$\tilde{\boldsymbol{b}}^2 = \boldsymbol{u} = \boldsymbol{b}^2 - \boldsymbol{v} = \boldsymbol{b}^2 - \lambda \boldsymbol{b}^1$$

- Geometrically $\tilde{\boldsymbol{b}}^2$ corresponds to projecting $\boldsymbol{b}^2$ to the subspace that is orthogonal to $\boldsymbol{b}^1$.

2.2 Properties

Slide 4

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

2.3 Example

SLIDE 5

- $\boldsymbol{b}^1 = (4,1)'$ and $\boldsymbol{b}^2 = (1,1)'$.
- The GS orthogonalization: $\tilde{\boldsymbol{b}}^1 = \boldsymbol{b}^1$ and

$$\tilde{\boldsymbol{b}}^2 = \boldsymbol{b}^2 - \mu_{2,1}\,\tilde{\boldsymbol{b}}^1 = (1,1)' - \frac{5}{17}\tilde{\boldsymbol{b}}^1 = \frac{1}{17}(-3,12)',$$

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

2.4 Nearest vector

SLIDE 6

Given $x \in \mathcal{R}$:

$$\lfloor x \rceil = \begin{cases} \lfloor x \rfloor, & \text{if } 0 \le x - \lfloor x \rfloor \le \dfrac{1}{2}, \\ \lceil x \rceil, & \text{if } \dfrac{1}{2} < x - \lfloor x \rfloor \le 1. \end{cases}$$

$\lfloor 1.5 \rceil = 1$, $\lfloor 3.7 \rceil = 4$ and $\lfloor 5.2 \rceil = 5$.
Let $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n$ be a basis of the lattice $\mathcal{L}$ with GS $\tilde{\boldsymbol{b}}^1, \ldots, \tilde{\boldsymbol{b}}^n$.

- For every $\boldsymbol{z} \in \mathcal{L} \setminus \{\boldsymbol{0}\}$,

$$||\boldsymbol{z}|| \ge \min\{||\tilde{\boldsymbol{b}}^1||, \ldots, ||\tilde{\boldsymbol{b}}^n||\}.$$

- If $\tilde{\boldsymbol{b}}^1, \ldots, \tilde{\boldsymbol{b}}^n$ is a basis of $\mathcal{L}$, then the nearest vector in $\mathcal{L}$ to the vector $\boldsymbol{x} = \sum_{j=1}^n \lambda_j \tilde{\boldsymbol{b}}^j$, $\boldsymbol{\lambda} \in \mathcal{R}^n$ is given by:

$$\boldsymbol{b}^* = \sum_{j=1}^n \mu_j \tilde{\boldsymbol{b}}^j, \qquad \text{where } \mu_j = \lfloor \lambda_j \rceil.$$

2.5 Proof

SLIDE 7

- $\boldsymbol{0} \ne \boldsymbol{z} = \sum_{i=1}^n \sigma_i \boldsymbol{b}^i$ with $\sigma_i \in \mathcal{Z}$, $i = 1, \ldots, n$.
- Let k be the largest index such that $\sigma_k \ne 0$, i.e., $|\sigma_k| \ge 1$,

$$\begin{aligned} \boldsymbol{z} &= \sum_{i=1}^k \sigma_i \left(\tilde{\boldsymbol{b}}^i + \sum_{j=1}^{i-1} \mu_{i,j} \tilde{\boldsymbol{b}}^j \right) \\ &= \sigma_k \tilde{\boldsymbol{b}}^k + \sum_{j=1}^{k-1} \left(\sigma_j + \sum_{i=j+1}^k \sigma_i \mu_{i,j} \right) \tilde{\boldsymbol{b}}^j \\ &= \sigma_k \tilde{\boldsymbol{b}}^k + \sum_{j=1}^{k-1} \lambda_j \tilde{\boldsymbol{b}}^j, \end{aligned}$$

where $\lambda_j = \sigma_j + \sum_{i=j+1}^k \sigma_i \mu_{i,j}$.

- Since $(\tilde{\boldsymbol{b}}^i)'\tilde{\boldsymbol{b}}^j = 0$,

$$||\boldsymbol{z}||^2 = \boldsymbol{z}'\boldsymbol{z} = \sum_{j=1}^{k-1} \lambda_j^2 ||\tilde{\boldsymbol{b}}^j||^2 + \sigma_k^2 ||\tilde{\boldsymbol{b}}^k||^2 \geq \sigma_k^2 ||\tilde{\boldsymbol{b}}^k||^2 \geq ||\tilde{\boldsymbol{b}}^k||^2.$$

- $||\boldsymbol{z}|| \geq ||\tilde{\boldsymbol{b}}^k|| \geq \min\{||\tilde{\boldsymbol{b}}^1||, \ldots, ||\tilde{\boldsymbol{b}}^n||\}$.

