暗号理論のための格子の数学

— 第4章　最短ベクトル問題 —

第29回情報セキュリティ研究会（2010/3/16）
広島市立大学　双紙正和

今日の内容

- いくつかの基本的な概念
- 第4章の概要
- Kannan の同次化技法
- Ajtai – Micciancio 埋め込み
- SVPのNP困難性
- まとめ

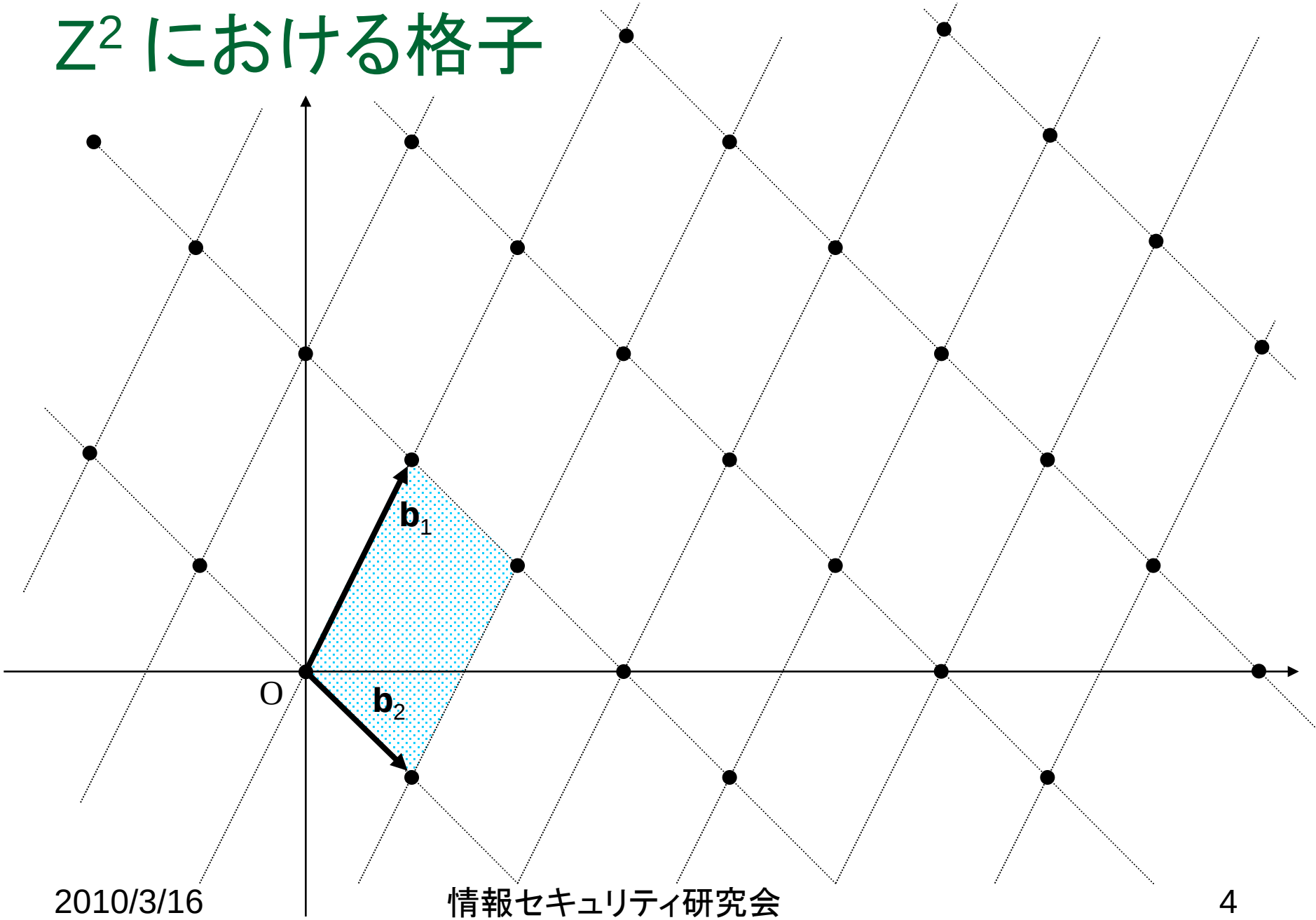
(整数)格子(lattice)

- $\mathbf{b}_1, \ldots, \mathbf{b}_n$ ($\in Z^m, m \geqq n$): 線形独立な(列)ベクトル
- Z^m における**格子**:
  $\mathbf{b}_1, \ldots, \mathbf{b}_n$ のすべての整数線形結合の集合:

$$L(\mathbf{b}_1, \ldots, \mathbf{b}_n) := \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \;\middle|\; x_i \in Z \right\}$$

- n: **階数**(rank), m: **次元**
- $\mathbf{b}_1, \ldots, \mathbf{b}_n$: **格子基底**.
- $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ ($\in Z^{m \times n}$): 格子基底の行列記法
- $L(\mathbf{B}) = \{ \mathbf{Bx} \mid \mathbf{x} \in Z^n \}$: 格子の行列記法
  - 文脈から明らかなときは, $\mathbf{B}$ を格子 $L(\mathbf{B})$ の意味で用いる

Z^2 における格子



言語

- **アルファベット**：記号の有限集合 Σ
  - 通常は，Σ = {0, 1} とする
- （Σ上の）**列**：Σからの記号の有限列
- **Σ^***：Σ上のすべての（有限）列の集合
- 言語：Σ^* の部分集合

判定（決定）問題 (decision problem)

- いま考えようとしている「問題」：なんらかの符号化により，Σ上の列 x に変換 ($x \in \Sigma^*$)
- **判定問題**：列 x が，ある特定の性質を満たすかどうか判定する
  - x を入力とし，{YES, NO}を出力する関数と考えてよい
  - **YES 例題**（YES instance）：性質を満たす x（YES が出力される x）

