暗号のための格子の理論
Daniele Micciancio (著), Shafi Goldwasser (著)
林 彬 (翻訳)

第7章 基底簡約問題

北陸先端科学技術大学院大学 (JAIST)
高信頼性組み込みシステム教育研究センター
研究員 江村恵太

本章の(大まかな)目的

- 格子に対する (基底の簡約に関連した) 問題を種々定義し, それぞれの関係性 (他方が解けると他方も解ける, 同値であるなど) を示すこと
  - Shortest Vector Problem（SVP）
  - Successive Minima Problem (SMP)
  - Shortest Linearly Independent Vectors Problem (SIVP)
  - Shortest Basis Problem (SBP)
  - Korkin-Zolotarev（コルキン―ゾルタレフ）problem (KZP) ・・・
- 基底の簡約に関連とは？
  - おおざっぱにいうと (問題ごとに定義される) ある条件をみたす基底を計算する (or そのような条件をみたす基底が存在するかどうかを判定する)
  - 例：格子がある基底 $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ で定義されているとき, 同じ格子を生成する ($\mathbf{B}$ とは別の) 基底 $\mathbf{B}' = (\mathbf{b}'_1, \ldots, \mathbf{b}'_n)$ で $\max_i ||\mathbf{b}'_i|| \leq \max_i ||\mathbf{b}_i||$ なものを求めよ (もしくはそのような $\mathbf{B}'$ が存在するかどうかを判定せよ)
- (たぶん) 本章の主要な結果
  - SVP_γ あるいは KZP_γ の解は (本テキストにある) 全ての格子簡約問題を因子 $\gamma\sqrt{n}$ 内で解く

(整数)格子 (Lattice)

格子基底 (lattice basis)

$\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^m$ $(m \geq n)$: 線型独立な (列) ベクトル

$\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{Z}^{m \times n}$: 行列表記

n : 格子の階数 (rank)

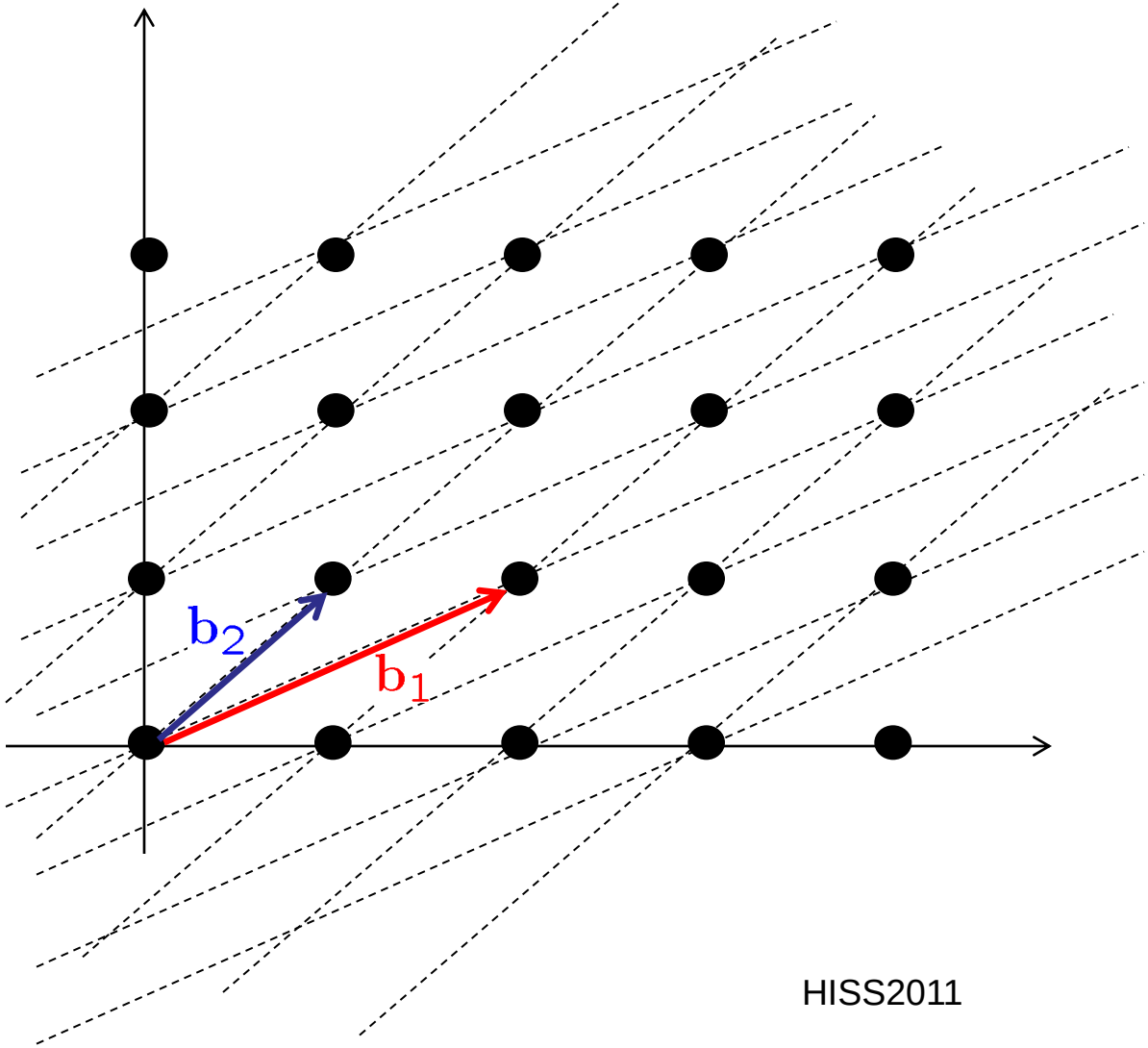
m : 格子の次元 (dimention)