Slide 8

- $\boldsymbol{b} = \sum_{j=1}^n \nu_j \tilde{\boldsymbol{b}}^j$ with $\nu_j \in \mathcal{Z}$, be an arbitrary vector of the lattice $\mathcal{L}$.
- Let $\boldsymbol{x} = \sum_{i=1}^n \lambda_j \tilde{\boldsymbol{b}}^j$, $\boldsymbol{\lambda} \in \mathcal{R}^n$. Then,

$$||\boldsymbol{b} - \boldsymbol{x}||^2 = \sum_{j=1}^{n} (\nu_j - \lambda_j)^2 ||\tilde{\boldsymbol{b}}^j||^2 \geq \sum_{j=1}^{n} (\mu_j - \lambda_j)^2 ||\tilde{\boldsymbol{b}}^j||^2 = ||\boldsymbol{b}^* - \boldsymbol{x}||^2.$$

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

3 Reduced Bases

3.1 Definition

Slide 9

Let $\mathcal{L} = \mathcal{L}(\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n)$ with $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n \in \mathcal{Q}^n$ and with GS: $\tilde{\boldsymbol{b}}^1, \ldots, \tilde{\boldsymbol{b}}^n$. The basis $\{\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n\}$ 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) $||\tilde{\boldsymbol{b}}^{i+1} + \mu_{i+1,i} \tilde{\boldsymbol{b}}^i||^2 \geq \frac{3}{4} ||\tilde{\boldsymbol{b}}^i||^2$, for all $i = 1, \ldots, n-1$.

3.2 Intuition

Slide 10

- Conditions (a) and (b) jointly imply that a reduced basis consists of nearly orthogonal vectors.
- $\tilde{\boldsymbol{b}}^1 = \boldsymbol{b}^1$, condition (a) for $i = 2$ implies that

$$\mu_{2,1} = \frac{(\boldsymbol{b}^2)'\boldsymbol{b}^1}{||\boldsymbol{b}^1||^2} \leq \frac{1}{2}.$$

- From GS $\boldsymbol{b}^2 = \tilde{\boldsymbol{b}}^2 + \mu_{2,1}\tilde{\boldsymbol{b}}^1$, and thus (b) for $i = 1$ $||\boldsymbol{b}^2||^2 \geq \frac{3}{4}||\boldsymbol{b}^1||^2$.
- Let θ be the angle between the two vectors $\boldsymbol{b}^1$ and $\boldsymbol{b}^2$. Then

$$\cos\theta = \frac{(\boldsymbol{b}^2)'\boldsymbol{b}^1}{||\boldsymbol{b}^2||\,||\boldsymbol{b}^1||} = \frac{(\boldsymbol{b}^2)'\boldsymbol{b}^1}{||\boldsymbol{b}^1||^2} \frac{||\boldsymbol{b}^1||}{||\boldsymbol{b}^2||} \leq \frac{1}{2}\frac{2}{\sqrt{3}} = \frac{1}{\sqrt{3}}.$$

  This implies that $\theta \geq \cos^{-1}(1/\sqrt{3}) = 54.7^o$,
- 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 θ would be at least $\cos^{-1}(1/2) = 60^o$.

3.3 Properties

Slide 11

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

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

3.4 Proof

Slide 12

- For all $i = 1, \ldots, n-1$:

$$\begin{aligned} \frac{3}{4}||\tilde{\boldsymbol{b}}^i||^2 &\leq ||\tilde{\boldsymbol{b}}^{i+1} + \mu_{i+1,i}\tilde{\boldsymbol{b}}^i||^2 \\ &= ||\tilde{\boldsymbol{b}}^{i+1}||^2 + \mu_{i+1,i}^2||\tilde{\boldsymbol{b}}^i||^2 \\ &\leq ||\tilde{\boldsymbol{b}}^{i+1}||^2 + \frac{1}{4}||\tilde{\boldsymbol{b}}^i||^2. \end{aligned}$$