判定問題と言語

- 判定問題に対応する言語 L

$$L = \{ \text{YES 例題の集合} \} \subseteq \Sigma^*$$

- 「(判定)問題を解く」とは
  - 入力列 x が, $x \in L$ かどうかを判定する
- 問題の困難さ
  - 問題が規定する関数 f ($f : \Sigma^* \rightarrow \{YES, NO\}$) の計算の困難さ

帰着

- A, B：判定問題
- A から B への**（Karp）帰着**
  - 多項式時間計算可能な関数 f：
    $f: \Sigma^* \rightarrow \Sigma^*$，ただし，$x \in A$ iff. $f(x) \in B$

- A から B への **Cook 帰着**（Turing 帰着）
  - 問題 B を解くオラクル O を利用できる，多項式時間チューリング機械 M（M^O）が，正しく A を解くならば，M は A を B に Cook 帰着する

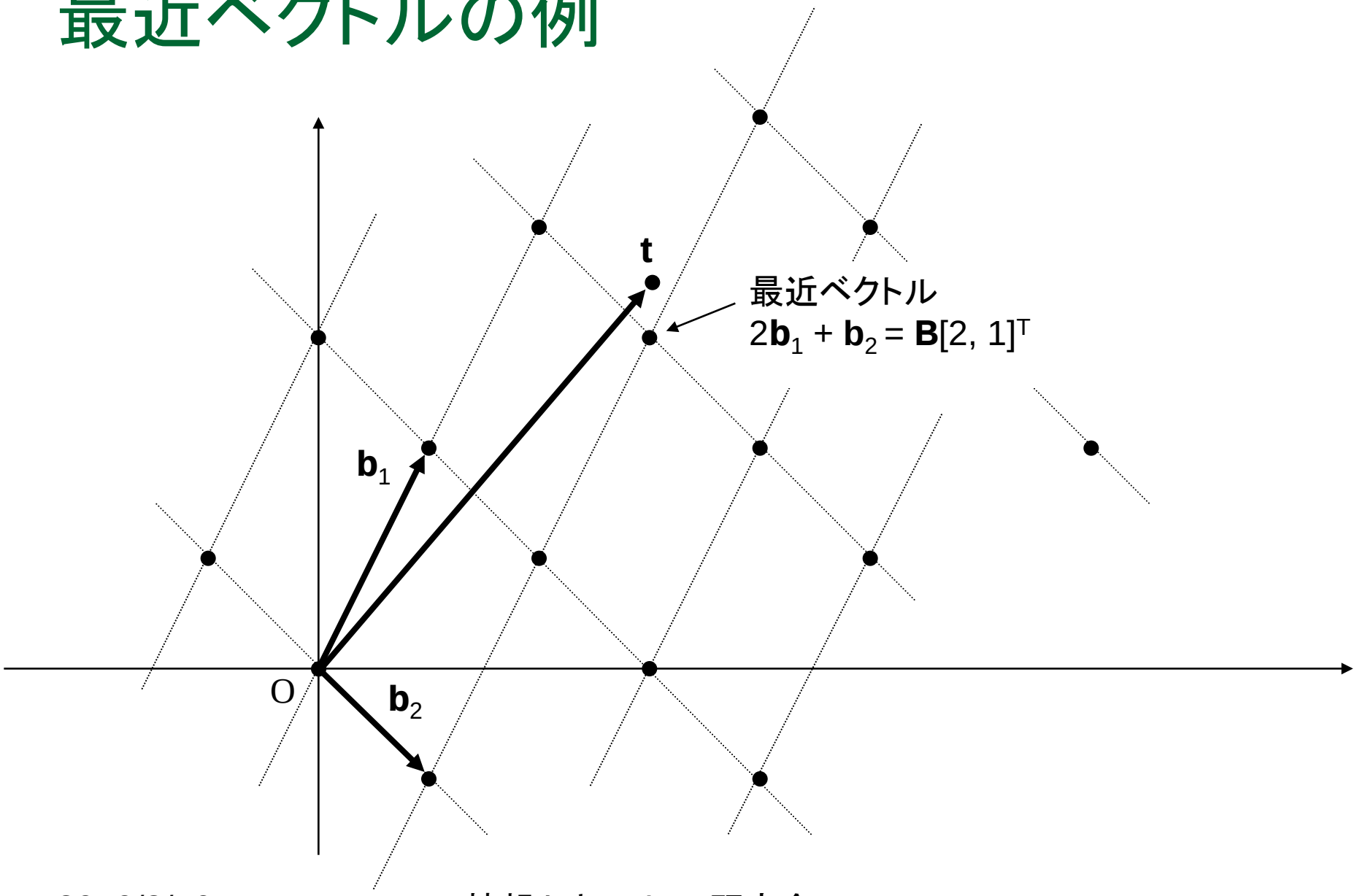
最短ベクトル問題（shortest vector problem, **SVP**）

- 格子基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$ が与えられるとき，非零格子ベクトル $\mathbf{Bx}$（$\mathbf{x} \in \mathbb{Z}^n - \{\mathbf{0}\}$）で，他のいかなる $\mathbf{y} \in \mathbb{Z}^n - \{\mathbf{0}\}$ に対しても，$\|\mathbf{Bx}\| \leqq \|\mathbf{By}\|$ であるようなものを求めよ.