$\mathbb{Z}^m$における格子

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

$$\Lambda = \mathcal{L}(\mathbf{B}) := \left\{ \mathbf{Bx} \ : \ \mathbf{x} \in \mathbb{Z}^n \right\}$$

（整数）格子 (Lattice)



$$\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2] \in \mathbb{Z}^{2\times 2}$$

帰着（Reduction）

- （問題Aから問題Bへの）Karp帰着
  - あるxがAの解　iff f(x)がBの解
  - f は多項式時間計算可能

- （問題Aから問題Bへの）Cook帰着
  - 問題Bの解を返すオラクルにアクセス可能なチューリングマシンがAを解くことが出来る

最短ベクトル問題 (定義1.1)
Shortest Vector Problem（SVP）

- Input

  基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$

- Output

  $\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ s.t.

どんなyを持ってきても, Bxの大きさよりByの大きさが同じか大きい

$$\forall \mathbf{y} \in \mathbb{Z}^n \setminus \{\mathbf{0}\},\ ||\mathbf{Bx}|| \leq ||\mathbf{By}||$$

(特筆しない場合はℓ_2ノルム)

最近ベクトル問題(定義1.2)
Closest Vector Problem（CVP）

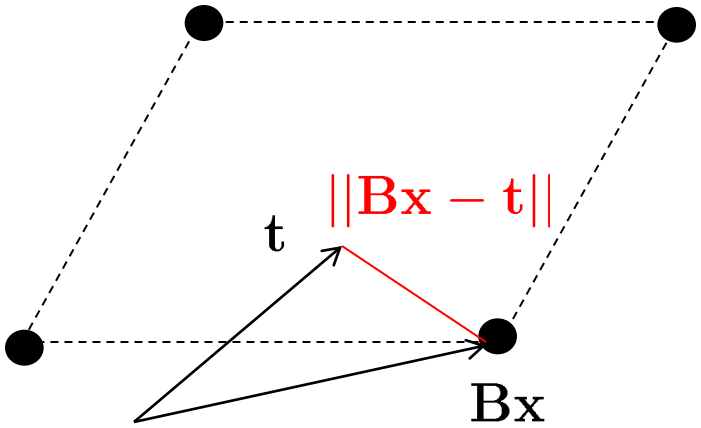
- Input

  基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$, 目標ベクトル $\mathbf{t} \in \mathbb{Z}^m$

- Output

  $\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ s.t.

