2010 年 5 月 28 日
輪講資料
廣瀬勝一（福井大）

Complexity of Lattice Problems

— A Cryptographic Perspective —

D. Micciancio & S. Goldwasser

5 Sphere Packings (球充填)

問題　格子点間の最小距離が λ 以上であるとき，半径 ρ の n 次元球の内部の格子点の最大可能個数はいくらか.

この問題の答は λ/ρ にのみ依存する.

(自明な) 事実

- λ/ρ が十分大きいとき，定数個の点しか詰め込めない.
  - $\lambda/\rho > 2$ のとき 1 個. $\lambda/\rho = 2$ のとき 2 個.
- $\lim_{n\to\infty} \lambda/\rho = 0$ のとき，指数的に多くの点が詰め込める.
  - $\lambda/\rho = 2/\sqrt{n}$ のとき，立方格子 $2\mathbb{Z}^n$ について，$\lambda = 2$. 中心 $\boldsymbol{s} = (1, 1, \ldots, 1)^{\mathrm{T}}$，半径 $\rho = \sqrt{n}$ の球を考える. この球を表す式は,

    $$(x_1 - 1)^2 + (x_2 - 1)^2 + \cdots + (x_n - 1)^2 = n \ .$$

    したがって，2^n 個の点 $(2 \pm 2, 2 \pm 2, \ldots, 2 \pm 2)^{\mathrm{T}}$ を含む.
- 1 より大きいある λ/ρ については，n に応じて増える任意に多くの点を含む.
  - $\{x \mid x \in \mathbb{Z}^n$ で $\sum_{i=1}^n x_i$は偶数 $\}$ を考える. これは，基底ベクトル $\boldsymbol{b}_i = \boldsymbol{e}_1 + \boldsymbol{e}_i$ $(i = 1, \ldots, n)$ により生成される格子で，$\lambda = \sqrt{2}$. 中心 $\boldsymbol{e}_1$，半径 $\rho = 1$ の球を考える. このとき，$\lambda/\rho = \sqrt{2}$ で，この球には $2n$ 個の点 $\boldsymbol{e}_1 \pm \boldsymbol{e}_i$ $(i = 1, \ldots, n)$ が含まれる.

次節以降で示される結果

1. $\lambda/\rho > \sqrt{2}$ のとき，定数個の点しか詰め込めない.
2. $\lambda/\rho = \sqrt{2}$ のとき，詰め込める点の最大個数は $2n$.
3. 任意の $\lambda/\rho < \sqrt{2}$ について，次元に関して指数的に多くの点が詰め込める.

上の 1, 2 は格子点でない場合も成立する.

5.1 Packing Points in Small Spheres

$\lambda/\rho \geq \sqrt{2}$ の場合について

- 格子点という制約を考えない．(上界なので，格子点の場合にも成立)
- 一般性を失うことなく，$\lambda = 2$, $\rho \leq \sqrt{2}$ と仮定．

定理 5.1 任意の $\rho < \sqrt{2}$ について，半径 ρ の球に詰め込むことのできる，互いの最小距離が 2 の点の最大数は $\lfloor 2/(2-\rho^2) \rfloor$ である．

証明 $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_N$ を以下を満たすベクトルの集合とする．

- $\|\boldsymbol{x}_i\| \leq \rho$
- $i \neq j$ のとき $\|\boldsymbol{x}_i - \boldsymbol{x}_j\| \geq 2$

このとき

$$
\begin{aligned}
4N(N-1) &\leq \sum_{i=1}^{N}\sum_{j=1}^{N} \|\boldsymbol{x}_i - \boldsymbol{x}_j\|^2 = \sum_{i=1}^{N}\sum_{j=1}^{N} (\|\boldsymbol{x}_i\|^2 + \|\boldsymbol{x}_j\|^2 - 2\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle) \\
&= \sum_{i=1}^{N} \left(N\|\boldsymbol{x}_i\|^2 + \sum_{j=1}^{N} \|\boldsymbol{x}_j\|^2 - 2\langle \boldsymbol{x}_i, \sum_{j=1}^{N} \boldsymbol{x}_j \rangle \right) \\
&= 2N\sum_{i=1}^{N} \|\boldsymbol{x}_i\|^2 - 2\left\| \sum_{i=1}^{N} \boldsymbol{x}_j \right\|^2 \leq 2N^2\rho^2
\end{aligned}
$$