最近ベクトル問題 (closest vector problem, **CVP**)

- 格子基底 $\mathbf{B} \in Z^{m \times n}$ と目標ベクトル $\mathbf{t} \in Z^{m}$ が与えられるとき，$\mathbf{t}$ に最も近い格子ベクトル $\mathbf{Bx}$（ただし $\mathbf{x} \in Z^{n}$）を求めよ.
  - すなわち，他のいかなる $\mathbf{y} \in Z^{n}$ に対しても，$\|\mathbf{Bx} - \mathbf{t}\| \leqq \|\mathbf{By} - \mathbf{t}\|$ であるような格子ベクトル$\mathbf{Bx}$（$\mathbf{x} \in Z^{n}$ ）を求めよ.

最近ベクトルの例


t
最近ベクトル
$2\mathbf{b}_1 + \mathbf{b}_2 = \mathbf{B}[2, 1]^T$
$\mathbf{b}_1$
O
$\mathbf{b}_2$

SVP, CVP の近似版

- SVP_{γ}
  - 基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$ が与えられるとき，他のどんな $\mathbf{y} \in \mathbb{Z}^{n} - \{\mathbf{0}\}$ に対しても $\|\mathbf{Bx}\| \leqq \gamma \cdot \|\mathbf{By}\|$ であるような非零格子ベクトル$\mathbf{Bx}$（$\mathbf{x} \in \mathbb{Z}^{n} - \{\mathbf{0}\}$）を求めよ.
- CVP_{γ}
  - 基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$ と目標ベクトル $\mathbf{t} \in \mathbb{Z}^{m}$が与えられるとき，他のどんな $\mathbf{y} \in \mathbb{Z}^{n}$ に対しても $\|\mathbf{Bx} - \mathbf{t}\| \leqq \gamma \cdot \|\mathbf{By} - \mathbf{t}\|$ であるような格子ベクトル$\mathbf{Bx}$（$\mathbf{x} \in \mathbb{Z}^{n}$）を求めよ.

今日の内容

- いくつかの基本的な概念

- 第4章の概要
- Kannan の同次化技法

- Ajtai – Micciancio 埋め込み
- SVPのNP困難性
- まとめ

第4章の概要

- 最短ベクトル問題（SVP）を近似する困難性について考察
- Kannan の同次化（同質化，homogenization）技法を拡張して，近似CVPを，近似SVPに帰着
- l_p ノルムにおいて，$2^{1/p}$ より小さな近似因子で SVP を近似することがNP困難であることを示す
- 言及しない限り，l_2 ノルムを仮定

Kannan の同次化技法 (homogenization technique)

- 最近ベクトル問題（CVP）を，最短ベクトル問題（SVP）に Cook 帰着する
- 格子 $L(\mathbf{B})$ の点で，目標ベクトル **t** に（近似的に）最も近いものを求めたい

CVP から SVP への帰着における，同次化のナイーブな方法

行列 [**B** | **t**] で生成される格子の中から，最短非零ベクトルを求める

もし最短非零ベクトルが **Bx** – **t**，**Bx** + **t** の形ならば，それぞれ **Bx**，– **Bx** が **t** に最も近いベクトル

しかし，求められたベクトルが，**Bx** ± **t** の形でないならば，この帰着は失敗する！

生成されるベクトルは，**Bx** + w **t** の形

w の取り得る値が重要

（この場合の帰着の失敗例については，教科書参照）

同次化技法の基本的なアイディア

- **B**, **t** を，より高次元の空間に埋め込む，すなわち，

$$\mathbf{B}' := \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0}^T & c \end{bmatrix}$$

によって生成される格子の最短ベクトルを考える．

- このとき，
  - **B** の列が線形独立なら，**B'** も同様 → **B'** はL(**B'**) の基底
  - c は有理数
  - **B'**の最後の列が，高々一回しか使えないような（十分大きい）c を適切に選ぶ（ただし，c が大きすぎると，最後の列は一回も使われない）

補題4.1

- 任意のμ ∈[1, 2)：$L(\mathbf{B})$ からの点 **t** の距離（μ= dist(**t**, $L(\mathbf{B})$）
- 定数　$c > \mu \Big/ \sqrt{(2/\gamma)^2 - 1}$
- このとき，もし

$$\mathbf{s} := \mathbf{B}' \begin{bmatrix} \mathbf{x} \\ w \end{bmatrix} = \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0}^T & c \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ w \end{bmatrix} = \begin{bmatrix} \mathbf{B}\mathbf{x} + w\mathbf{t} \\ wc \end{bmatrix}$$

が $L(\mathbf{B}')$ の γ 近似最短ベクトルならば，$|w| \leqq 1$

補題4.1の証明(1)

- 格子 $L(\mathbf{B}')$ は,
  - $\mathbf{x}$: ただし, $\mathbf{t}$ と $\mathbf{Bx}$ の距離がμ (=dist($\mathbf{t}$, $L(\mathbf{B})$)
  - $w = -1$

について, ベクトル

$\mathbf{v} := \mathbf{B}'[\mathbf{x}^T, -1]^T = [(\mathbf{Bx} - \mathbf{t})^T, -c]^T$

を含む. $||\mathbf{v}|| = (\mu^2 + c^2)^{(1/2)}$ であるから,

$||\mathbf{s}||^2 \leqq \gamma^2 (\mu^2 + c^2)$

また, $||\mathbf{s}||^2 = ||\mathbf{Bx} + w\mathbf{t}||^2 + (wc)^2 \geqq (wc)^2$

以上より, $(wc)^2 \leqq \gamma^2 (\mu^2 + c^2)$

補題4.1の証明(2)

- （続き）
  w について解き，$c > \mu \Big/ \sqrt{(2/\gamma)^2 - 1}$ を使って，

$$w \le \gamma \sqrt{\frac{\mu^2}{c^2} + 1} < 2$$

  w は整数なので，$|w| \leqq 1$ （証明終）

定理4.2

- 格子の階数 n, 任意の近似因子 $\gamma \in [1, 2)$ と任意の関数

$$\gamma'(n) > \frac{\sqrt{n}}{\sqrt{(2/\gamma)^2 - 1}}$$

に対して, CVP$_{\gamma'(n)}$ 探索問題は SVP$_{\gamma}$ 探索問題に Cook 帰着可能である. さらに, 帰着がオラクルを呼び出す回数は $O(n \log n)$ である.