  $\forall \mathbf{y} \in \mathbb{Z}^n \setminus \{\mathbf{0}\},\ ||\mathbf{Bx} - \mathbf{t}|| \leq ||\mathbf{By} - \mathbf{t}||$



SVPとCVPとの関係性
(SVPはCVPにCook帰着可能) は3章参照

GapSVPγ (定義1.5)

- Input

  基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$, 実数 r

本では有理数だが, 下記の参考論文でreal numberと定義されていたので, ここでは実数とした

- Output
  - Yes if

    $\mathbf{B}$のshortest vector $\mathbf{x}$に対し, $||\mathbf{Bx}|| \leq r$

  - No if

    $\mathbf{B}$のshortest vector $\mathbf{x}$に対し, $||\mathbf{Bx}|| > \gamma r$

Approximation factor γは通常格子次元mの関数 (γ=γ(m))

- （参考）
  - Vadim Lyubashevsky and Daniele Micciancio, “On Bounded Distance Decoding Unique Shortest Vectors, and the Minimum Distance Problem”, CRYPTO2009.
- GapSVPγ：任意のγに対し, NP-hard
  - S. Khot, Hardness of approximating the shortest vector problem in lattices, FOCS, 2004, pp. 126–135.

γ近似逐次最小問題(定義7.1)
Successive Minima Problem (SMPγ)

- Successive minima (逐次最小)
  - Johannes Blomer and Stefanie Naewe, “Sampling Methods for Shortest Vectors, Closest Vectors and Successive Minima”, ICALP2007
- $i \in \mathbb{Z}$ s.t. $i \leq n$ (n： 格子Λのrank) に対しΛがi個の線型独立な(高々長さ$r \in \mathbb{R}$の)ベクトルを含むとき, rをΛのi-th successive minimumと呼び, $\lambda_i = \lambda_i(\Lambda)$と表記する.

  格子Λの線形独立な格子ベクトルを短い順に並べたものを$\mathbf{s}_1, \ldots, \mathbf{s}_n$と書くと, 長さがそれぞれ$\lambda_1, \ldots, \lambda_n$というように取れるということ

- SMPγ
  - Input

    基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$
  - Output

    全ての$i = 1, 2, \ldots, n$に対して $||\mathbf{s}_i|| \leq \gamma \lambda_i$であるような線型独立なベクトルの集合$\mathbf{S} = (\mathbf{s}_1, \ldots, \mathbf{s}_n)$

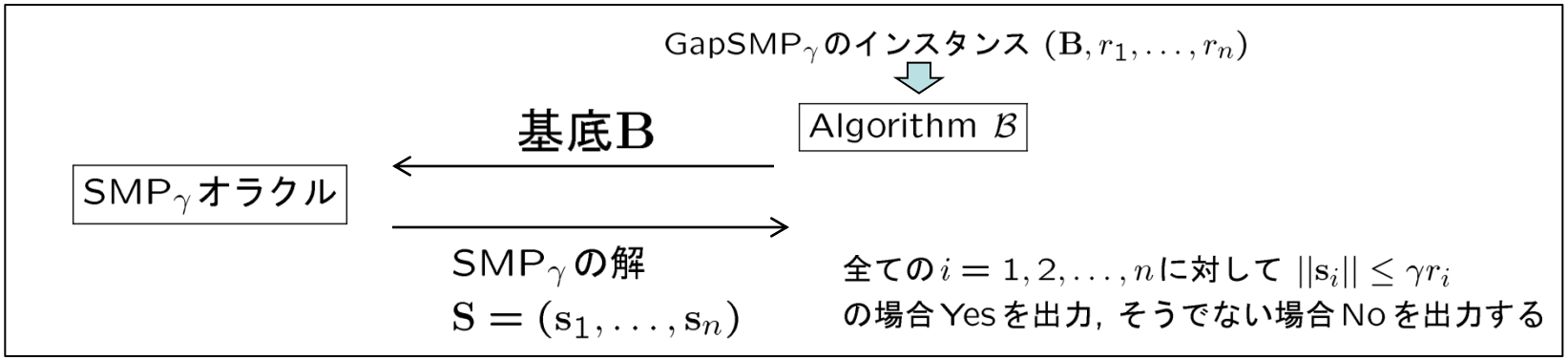
  In the successive minima problem SMP_γ we are given a lattice Λ with rank n. We are asked to find n linearly independent vectors $\mathbf{s}_1, \ldots, \mathbf{s}_n$ such that the length of $\mathbf{s}_i$ $(i = 1, \ldots, n)$ is at most $\gamma \lambda_i(\Lambda)$.
- GapSMPγ
  - Input