したがって，$2(N-1) \leq N\rho^2$ で，N は整数だから，定理が成り立つ． □

定理 5.2 半径 $\sqrt{2}$ の n 次元球に詰め込むことのできる，互いの最小距離が 2 以上の点の最大数は $2n$ である．

証明 n に関する帰納法．$n = 1$ のときは明らか．ある n について成立を仮定して，$n+1$ の場合を考える．

$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_N \in \mathbb{R}^{n+1}$ を以下を満たすベクトルの集合とする．

- $\|\boldsymbol{x}_i\| \leq \sqrt{2}$
- $i \neq j$ のとき $\|\boldsymbol{x}_i - \boldsymbol{x}_j\| \geq 2$

$i \neq j$ のとき，

$$
\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle = \frac{1}{2}(\|\boldsymbol{x}_i\|^2 + \|\boldsymbol{x}_j\|^2 - \|\boldsymbol{x}_i - \boldsymbol{x}_j\|^2) \leq \frac{1}{2}(2+2-4) = 0
$$

なので，任意のベクトルの組の間の角度は $\pi/2$ 以上．

$\boldsymbol{x}_N \neq \boldsymbol{0}$ に注意して（$\boldsymbol{x}_N = \boldsymbol{0}$ なら，最小距離が 2 以上とならない），

$$
\boldsymbol{x}'_i = \begin{cases} \langle \boldsymbol{x}_N, \boldsymbol{x}_N \rangle \boldsymbol{x}_i - \langle \boldsymbol{x}_i, \boldsymbol{x}_N \rangle \boldsymbol{x}_N & \text{if } \langle \boldsymbol{x}_N, \boldsymbol{x}_N \rangle \boldsymbol{x}_i \neq \langle \boldsymbol{x}_i, \boldsymbol{x}_N \rangle \boldsymbol{x}_N \\ \boldsymbol{x}_i & \text{otherwise} \end{cases}
$$

を定義し，$\boldsymbol{x}''_i = \sqrt{2}\boldsymbol{x}'_i / \|\boldsymbol{x}'_i\|$ とする．このとき，以下が成立することが確認できる．

- $\|\boldsymbol{x}_i''\| = \sqrt{2}$ かつ，$i \neq j$ のとき，$\|\boldsymbol{x}_i'' - \boldsymbol{x}_j''\| \geq 2$
- $\boldsymbol{x}_i'' = \pm \boldsymbol{x}_N''$ または $\langle \boldsymbol{x}_i'', \boldsymbol{x}_N'' \rangle = 0$

$\boldsymbol{x}_1'', \ldots, \boldsymbol{x}_N''$ は，高々2個を除いて，$\boldsymbol{x}_N$ と直交する n 次元部分空間に存在するので，帰納法の仮定より，$N \leq 2(n+1)$. □

5.2 The Exponential Sphere Packing

$\lambda/\rho < \sqrt{2}$ の場合について

- 任意の ℓ_p ノルムを仮定 $(p \geq 1)$

$$\|\boldsymbol{x}\|_p = \left(\sum_i |x_i|^p \right)^{1/p}$$

5.2.1 The Schnorr-Adleman prime number lattice

補題 5.3 $a_1, \ldots, a_k$ を互いに素な正の奇数の列とする．任意の ℓ_p ノルムと任意の実数 $\alpha > 0$ について，

$$\tilde{\mathbf{L}} = \begin{pmatrix} \sqrt[p]{\ln a_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt[p]{\ln a_k} \\ \alpha \ln a_1 & \cdots & \alpha \ln a_k \end{pmatrix} \in \mathbb{R}^{(k+1)\times k}$$

の列により生成される格子のすべての非零ベクトルの ℓ_p ノルムは $\sqrt[p]{2\ln\alpha}$ より大きい．

証明 すべての非零整数ベクトル $\boldsymbol{z} \in \mathbb{Z}^k$ について，$\|\tilde{\mathbf{L}}\boldsymbol{z}\|_p^p > 2\ln\alpha$ を示す．必ずしも自明ではないが，単に計算による証明なので省略． □

格子の最短ベクトルの長さを大きくする自明な方法は，すべての座標を α 倍すること．一方，$\mathcal{L}(\tilde{\mathbf{L}})$ では，最後の座標のみ α 倍することで長さが大きくできる．ただし，α の対数．