定理4.2の証明の流れ

- 因子 γ 内で SVP を近似するオラクルがあるとき，因子 γ' 内で CVP を効率的に近似できることを示す
- 補題4.1の**B'** について，SVP$_\gamma$オラクルが返すベクトルにおいて $|w| \leqq 1$が成立するような c を求める
  - c のある範囲について，SVP$_\gamma$オラクルを呼び出しつつ2分探索を行う
- $w = \pm 1$, $w = 0$ で場合分け
  - $w = \pm 1$の場合は容易に題意を示せる
  - $w = 0$ のとき．SVP$_\gamma$オラクルが返す **s** = **Bx** は，L(**B**) の短い非零ベクトル．このとき，**B**, **t** を **s** の直交補空間に射影し，階数を減らしながら，再帰的に解いていく．

定理4.2の証明（1 of 10）

- 任意の因子 $\gamma \in [1, 2)$，ある定数 $\varepsilon \in (0,1]$ について，

$$\gamma' := \frac{\sqrt{n(1+\varepsilon)}}{\sqrt{(2/\gamma)^2 - 1}}$$

とおく.

- **B**：階数 n の格子基底，**t**： 目標ベクトル
- **B'**，μ，c：補題4.1と同様

- 因子 γ 内で SVP を近似するオラクルが与えられたとき，因子 γ' 内で CVP を効率的に近似できることを示したい

定理4.2の証明（2 of 10）

- c の値は，補題4.1より，$\mu \Big/ \sqrt{(2/\gamma)^2 - 1}$ よりわずかに大きい値，たとえば，

$$c \leq \mu \sqrt{\frac{1+\varepsilon}{(2/\gamma)^2 - 1}}$$

  とすればよい
- しかし，現段階では μ の値が分からないので，$c = \mu\sqrt{1+\varepsilon} \Big/ \sqrt{(2/\gamma)^2 - 1}$ とすることはできない！
- ではどうするか？

定理4.2の証明(3 of 10)

- 最近平面CVP近似アルゴリズム(2章, 43ページ参照)により, 多項式時間で $\mu \le M \le 2\left(2/\sqrt{3}\right)^n \mu < 2^n \mu$ となる実数 M を求める. さらに, $k \geqq 0$ について単調減少列

$$c_k = \frac{M\left(\sqrt{1+\varepsilon}\right)^{1-k}}{\sqrt{(2/\gamma)^2 - 1}}$$

を考える. すると, 特に $c_0 > \mu \Big/ \sqrt{(2/\gamma)^2 - 1}$ であるから, $c = c_0$ とすると, 補題4.1より, SVP$_\gamma$オラクルは, **B'**の最後の列を $|w| \leqq 1$回使う最短ベクトルを返す.

- しかし, $c_0 \le \mu\sqrt{1+\varepsilon} \Big/ \sqrt{(2/\gamma)^2 - 1}$ とは限らない!

定理4.2の証明(4 of 10)

- 次に, $k = K := \lceil 2n / \log_2(1+\varepsilon) \rceil$ とする.
- このとき, $c_K \le \mu\sqrt{1+\varepsilon} \Big/ \sqrt{(2/\gamma)^2 - 1}$ は満たされるが, 今度は $c_K > \mu \Big/ \sqrt{(2/\gamma)^2 - 1}$ を満たすとは限らない.
- そこで, $\{0, \ldots, K\}$ において, SVP$_\gamma$オラクルを呼び出しつつ2分探索を実行し,
  - $c = c_k$ のとき, SVP$_\gamma$オラクルが返すベクトルにおいて $|w| \leqq 1$
  - $c = c_{k+1}$ のとき, SVP$_\gamma$オラクルが返すベクトルにおいて $|w| > 1$

  となるような k を求める (c_k は k の単調減少列であることに注意).
- このときの, SVP$_\gamma$オラクルの呼出し回数は $O(\log n)$

定理4.2の証明（5 of 10）

- いま求めた k について，$|w| \leqq 1$
- $w = \pm 1$, $w = 0$ で場合分けして考える．一般性を失うことなく $n \geqq 3$ と仮定．
- $w = \pm 1$ のとき．
  - $-w\mathbf{Bx}$ が CVP例題 (**B**, **t**) の γ'近似解であることを容易に示すことができる．すなわち，
    $\|\mathbf{t} - (-w\mathbf{Bx})\| \leqq \gamma'\mu$.
  - 導出は，教科書81，82ページ参照．ただし，82ページの最初の式に typo があるので注意．