    基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$, 実数列$r_1, \ldots, r_n$
  - Output
    - Yes if 全ての$i = 1, 2, \ldots, n$に対して $\lambda_i \leq r_i$
    - No if $\lambda_i > \gamma r_i$なる$i \in [1, n]$が存在する

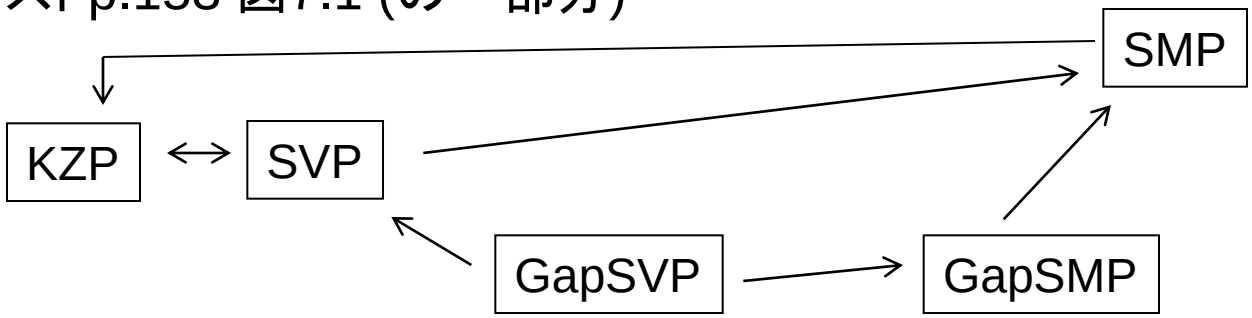
基底ではない可能性もある

SMPγとそれ以外の問題との関係性

- SMPγが解ければGapSMPγも解ける
  - SMP_γ を解くオラクルが出力する $\mathbf{S} = (\mathbf{s}_i, \ldots, \mathbf{s}_n)$ に対し，各 i で $||\mathbf{s}_i|| \leq \gamma r_i$ かどうかを確認すればいい



- SMPγが解ければSVPγも解ける
  - SMP_γ を解くオラクルが出力する $\mathbf{S} = (\mathbf{s}_1, \ldots, \mathbf{s}_n)$ に対し，$\mathbf{s}_1$ は SVP_γ の解
- GapSMPγが解ければGapSVPγも解ける
- テキストp.153 図7.1 (の一部分)



ミンコフスキー簡約基底

- 定義7.2 Minkowski reduced basis

  …

- P.140より抜粋
  - ミンコフスキー簡約基底は格子問題の計算量の研究において, 特に重要な役割を果たすことがないので,ミンコフスキー簡約基底に付随する問題を定義しない等々
  - というわけで略

γ近似最短基底問題
Shortest Basis Problem (SBPγ)

- 基底ベクトル $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^m$ $(m \geq n)$ に対し，

$$\mu(\mathbf{B}) := \max_i ||\mathbf{b}_i||$$

格子 Λ を生成する全ての基底 $\mathbf{B}$ に対し，$\mu(\Lambda)$ を $\mu(\mathbf{B})$ の最小値と定義する

- SBPγ
  - Input
    基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$
  - Output
    $\mu(\mathbf{B}') \leq \gamma\mu(\Lambda)$ $(\Lambda = \mathcal{L}(\mathbf{B}))$ をみたす Λ の基底 $\mathbf{B}'$
- GapSBPγ
  - Input
    基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$，実数 r
  - Output
    - Yes if　$\mu(\mathbf{B}') \leq r$ をみたす Λ の基底 $\mathbf{B}'$ が存在する
    - No if　$\mathbf{B}$ と同値な (=Λ を生成する) 全ての基底 $\mathbf{B}'$ に対し，$\mu(\mathbf{B}') > \gamma r$