5.2.2 Finding clusters

$$\tilde{\boldsymbol{s}} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \alpha \ln b \end{pmatrix} \in \mathbb{R}^{k+1}$$

を中心とする球に含まれる格子点の個数を考える．a_i の部分集合の積で b が近似できるとき，$\tilde{\boldsymbol{s}}$ に近い格子点が存在することを示す．

補題 5.4 $\tilde{\mathbf{L}}$, $\tilde{\boldsymbol{s}}$ を先の定義のとおりとする．任意の ℓ_p ノルム，実数 α，$b \geq 1$，正整数 $a_1, \ldots, a_k$，$\boldsymbol{z} \in \{0,1\}^k$ について，$g = \prod_i {a_i}^{z_i} \in [b, b(1+1/\alpha)]$ ならば，

$$\|\tilde{\mathbf{L}}\boldsymbol{z} - \tilde{\boldsymbol{s}}\|_p \leq \sqrt[p]{\ln b + 2}$$

が成立する．

証明 単に計算による証明なので，省略． □

$0 < \epsilon < 1$ について $\alpha = b^{1-\epsilon}$ とすると

1. 補題 5.3 より，格子点間の最小距離は $\lambda = \sqrt[p]{2(1-\epsilon)\ln b}$ より大きい．
2. 補題 5.4 より，区間 $[b, b+b^\epsilon]$ が多数の $\prod_{i \in S} a_i$ $(S \subseteq \{1, \ldots, k\})$ を含めば，$\tilde{\boldsymbol{s}}$ から $\sqrt[p]{\ln b + 2} \approx \lambda/\sqrt[p]{2}$ 以内の距離に多数の格子点が存在する．

$a_1, \ldots, a_k$ を最初の k 個の奇素数とすれば，上記 2 の前提条件は，

区間 $[b, b+b^\epsilon]$ が多数の無平方で a_k-smooth な奇数を含めば

となる．以下では，この前提条件が，どのような k, b について成立するかを考える．

補題 5.5 任意の実数 $\epsilon \in [0,1)$, $\mu > 1$ と，任意の整数 $H \geq 1$ と，任意の有限集合 $M \subset [1, \mu)$ について，b が M から無作為に選択されるとき，

$$\Pr\left[\left|[b, b+b^\epsilon) \cap M\right| < H\right] < \frac{\mu^{1-\epsilon} \cdot H}{\kappa(\epsilon) \cdot |M|}$$

が成立する．ここで $\kappa(\epsilon) = 1 - 2^{\epsilon-1}$ である．

証明 集合 B を以下のように定義する．

$$B = \left\{b \,\middle|\, b \in M \wedge \left|[b, b+b^\epsilon) \cap M\right| < H\right\}$$

次に示すとおり，B は $(H-1)$ 個以下の要素からなる $K < \mu^{1-\epsilon}/\kappa(\epsilon)$ 個の集合に分割できる．したがって，b が M から無作為に選択されるとき，

$$\Pr\left[\left|[b, b+b^\epsilon) \cap M\right| < H\right] = \Pr[b \in B] = \frac{|B|}{|M|} < \frac{\mu^{1-\epsilon} \cdot H}{\kappa(\epsilon) \cdot |M|}$$

分割法は以下のとおり．

1. $[1, \mu)$ を $[2^m, 2^{m+1})$ に分割．$m = 0, 1, \ldots, \lceil \log_2 \mu \rceil - 1$.
2. 各 $[2^m, 2^{m+1})$ を大きさ $2^{\epsilon m}$ の $2^m/2^{\epsilon m}$ 個の区間に分割．

上記 2 で得られる各区間は，ある $y \leq x^\epsilon$ について $[x, x+y)$ と表される．したがって，各区間は B の元を高々$H-1$ 個しか含まない（さもないと B の定義に矛盾）．2 で得られる区間の総数 K について，$K < \mu^{1-\epsilon}/\kappa(\epsilon)$ が成立することは，単純な数え上げで確認できる． □

系 5.6 すべての実数 $0 < \epsilon < 1$ と $\delta > 0$ に対し，任意の十分大きな整数 h について以下を満たす定数 c が存在する．

$k = h^c$ とし，最初の k 個の奇素数を $a_1, \ldots, a_k$ とする．また，

$$M = \left\{ \prod_{i \in S} a_i \,\middle|\, S \subset \{1, \ldots, k\} \wedge |S| = h \right\}$$