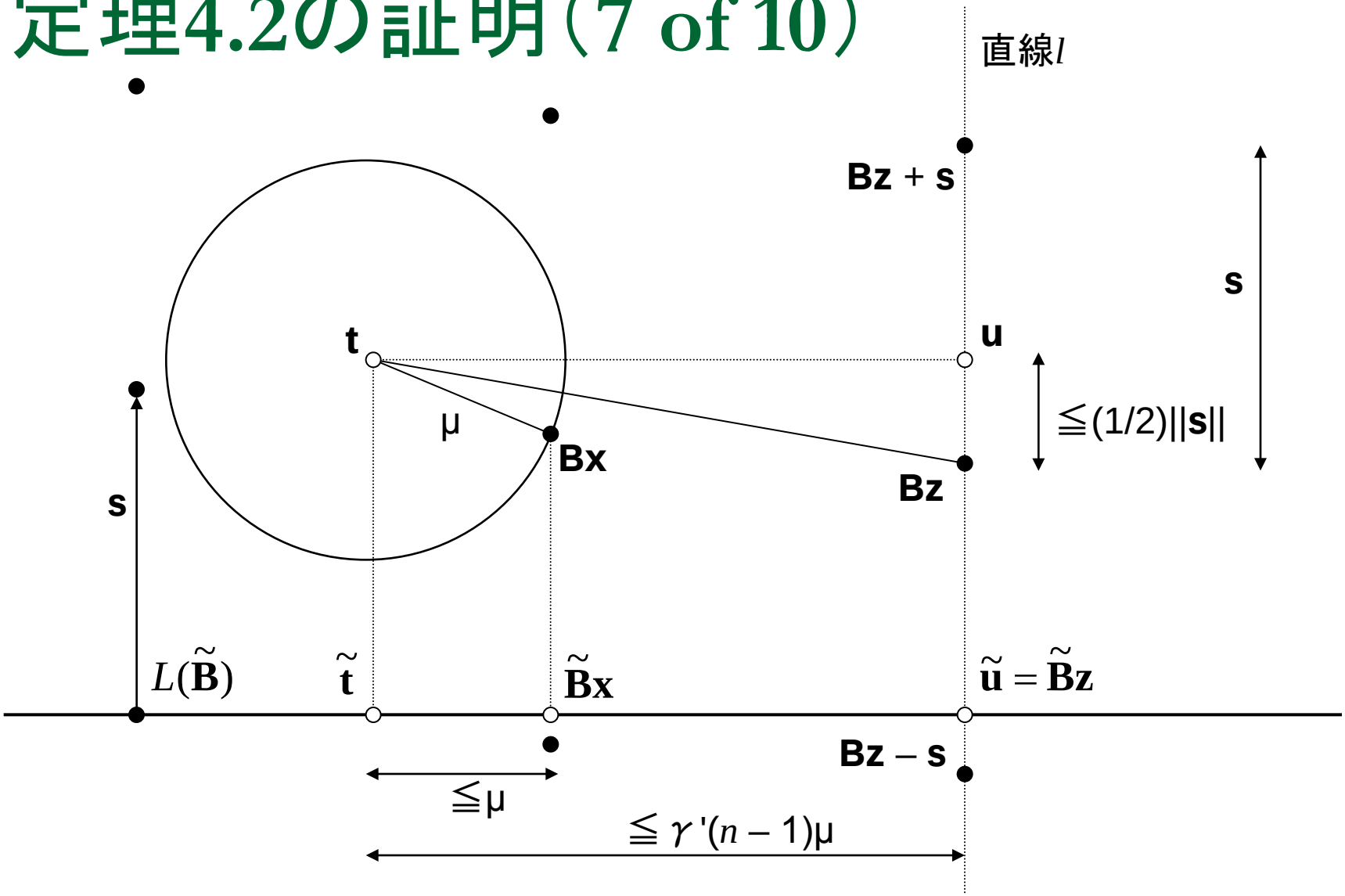
定理4.2の証明（6 of 10）

- $w = 0$ のとき
  - このとき，**s** := **Bx** は，$L(\mathbf{B})$ の短い非零ベクトル
  - すると，$\|\mathbf{s}\|^2 \leqq \gamma^2(\mu^2 + c^2)$（補題4.1の証明参照），$c \leq \mu\sqrt{1+\varepsilon} \Big/ \sqrt{(2/\gamma)^2 - 1}$ より，

$$\|\mathbf{s}\| < 2\mu\sqrt{\frac{1+\varepsilon}{(2/\gamma)^2 - 1}}$$

  - 次に，**B**，**t** を，**s** の直交補空間に射影する

定理4.2の証明（7 of 10）



定理4.2の証明（8 of 10）

- $\tilde{\mathbf{B}}, \tilde{\mathbf{t}}$ ：**B**, **t** を，**s** の直交補空間に射影したもの
  - $L(\tilde{\mathbf{B}})$ の階数は $n-1$ になる
- **Bx**：CVP例題（**B**，**t**）の解
  - よって，|| **Bx** – **t** || = μ = dist(**t**, L(**B**))
- 以上より，CVP例題 $(\tilde{\mathbf{B}}, \tilde{\mathbf{t}})$ の近似解を再帰的に探せば，$\tilde{\mathbf{t}}$ から距離 $\gamma'(n-1) \times \mu$ 以内，すなわち，

$$\left\| \tilde{\mathbf{u}} - \tilde{\mathbf{t}} \right\| \le \mu \sqrt{\frac{(n-1)(1+\varepsilon)}{(2/\gamma)^2 - 1}}$$

のようなベクトル $\tilde{\mathbf{u}} = \tilde{\mathbf{B}}\mathbf{z}$ を求められる.
（n≦2のとき，CVPを厳密に解くことができることに注意）

定理4.2の証明（9 of 10）

- 直線 $\ell := \left\{ \tilde{\mathbf{u}} + \alpha \mathbf{s} \,\middle|\, \alpha \in \mathrm{R} \right\}$
  - $\tilde{\mathbf{u}}$ に射影するすべての点の集合
- **u**：**t** の直線 l の上への直交射影
- 一般性を失うことなく，**Bz** が射影 **u** に最も近い，直線 l 上の格子点と仮定できる
  - もしそうでなければ，**s** の適当な整数倍を **Bz** に加えればよい
  - また，このことから，||**u** – **Bz**||≦(1/2)||**s**||がいえる

定理4.2の証明（10 of 10）

- 以上まとめて，Bz がもとの CVP例題の γ' 近似解であることが示せる．これは以下のとおり：

$$\|\mathbf{t}-\mathbf{Bz}\|^2 = \|\mathbf{t}-\mathbf{u}\|^2 + \|\mathbf{u}-\mathbf{Bz}\|^2$$