SBPγが解ければ
GapSBPγも解ける

GapSBP → SBP

図7.1 (の一部分)

γ近似最短独立ベクトル問題
Shortest Independent Vectors Problem (SIVPγ)

- SIVPγ
  - Input

    基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$
  - Output

    全ての$i = 1, 2, \ldots, n$に対して $\max ||\mathbf{s}_i|| \leq \gamma \lambda_n(\mathcal{L}(\mathbf{B}))$ であるような線型独立な格子ベクトル$\mathbf{s}_1, \ldots, \mathbf{s}_n$
- GapSIVPγ
  - Input

    基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$, 実数$r$
  - Output
    - Yes if $\lambda_n(\mathcal{L}(\mathbf{B})) \leq r$
    - No if $\lambda_n(\mathcal{L}(\mathbf{B})) > \gamma r$

逐次最小問題 (SMP) と異なり,
各$\mathbf{s}_i$が$||\mathbf{s}_i|| \leq \gamma \lambda_i$ でなくともよい

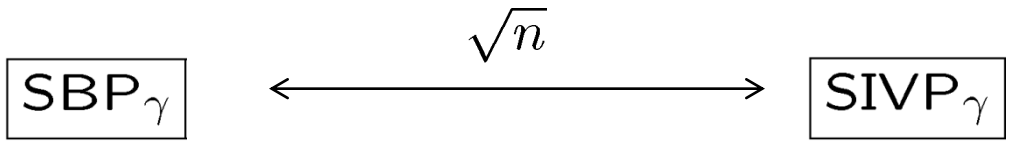
SMP_γの任意の解はSIVP_γの解なので,
SIVP_γはSMP_γに自明に帰着される

SVIP ⟶ SMP

SBPとSIVPとの関係性

- 定理7.3

  任意の近似因子γ, 格子のrank nに対し, $\mathrm{SBP}_{\gamma\sqrt{n}}$から$\mathrm{SIVP}_{\gamma}$へのCook帰着,
  及び$\mathrm{SIVP}_{\gamma\sqrt{n}}$から$\mathrm{SBP}_{\gamma}$へのCook帰着が存在する.



- 証明 (SBP→SIVP (SIVPが解けたらSBPが解ける))