  This gives

$$||\tilde{\boldsymbol{b}}^{i+1}||^2 \geq \frac{1}{2}||\tilde{\boldsymbol{b}}^i||^2, \quad \text{for all } i = 1, \ldots, n-1,$$

  leading to

$$||\tilde{\boldsymbol{b}}^j||^2 \geq 2^{i-j}\ ||\tilde{\boldsymbol{b}}^i||^2, \quad \text{for all } 1 \leq i < j \leq n.$$

- Applying part (a) for $i = 1$ we obtain

$$||\tilde{\boldsymbol{b}}^j||^2 \geq 2^{1-j}\ ||\tilde{\boldsymbol{b}}^1||^2 = 2^{1-j}\ ||\boldsymbol{b}^1||^2, \qquad \text{for all } 1 \leq j \leq n.$$

  From Proposition 6.2(c), we have

$$\det(\mathcal{L})^2 = \prod_{j=1}^{n} ||\tilde{\boldsymbol{b}}^j||^2 \geq \left(\prod_{j=1}^{n} 2^{1-j}\right) ||\boldsymbol{b}^1||^{2n} = \left(\frac{1}{2}\right)^{(n(n-1))/2} ||\boldsymbol{b}^1||^{2n},$$

  proving part (b).

- From Proposition 6.3, we have that for every $\boldsymbol{b} \in \mathcal{L} \setminus \{\boldsymbol{0}\}$,

$$||\boldsymbol{b}||^2 \geq \min\{||\tilde{\boldsymbol{b}}^j||^2 :\ j = 1, \ldots, n\} \geq 2^{1-n}||\boldsymbol{b}^1||^2,$$

  proving part (c).

- From GS, Proposition 6.2 and the definition of a reduced basis we obtain

$$\begin{aligned} ||\boldsymbol{b}^i||^2 = ||\tilde{\boldsymbol{b}}^i||^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 ||\tilde{\boldsymbol{b}}^j||^2 &\leq ||\tilde{\boldsymbol{b}}^i||^2 + \frac{1}{4}\sum_{j=1}^{i-1} ||\tilde{\boldsymbol{b}}^j||^2 \\ &\leq ||\tilde{\boldsymbol{b}}^i||^2 + \frac{1}{4}\sum_{j=1}^{i-1} 2^{i-j}\ ||\tilde{\boldsymbol{b}}^i||^2 \\ &= ||\tilde{\boldsymbol{b}}^i||^2\ \left(1 + \frac{1}{4}\ (2 + \ldots + 2^{i-1})\right) \\ &= ||\tilde{\boldsymbol{b}}^i||^2\ \left(1 + \frac{1}{4}\ (2^i - 2)\right) \\ &\leq ||\tilde{\boldsymbol{b}}^i||^2\ 2^{i-1}. \end{aligned}$$

Using Proposition 6.2(c) we obtain

$$\prod_{i=1}^{n} ||\boldsymbol{b}^i||^2 \leq 2^{(n(n-1))/2} \prod_{i=1}^{n} ||\tilde{\boldsymbol{b}}^i||^2 = 2^{(n(n-1))/2} \det(\mathcal{L})^2,$$

proving part (d).

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

3.5 Algorithm 6.2

SLIDE 13

- **Input**: A basis $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n \in \mathcal{Z}^n$ of a lattice $\mathcal{L}$.
- **Output**: A basis of $\mathcal{L}$ 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 $\boldsymbol{b}^i = \boldsymbol{b}^i - \lfloor \mu_{i,j} \rceil \boldsymbol{b}^j$.

  (b) Compute the GS of $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n$ and the corresponding multipliers $\mu_{i,j}$.

  2. Return $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n$.

3.6 Correctness

SLIDE 14

- 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 $\mathcal{L}$ remains unchanged, i.e.,

$$\tilde{\boldsymbol{b}}^i = \tilde{\boldsymbol{q}}^i \text{ for all } i = 1, \ldots, n.$$

3.7 Basis Reduction

SLIDE 15

- **Input**: A basis $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n \in \mathcal{Z}^n$ of a lattice $\mathcal{L}$.
- **Output**: A basis of $\mathcal{L}$ satisfying conditions (a) and (b).
- **Algorithm**:

  1. Compute the Gram-Schmidt orthogonalization $\tilde{\boldsymbol{b}}^1, \ldots, \tilde{\boldsymbol{b}}^n$ of the vectors $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n$.