とする．b が M から無作為に選択されるとき，

$$\Pr\left[\left| [b, b + b^\epsilon) \cap M \right| < h^{\delta h} \right] < \frac{1}{2^h}$$

が成立する．

証明 ϵ, δ について，c を $c > (1+\delta)/\epsilon > 1$ なる整数とする．$\mu = {a_k}^h$ とすれば，$M \subset [1, \mu)$．また，

$$|M| = \binom{k}{h} = \prod_{i=0}^{h-1} \frac{k-i}{h-i} \geq \prod_{i=0}^{h-1} \frac{k}{h} = \frac{k^h}{h^h} = h^{(c-1)h}$$

である（上の不等号は $k \geq h$ より）．

$$\Pr\left[\left| [b, b + b^\epsilon) \cap M \right| < h^{\delta h} \right] < \frac{{a_k}^{(1-\epsilon)h} \cdot h^{\delta h}}{\kappa(\epsilon) \cdot h^{(c-1)h}}$$

素数定理より，$a_k = O(k \ln k) = O(h^c \ln h)$．また，$\kappa(\epsilon) = 1 - 2^{\epsilon - 1}$．

$$\begin{aligned} \Pr\left[\left| [b, b + b^\epsilon) \cap M \right| < h^{\delta h} \right] &< \frac{O(h^c \ln h)^{(1-\epsilon)h} \cdot h^{\delta h}}{h^{(c-1)h}} \\ &< \left(\frac{O(\ln h)}{h^{\epsilon c - (1+\delta)}} \right)^h < \frac{1}{2^h} \end{aligned}$$

□

定理 5.7 すべての実数 $0 < \epsilon < 1$ と $\delta > 0$ に対し，以下を満たす定数 c が存在する．

- h を十分大きな正整数とし，$k = h^c$ とする．
- 最初の k 個の奇素数を $a_1, \ldots, a_k$ とする．
- b を $\{a_1, \ldots, a_k\}$ から無作為に選択した h 個の素数の積とする．
- $\alpha = b^{1-\epsilon}$ とし，

$$\tilde{\mathbf{L}} = \begin{pmatrix} \sqrt[p]{\ln a_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt[p]{\ln a_k} \\ \alpha \ln a_1 & \cdots & \alpha \ln a_k \end{pmatrix} \qquad \tilde{\boldsymbol{s}} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \alpha \ln b \end{pmatrix}$$

  とする．
- $\tilde{r} = \sqrt[p]{(1+\epsilon) \ln b} > 1$ とする．

このとき

1. $\mathcal{L}(\tilde{\mathbf{L}})$ のすべての非零ベクトルの ℓ_p ノルムは $\sqrt[p]{2\left(\frac{1-\epsilon}{1+\epsilon}\right)}\tilde{r}$ より大きい．

2. 少なくとも $1-2^{-h}$ の確率で，球 $\mathcal{B}(\tilde{\boldsymbol{s}}, \tilde{r})$ に，$h^{\delta h}$ 個以上の格子点 $\tilde{\mathbf{L}}\boldsymbol{z}$ が含まれる．ただし，$\boldsymbol{z} \in \{0,1\}^k$ で丁度 h 個の 1 を持つ．

証明　補題 5.3，補題 5.4，系 5.6 から直ちに導かれる．

系 5.8 任意の $0 < \gamma < \sqrt{2}$ に対して，以下を満たす定数 $0 < \epsilon < 1$ が存在する．

任意の十分大きな正整数 k について，最小距離が λ の階数 k のある格子 $\tilde{\mathbf{L}}$ とある点 $\tilde{\boldsymbol{s}}$ が存在して，球 $\mathcal{B}(\tilde{\boldsymbol{s}}, \lambda/\gamma)$ が 2^{k^ϵ} 個の格子点を含む．

証明　定理 5.7 で，$p=2$ とし，$\gamma = \sqrt{2\left(\frac{1-\epsilon}{1+\epsilon}\right)} < \sqrt{2}$ となるよう ϵ を決める．したがって，$\epsilon = \frac{2-\gamma^2}{2+\gamma^2}$．

5.2.3 Some additional properties

この節の内容は，この本の他の部分では利用されないので，省略して差し支えない．

命題 5.9 $\tilde{\mathbf{L}}$ の行列式は

$$\sqrt{\left(1+\alpha^2\sum_{i=1}^{k}\ln a_i\right)\prod_{i=1}^{k}\ln a_i}$$

定義 5.1 x を任意の（正の）実数とし，p/q を有理数とする．$|p-qx| < \delta$ のとき，p/q を x のディオファントス δ 近似と呼ぶ．