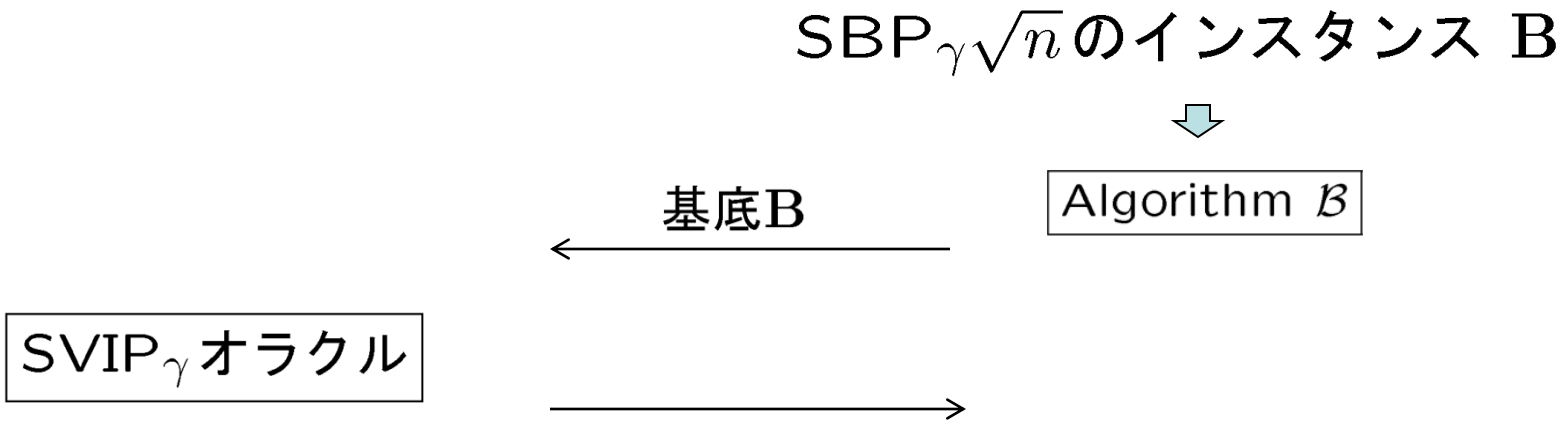
  以下の補題7.1を利用する

補題7.1 格子基底$\mathbf{B}$及び線型独立なベクトル$\mathbf{s}_1, \ldots, \mathbf{s}_n$ (ただし$||\mathbf{s}_1|| \leq ||\mathbf{s}_2|| \leq \cdots \leq ||\mathbf{s}_n||$
かつ$\mathbf{S} := (\mathbf{s}_1, \ldots, \mathbf{s}_n) \subset \mathcal{L}(\mathbf{B})$) を入力すると, 以下をみたす$\mathbf{R} := (\mathbf{r}_1, \ldots, \mathbf{r}_n)$を出力する
多項式時間アルゴリズムが存在する.

Sは(基底ではないかもしれないが)格子には属している

- すべての$i = 1, \ldots, n$に対し, $||\mathbf{r}_i|| \leq \max\{(\sqrt{i}/2)||\mathbf{s}_i||, ||\mathbf{s}_i||\}$
- $\mathbf{R}$は$\mathbf{B}$と同値 (同じ格子を生成する)

SBP→SIVP



SVIP$_\gamma$の解$\mathbf{S} = (\mathbf{s}_1, \ldots, \mathbf{s}_n)$

$$\mu(\mathbf{S}) := \max_i ||\mathbf{s}_i|| \leq \gamma \lambda_n(\mathcal{L}(\mathbf{B}))$$

入力$\mathbf{B}$, $\mathbf{S}$について補題7.1を実行すると，以下をみたす$\mathbf{R} = (\mathbf{r}_1, \ldots, \mathbf{r}_n)$を得る

$$||\mathbf{r}_i|| \leq \max\{(\sqrt{i}/2)||\mathbf{s}_i||, ||\mathbf{s}_i||\} \leq \sqrt{n}||\mathbf{s}_i||$$

$(i \in [1, n])$

SBP→SIVP

$$||\mathbf{r}_i|| \leq \max\{(\sqrt{i}/2)||\mathbf{s}_i||, ||\mathbf{s}_i||\} \leq \sqrt{n}||\mathbf{s}_i||$$

$(i \in [1, n])$

$n \geq 1$ より, $||\mathbf{s}_i|| \leq \sqrt{n}||\mathbf{s}_i||$

$i \leq n$ より, $\sqrt{i}/2 \leq \sqrt{n}/2 \leq \sqrt{n}$ なので, $\sqrt{i}/2||\mathbf{s}_i|| \leq \sqrt{n}||\mathbf{s}_i||$

⇧

(今 $\sqrt{n}/2 \geq 1$ の場合を考えれば十分なので成立)

$\mathbf{S} = (\mathbf{s}_1, \ldots, \mathbf{s}_n)$ はSVIP$_\gamma$の解なので

$$\sqrt{n}||\mathbf{s}_i|| \leq \sqrt{n}\left(\gamma\lambda_n(\mathcal{L}(\mathbf{B}))\right) = \left(\gamma\sqrt{n}\right)\lambda_n(\mathcal{L}(\mathbf{B}))$$

⇒ 基底 $\mathbf{R} = (\mathbf{r}_1, \ldots, \mathbf{r}_n)$ はSBP$_{\gamma\sqrt{n}}$の解

SIVP→SBP

- 証明 (SIVP→SBP (SBPが解けたらSIVPが解ける)))

以下の系7.2を利用する

階数nの任意の格子Λに対し，全ての$k = 1, \ldots, n$について

$$||\mathbf{b}_k|| \leq \max\{1, \sqrt{k}/2\} \cdot \lambda_k$$

である基底が存在する

特に$\mu(\Lambda) := \max_i ||\mathbf{b}_i|| \leq \max\{1, \sqrt{n}/2\} \cdot \lambda_n(\Lambda) \leq \sqrt{n} \cdot \lambda_n(\Lambda)$