- 第一項：$\|\mathbf{t}-\mathbf{u}\|^2 = \|\tilde{\mathbf{u}}-\tilde{\mathbf{t}}\|^2 \le \dfrac{\mu^2(n-1)(1+\varepsilon)}{(2/\gamma)^2-1}$
- 第二項：$\|\mathbf{u}-\mathbf{Bz}\|^2 \le \left(\dfrac{1}{2}\|\mathbf{s}\|\right)^2 \le \dfrac{\mu^2(1+\varepsilon)}{(2/\gamma)^2-1}$
- 以上まとめて，$\|\mathbf{t}-\mathbf{Bz}\| \le \sqrt{\dfrac{(1+\varepsilon)n}{(2/\gamma)^2-1}}\mu = \gamma'(n)\times\mu$

（証明終）

今日の内容

- いくつかの基本的な概念
- 第4章の概要
- Kannan の同次化技法
- Ajtai – Micciancio 埋め込み
- SVPのNP困難性
- まとめ

定理4.2の帰着の問題点

- 再帰的に格子の階数を減らすことにより帰着している

再帰の各段階での誤差が累積して，
最適解から $O(n^{1/2})$ 離れる可能性がある

- 以降では，ある CVP例題を SVP の単一の例題に埋め込む，より効率の良い帰着について考える

準備 — 約定問題(promise problems)

- 判定問題の一般化
  - 近似の困難さを研究するのに適している.
- 約定問題の定義:
  - 互いに素な言語, すなわち, Π_{YES}, $\Pi_{NO} \subseteq \Sigma^*$ かつ, $\Pi_{YES} \cap \Pi_{NO} = \phi$, の対 (Π_{YES}, Π_{NO})
- 約定問題を解くとは
  - 例題 $I \in \Pi_{YES} \cup \Pi_{NO}$ が入力されるとき, $I \in \Pi_{YES}$ か $I \in \Pi_{NO}$ かを正しく決定することをいう
- 判定問題
  - 約定問題において $\Pi_{NO} = \Sigma^* - \Pi_{YES}$ となる場合.

約定問題における帰着

- 関数 $f : \Sigma^* \rightarrow \Sigma^*$ が (Π_{YES}, Π_{NO})から (Π_{YES}', Π_{NO}') への帰着であるとは，f がYES例題をYES例題に，NO例題をNO例題に写像することをいう
  - すなわち，$f(\Pi_{YES}) \subseteq \Pi_{YES}'$，かつ，$f(\Pi_{NO}) \subseteq \Pi_{NO}'$

約定問題 GapSVP$_\gamma$

- ギャップ関数 γ (階数 n の関数)によって，以下のように定義する:
  - YES例題: 基底 $\mathbf{B} \in Z^{m \times n}$，ある $\mathbf{z} \in Z^n - \{\mathbf{0}\}$ について$||\mathbf{Bz}|| \leqq r$ となるような有理数 $r \in Q$，について，対(**B**, r).
  - NO例題: 基底 $\mathbf{B} \in Z^{m \times n}$，すべての $\mathbf{z} \in Z^n - \{\mathbf{0}\}$ について$||\mathbf{Bz}|| > \gamma r$ となるような有理数 $r \in Q$，について，対(**B**, r).
- $\gamma = 1$ のとき，GapSVP$_\gamma$ は，厳密な SVP判定問題と同値

約定問題 $\mathbf{BinCVP}_{\gamma}$

- 基底 $\mathbf{B} \in \mathrm{Z}^{m \times n}$，目標ベクトル $\mathbf{t} \in \mathrm{Z}^{m}$，$r$ を正の整数，とする．このとき，
  - （$\mathbf{B}$, $\mathbf{t}$, r）は，$\mathbf{t} - \mathbf{Bz}$ が高々 r 個の1を含む 0-1 ベクトルであるようなベクトル $\mathbf{z} \in \{0,1\}^{n}$ が存在するなら，YES 例題．
  - （$\mathbf{B}$, $\mathbf{t}$, r）は，すべての $\mathbf{z} \in \mathrm{Z}^{n}$ とすべての $w \in \mathrm{Z} - \{0\}$ に対し，ベクトル $w\mathbf{t} - \mathbf{Bz}$ が $\gamma(m) \cdot r$ より多くの非零成分をもつなら，NO 例題．

Ajtai – Micciancio 埋め込みの概要(1)

- NP困難問題(BinCVP$_\gamma$)を，GapSVP$_\gamma$に帰着する
- 格子基底 **B** $\in Z^{m\times n}$，目標ベクトル **t** $\in Z^m$
- 整数行列 **T** $\in Z^{n\times k}$をかけて **B** をランダム化
- **BT** と **t** を，特殊な格子 **L** を使って高い次元に埋め込む
- 格子 **L** の性質:
  - 任意の格子間の距離が大きい
  - しかし，「密集した」格子点の集合があり，それらの点すべては span(**L**) の一点 **s** に近い

Ajtai – Micciancio 埋め込みの概要(2)

- (続き)格子

$$\mathbf{B}' := \begin{bmatrix} a\mathbf{BT} & a\mathbf{t} \\ b\mathbf{L} & b\mathbf{s} \end{bmatrix}$$

を考える. a, b は適当な因子.

- 基本的なアイディア: **t** に近い格子ベクトル **v**$\in L$(**B**) が存在すれば, **B'** の最後の列に –1 を掛けて, **BTz** = **v** となるような **s** に近い格子点 **Lz** を探すことで, **B'** の中に短いベクトルを見出すことができる.