命題 5.10 $\alpha > 0,\ b > 0$ を任意の正の定数とする．任意の整数ベクトル $\boldsymbol{z}$ について，$\|\tilde{\mathbf{L}}\boldsymbol{z} - \tilde{\boldsymbol{s}}\|_1 < \ln b$ ならば，$\prod {a_i}^{z_i}$ は b のディオファントス b/α 近似である．

命題 5.10 は補題 5.4 の逆．一般の ℓ_p ノルムについても同様の結果が成立する．

5.3 Integer Lattices

$\tilde{\mathbf{L}}$ と $\tilde{\boldsymbol{s}}$ の適当な整数近似についても，前節と同様の結果が得られることを示す．

補題 5.11 すべての $\eta \geq 1$ とすべての整数ベクトル $\boldsymbol{z} \in \mathbb{Z}^k$ について，

$$\|\mathbf{L}\boldsymbol{z}\|_p \geq (\eta-1)k\|\tilde{\mathbf{L}}\boldsymbol{z}\|_p$$

ここで，$\mathbf{L} = \lfloor(k\eta)\tilde{\mathbf{L}}\rceil$ は，$(k\eta)\tilde{\mathbf{L}}$ の各要素をそれに最も近い整数で置き換えて得られる行列である．

証明　単に計算による証明なので省略．

補題 5.12 すべての $\eta \geq 0$ とすべての整数ベクトル $\boldsymbol{z} \in \mathbb{Z}^k$ について，

$$\|\mathbf{L}\boldsymbol{z} - \boldsymbol{s}\|_p \leq (\eta + 1)k\|\tilde{\mathbf{L}}\boldsymbol{z} - \tilde{\boldsymbol{s}}\|_p$$

ここで，$\mathbf{L} = \lfloor (k\eta)\tilde{\mathbf{L}} \rceil$, $\boldsymbol{s} = \lfloor (k\eta)\tilde{\boldsymbol{s}} \rceil$.

証明　単に計算による証明なので省略.

定理 4.5 の証明

定理 4.5　任意の $p \geq 1$, $\gamma \in [1, \sqrt[p]{2})$, $\delta > 0$ について，整数 h が与えられたとき，以下を満たす整数 k, r，行列 $\mathbf{L} \in \mathbb{Z}^{(k+1)\times k}$，整数ベクトル $\boldsymbol{s} \in \mathbb{Z}^{k+1}$ を出力する確率アルゴリズムが存在する．なお，時間計算量は h の多項式である．

1. $\mathcal{L}(\mathbf{L})$ のすべてのベクトルの ℓ_p ノルムは γr より大きい．

2. すべての十分大きな h について，少なくとも $1 - 2^{-h}$ の確率で，球 $\mathcal{B}(\boldsymbol{s}, r)$ は少なくとも $h^{\delta h}$ 個の格子点 $\mathbf{L}\boldsymbol{y}$ を含む．ここで，$\boldsymbol{y}$ は丁度 h 個の 1 を持つ $\{0,1\}$ ベクトルである．

証明　1 については，定理 5.7 と補題 5.11 を用いる．定理 5.7 より，$k = h^c$ とする．また，補題 5.11 について，$\eta = 1/\epsilon$ とし，$r = \lceil (1 + 1/\epsilon)k\tilde{r} \rceil$ とする．ただし，ϵ は定理 5.7 の ϵ.
　2 については，定理 5.7 と補題 5.12 を用いる．1 の場合と同様に，補題 5.12 について，$\eta = 1/\epsilon$ とする．　□

5.4 Deterministic Construction

予想 1 任意の $\epsilon > 0$ に対して，ある d が存在して，十分大きなすべての n について，区間 $[n, n + n^\epsilon]$ に無平方で $(\log^d n)$-smooth な奇数が存在する．

定理 4.9　予想 1 が正しければ，任意の $p \geq 1$, $\gamma \in [1, \sqrt[p]{2})$ について，整数 h が与えられたとき，以下を満たす整数 $k(> h)$, r，行列 $\mathbf{L} \in \mathbb{Z}^{(k+1)\times k}$，整数ベクトル $\boldsymbol{s} \in \mathbb{Z}^{k+1}$ を出力する決定性アルゴリズムが存在する．なお，時間計算量は h の多項式である．