  2. Apply Algorithm 6.2.

  3. For $i = 1, \ldots, n$
  If $||\tilde{\boldsymbol{b}}^{i+1} + \mu_{i+1,i}\tilde{\boldsymbol{b}}^i||^2 < 3/4\ ||\tilde{\boldsymbol{b}}^i||^2$, then interchange $\boldsymbol{b}^i$ and $\boldsymbol{b}^{i+1}$ and return to Step 1.

  4. Return $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n$.

3.8 Polynomiality

SLIDE 16

Let $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n \in \mathcal{Z}^n$ be a basis of the lattice $\mathcal{L}$. The basis reduction algorithm returns a reduced basis of $\mathcal{L}$ by performing $O(n^6 \log_2 b_{\max})$ arithmetic operations, where $b_{\max}$ is the largest integer (in absolute value) among the entries in $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^n$.

4 Simultaneous diophantine approximation

SLIDE 17

- For given numbers $\alpha_1, \ldots, \alpha_n \in \mathcal{Q}$, $0 < \epsilon < 1$ and a given integer number $N > 1$, find $p_1, \ldots, p_n \in \mathcal{Z}$ and $q \in \mathcal{Z}_+$ 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 $p_1, \ldots, p_n \in \mathcal{Z}$ and $q \in \mathcal{Z}_+$ with $0 < q \leq N$ satisfying (*).
- Proof We define a lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{b}^0, \ldots, \boldsymbol{b}^n) \subseteq \mathcal{Q}^{n+1}$ where

$$\boldsymbol{b}^0 = (\alpha_1, \ldots, \alpha_n, \delta)', \ \boldsymbol{b}^i = -\boldsymbol{e}_i, \ i = 1, \ldots, n,$$

  $\delta = \epsilon^{n+1}$.
- Since $\det(\mathcal{L}) = \delta = \epsilon^{n+1}$ and $\dim(\mathcal{L}) = n+1$, from Convex body theorem we obtain that there exists an $\boldsymbol{a} \in \mathcal{L}$, $\boldsymbol{a} \neq \boldsymbol{0}$ with $||\boldsymbol{a}||_\infty \leq (\det(\mathcal{L}))^{1/(n+1)} = \epsilon$. Hence, there exist $q, p_1, \ldots, p_n \in \mathcal{Z}$ such that

$$\boldsymbol{a} = q\boldsymbol{b}^0 + \sum_{i=1}^{n} p_i \boldsymbol{b}^i,$$

  with $|a_i| \leq \epsilon$, or equivalently

$$|a_i| = |q\alpha_i - p_i| \leq \epsilon, \qquad i = 1, \ldots, n$$

$$a_n = q\delta \leq \epsilon, \ \text{i.e., } q \leq \epsilon^{-n}.$$

- 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 $-\boldsymbol{a}$ instead of $\boldsymbol{a}$. If $q = 0$, then $|p_i| \leq \epsilon$ for all i. Since $p_i \in \mathcal{Z}$ and $0 < \epsilon < 1$, we have $p_i = 0$. This leads to $\boldsymbol{a} = \boldsymbol{0}$, which is a contradiction since $\boldsymbol{a} \neq \boldsymbol{0}$.

4.1 Using Basis Reduction

SLIDE 18

- Theorem If $N \geq 2^{n(n+1)/4}\epsilon^{-n}$, we can find in polynomial time $p_1, \ldots, p_n \in \mathcal{Z}$ and $q \in \mathcal{Z}_+$ 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 $\boldsymbol{c} \in \mathcal{L}$ in the reduced basis satisfies (recall that we use $n+1$ instead of n, since $\dim(\mathcal{L}) = n+1$)

$$||\boldsymbol{c}||_\infty \leq ||\boldsymbol{c}||_2 \leq 2^{n/4} \det(\mathcal{L})^{1/(n+1)} = 2^{n/4}\delta^{1/(n+1)} = \epsilon.$$

Hence, we can find $p_1, \ldots, p_n \in \mathcal{Z}$ and $q \in \mathcal{Z}_+$ such that

$$\boldsymbol{c} = q\boldsymbol{b}^0 + \sum_{i=1}^{n} p_i \boldsymbol{b}^i,$$

with $|c_i| \leq \epsilon$, or equivalently

$$|c_i| = |q\alpha_i - p_i| \leq \epsilon, \qquad i = 1, \ldots, n$$

$c_n = q\delta \leq \epsilon,$ i.e., $q \leq 2^{n(n+1)/4}\epsilon^{-n}$.