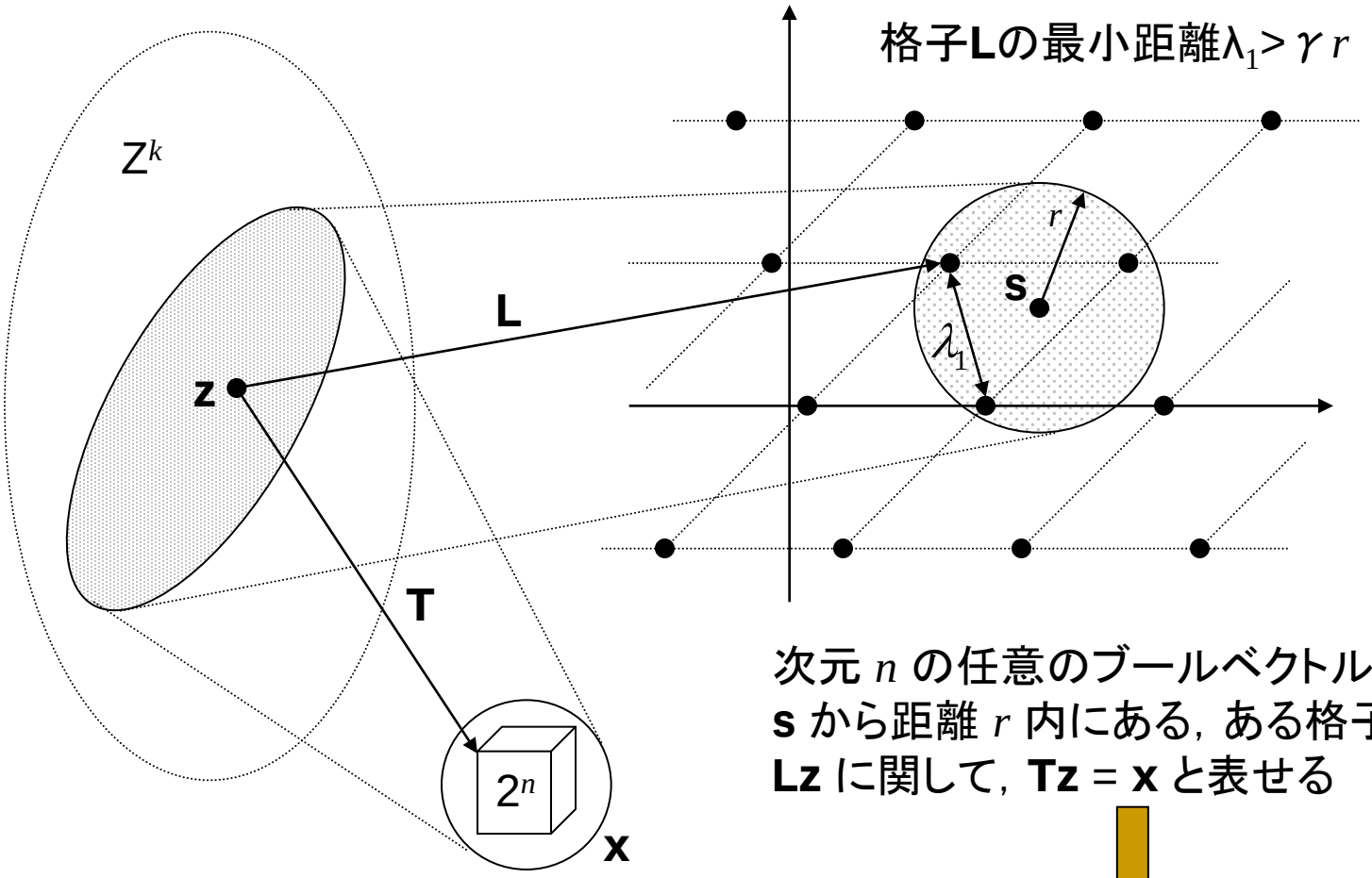
補題4.3（球充填補題）

- 任意の l_p ノルム（$p \geqq 1$）と定数 $\gamma < 2^{1/p}$ に対し，n が入力されるとき，n の多項式時間で，
  - 格子 $\mathbf{L} \in Z^{k' \times k}$
  - ベクトル $\mathbf{s} \in Z^{k'}$
  - 行列 $\mathbf{T} \in Z^{n \times k}$
  - 有理数 r

  を出力する多項式時間アルゴリズム（確率的または非一様の可能性あり）が存在する．ただし，$\mathbf{L}$，$\mathbf{s}$，$\mathbf{T}$，r は以下を満たすものとする．
  - すべての $\mathbf{z} \in Z^k - \{\mathbf{0}\}$ に対して $\|\mathbf{Lz}\|_p > \gamma r$ ．
  - （高い確率で）すべてのブールベクトル $\mathbf{x} \in \{0, 1\}^n$ に対して，$\mathbf{Tz} = \mathbf{x}$ かつ $\|\mathbf{Lz} - \mathbf{s}\|_p < r$ である $\mathbf{z} \in Z^k$ が存在する．

- 上記の種々のアルゴリズム（確定的，確率的，非一様）の証明は後ほど！

同次化の仕掛け



次元 n の任意のブールベクトル **x** は，
s から距離 r 内にある，ある格子ベクトル
Lz に関して，**Tz** = **x** と表せる

s を中心とする半径 r の球が，
少なくとも 2^n 個の格子点を含む

定理4.4

- 任意の $p \geqq 1$ に対し，補題4.3のアルゴリズムが与えられると，NP困難問題を l_p における GapSVP $_\gamma$ に，任意の定数近似因子 $\gamma < 2^{1/p}$ に対し，多項式時間で帰着することができる.