1. $\mathcal{L}(\mathbf{L})$ のすべてのベクトルの ℓ_p ノルムは γr より大きい．

2. 任意の $\boldsymbol{x} \in \{0,1\}^h$ に対して，ある $\boldsymbol{y} \in \{0,1\}^{k-h}$ が存在して，$\mathbf{L}(\boldsymbol{y}^{\mathrm{T}}, \boldsymbol{x}^{\mathrm{T}})^{\mathrm{T}}$ が球 $\mathcal{B}(\boldsymbol{s}, r)$ に含まれる．

証明　$0 < \epsilon < 1$ を実数とする．十分大きなすべての n について，区間 $[n, n + n^{\epsilon/2}]$ に無平方で $(\log^d n)$-smooth な奇数が存在するような整数 d を考える（予想 1）．
　$k = h^{d+1} + h$ とし，$a_1, \ldots, a_k$ を最初の k 個の奇素数，$b = {a_k}^{2h/\epsilon}$, $\alpha = b^{1-\epsilon}$ とする．k が h の多項式であることに注意する．
　補題 5.3 より，すべての $\boldsymbol{z} \in \mathbb{Z}^k \setminus \{\mathbf{0}\}$ について

$$\|\tilde{\mathbf{L}}\boldsymbol{z}\|_p \geq \sqrt[p]{2(1-\epsilon)\ln b}$$

が成立する．

以下では，すべての $\boldsymbol{x} \in \{0,1\}^h$ に対して，

$$\left\| \tilde{\mathbf{L}} \begin{pmatrix} \boldsymbol{y} \\ \boldsymbol{x} \end{pmatrix} - \tilde{\boldsymbol{s}} \right\|_p < \sqrt[p]{\ln b + 2}$$

を満たす $\boldsymbol{y} \in \{0,1\}^{h^{d+1}}$ が存在することを示す．

$g_{\boldsymbol{x}} = \prod_{i=1}^{h} (a_{h^{d+1}+i})^{x_i}$ とおくと，

$$\frac{b}{g_{\boldsymbol{x}}} > \frac{b}{{a_k}^h} = {a_k}^{(2/\varepsilon-1)h} > 2^h$$

したがって，十分大きなすべての h について，区間 $[b/g_{\boldsymbol{x}}, b/g_{\boldsymbol{x}} + (b/g_{\boldsymbol{x}})^{\epsilon/2}]$ に無平方で $\log^d(b/g_{\boldsymbol{x}})$-smooth な奇数が存在する．ところで，素数定理より $a_k = O(k \ln k)$ なので，

$$\log^d(b/g_{\boldsymbol{x}}) \leq \log^d b = O(h \log h)^d < h^{d+1}$$

である．したがって，この奇数は，ある $\boldsymbol{y} \in \{0,1\}^{h^{d+1}}$ を用いて，

$$g_{\boldsymbol{y}} = \prod_{i=1}^{h^{d+1}} {a_i}^{y_i}$$

と表すことができる．$g_{\boldsymbol{y}} \in [b/g_{\boldsymbol{x}}, b/g_{\boldsymbol{x}} + (b/g_{\boldsymbol{x}})^{\epsilon/2}]$, $g_{\boldsymbol{x}} \leq {a_k}^h = b^{\epsilon/2}$ より，

$$g_{\boldsymbol{y}} g_{\boldsymbol{x}} \in [b, b + b^{\epsilon/2} {g_{\boldsymbol{x}}}^{1-\epsilon/2}] \subset [b, b + b^{\epsilon}]$$

が成立するので，補題 5.4 より，

$$\left\| \tilde{\mathbf{L}} \begin{pmatrix} \boldsymbol{y} \\ \boldsymbol{x} \end{pmatrix} - \tilde{\boldsymbol{s}} \right\|_p < \sqrt[p]{\ln b + 2}$$

が成立する．$r = \sqrt[p]{\ln b + 2}$ として，

$$\frac{\sqrt[p]{2(1-\epsilon)\ln b}}{r} = \sqrt[p]{2} \left(\frac{(1-\epsilon)\ln b}{\ln b + 2} \right)^{1/p} > \lambda$$

を満たすように ϵ を選ぶ．$\mathbf{L}$, $\boldsymbol{s}$ は，補題 5.11 と補題 5.12 を用いて得ることができる．□

5.5 Notes

省略