定理4.4 の証明(1)

- l_p ノルムと $\gamma < 2^{1/p}$ を固定し，$\tilde{\gamma} < (\gamma, \sqrt[p]{2})$ とする
- さらに

$$\hat{\gamma} := \frac{2^p}{(1/\gamma)^p - (1/\tilde{\gamma})^p}$$

とする

- $\mathrm{BinCVP}_{\hat{\gamma}}$ を，GapSVP_{γ} に帰着する． $\hat{\gamma}$ は n に

独立なので，$\mathrm{BinCVP}_{\hat{\gamma}}$ は NP 困難．

定理4.4 の証明(2)

- $(\mathbf{B}, \mathbf{t}, d)$ を，$\mathrm{BinCVP}_{\hat{\gamma}}$ の例題とする．ここで，$\mathbf{B} \in \mathbb{Z}^{m \times n}$，$\mathbf{t} \in \mathbb{Z}^{m}$．
- 補題 4.3 のアルゴリズムを実行し，以下のような $\mathbf{L} \in \mathbb{Z}^{k' \times k}$，$\mathbf{s} \in \mathbb{Z}^{k'}$，$\mathbf{T} \in \mathbb{Z}^{n \times k}$，有理数 r を得る:
  - すべての $\mathbf{z} \in \mathbb{Z}^{k} - \{\mathbf{0}\}$ に対して $\left\|\mathbf{Lz}\right\|_{p} > \tilde{\gamma} r$ ．
  - (高い確率で)すべての $\mathbf{x} \in \{0, 1\}^{n}$ に対して，$\mathbf{Tz} = \mathbf{x}$ かつ $\|\mathbf{Lz} - \mathbf{s}\|_{p} < r$ である $\mathbf{z} \in \mathbb{Z}^{k}$ が存在する．

定理4.4 の証明(3)

- a, b を,

$$\frac{r}{2\sqrt[p]{d}}\sqrt[p]{\left(\frac{\tilde{\gamma}}{\gamma}\right)^p - 1} < \frac{a}{b} < \frac{r}{\sqrt[p]{d}}\sqrt[p]{\left(\frac{\tilde{\gamma}}{\gamma}\right)^p - 1}$$

  を満たす二つの整数とする.

- このとき,

$$\sqrt[p]{a^p d + b^p r^p} < d' < br\left(\frac{\tilde{\gamma}}{\gamma}\right)$$

  となる有理数 d' を見出せる. 導出は略(教科書は typo があるので注意)

定理4.4 の証明(4)

- 格子

$$\mathbf{B}' := \begin{bmatrix} a\mathbf{BT} & a\mathbf{t} \\ b\mathbf{L} & b\mathbf{s} \end{bmatrix}$$

を考える

- (**B**, **t**, d) が $\mathrm{BinCVP}_{\hat{\gamma}}$のYES例題なら (**B'**, d') は GapSVP_{γ} のYES例題であり，もし(**B**, **t**, d) がNO例題であれば，(**B'**, d')もNO例題になることを示せばよい.

定理4.4 の証明(5)

- (**B**, **t**, d) を, $\mathrm{BinCVP}_{\hat{\gamma}}$ のYES例題とする
  - すなわち, **t** – **Bx** が 0-1 ベクトルでありかつその1の個数が高々 d であるような, **x** $\in\{0, 1\}^k$ が存在する. このとき, $\|\mathbf{Bx} - \mathbf{t}\|_p \leqq d^{1/p}$.
- 構成より, **Tz** = **x** かつ $\|\mathbf{Lz} - \mathbf{s}\|_p < r$ であるような, **z** $\in Z^k$ が存在. ここで, **w** = [**z**^{T}, -1]^{T}とすると,

$$\left\|\mathbf{B}'\mathbf{w}\right\|_p^p = a^p \left\|\mathbf{Bx}-\mathbf{t}\right\|_p^p + b^p \left\|\mathbf{Lz}-\mathbf{s}\right\|_p^p$$

$$\leq a^p d + (br)^p < (d')^p$$

これは, (**B'**, d') がYES例題であることを意味する.

定理4.4 の証明(6)

- (**B**, **t**, d) を, $\mathrm{BinCVP}_{\hat{\gamma}}$ のNO例題とし, **w** = $[\mathbf{z}^T, w]^T$ とする.

$$\left\|\mathbf{B}'\mathbf{w}\right\|_p^p = a^p \left\|\mathbf{B}\mathbf{x} + w\mathbf{t}\right\|_p^p + b^p \left\|\mathbf{L}\mathbf{z} + w\mathbf{s}\right\|_p^p$$

ここで, $a||\mathbf{Bx} + w\mathbf{t}||_p > \gamma d'$ あるいは $b||\mathbf{Lz} + w\mathbf{s}||_p > \gamma d'$ を証明することができる. 詳細は教科書参照.

(証明終)

今日の内容

- いくつかの基本的な概念
- 第4章の概要
- Kannan の同次化技法
- Ajtai – Micciancio 埋め込み
- SVPのNP困難性
- まとめ

SVP のNP困難性について

- 補題4.3において（**L**, **T**, **s**, r）を計算するアルゴリズムがあれば，NP困難問題を，GapSVPに効率よく帰着できた
- しかし，決定性多項式時間で計算するアルゴリズムは知られていない
  - 定理4.4 は，Karp or Cook 帰着ではない
- 以降では，NP困難問題が，GapSVPに異なるタイプで帰着されることを考察
  - ランダム帰着の下での困難性
  - 非一様帰着の下での困難性
  - 決定性帰着の下での困難性

各種の帰着について

- 具体的な内容は本発表では省略，教科書を参照されたい

今日の内容

- いくつかの基本的な概念
- 第4章の概要
- Kannan の同次化技法
- Ajtai – Micciancio 埋め込み
- SVPのNP困難性

- まとめ

まとめ

- 最短ベクトル問題（SVP）を近似する困難性について考察
- Kannan の同次化（同質化，homogenization）技法を拡張して，近似CVPを，近似SVPに帰着
- l_p ノルムにおいて，$2^{1/p}$ より小さな近似因子で SVP を近似することが困難であることを示した