SIVP$_{\gamma\sqrt{n}}$の
解を作るための変形

最短基底の長さ$\mu(\Lambda)$は高々$(\sqrt{n}/2)\lambda_n$なので，
もちろん$\mu(\Lambda)$は$\sqrt{n} \cdot \lambda_n(\Lambda)$で抑えられる

SIVP→SBP

$\mathrm{SIVP}_{\gamma\sqrt{n}}$のインスタンス $\mathbf{B}$

Algorithm $\mathcal{B}$

基底$\mathbf{B}$ ←

SBP_γオラクル →

SBP_γの解$\mathbf{R} = (\mathbf{r}_1, \ldots, \mathbf{r}_n)$

$$\mu(\mathbf{R}) \leq \gamma \cdot \mu(\mathcal{L}(\mathbf{B})) \leq \left(\gamma\sqrt{n}\right)\lambda_n(\mathcal{L}(\mathbf{B}))$$

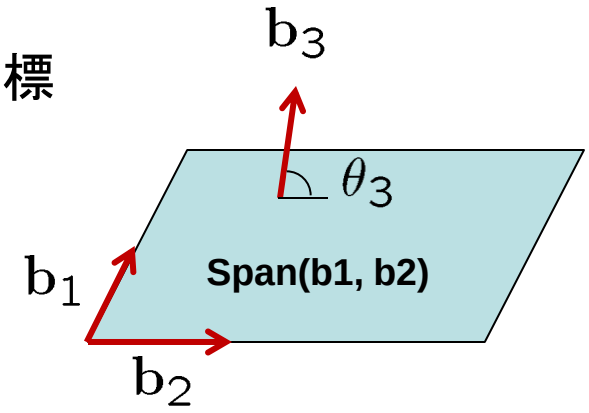
$\mathbf{R}$はSBP_γの解

系7.2より

基底$\mathbf{R} = (\mathbf{r}_1, \ldots, \mathbf{r}_n)$は$\mathrm{SIVP}_{\gamma\sqrt{n}}$の解

直交性欠陥とKZ簡約
Orthogonality Defect and KZ reduction

- 直交性欠陥
  - 基底がどの程度直交に近いのか？を測る指標



θ_i ： $\mathbf{b}_i$ と $\mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})$ との間の角

$\mathbf{b}_i^*$ ： $\mathbf{b}_i$ のグラムシュミット直交化ベクトル

$\det(\mathcal{L}(\mathrm{B})) = \prod_{i=1}^{n} ||\mathbf{b}_i^*||$ （格子の行列式は直交化ベクトルの長さの積）

$||\mathbf{b}_i^*|| = ||\mathbf{b}_i|| \cos\theta_i$

$$\prod_i ||\mathbf{b}_i|| = \prod_i \frac{||\mathbf{b}_i^*||}{\cos\theta_i} = \frac{\det \mathbf{B}}{\prod_i \cos\theta_i} \geq \det \mathbf{B}$$

$$\frac{\prod_i ||\mathbf{b}_i||}{\det \mathbf{B}} \quad (\geq 1)$$ を直交性欠陥 (Orthogonality Defect) と定義

全ての基底ベクトルが直交する（$\theta_i = \pi/2$）ときに限り，最小値１を取る

(直交性欠陥をより1に近づけることが，より直交している基底ベクトルを見出すことに対応)

コルキン―ゾルタレフ簡約
Korkin-Zolotarev reduction

- 定義7.8

  $\mathbf{B}$: 階数nの格子基底

  $\mathbf{B}^*$: $\mathbf{B}$に対応するグラム-シュミット直交化基底

ベクトル$\mathbf{x}$を$\mathrm{span}(\mathbf{b}_i^*, \ldots, \mathbf{b}_n^*)$に直交写像 (map $\mathbf{x}$ to orthogonally to $\mathrm{span}(\mathbf{b}_i^*, \ldots, \mathbf{b}_n^*)$)
する関数π_iを以下で定義する

$$\pi_i(\mathbf{x}) = \sum_{j \geq i} \frac{\langle \mathbf{x}, \mathbf{b}_j^* \rangle}{||\mathbf{b}_j^*||^2} \mathbf{b}_j^*$$

i より大きい j に対して計算 (明示的には書いてはいないが j は n まで動く)

基底$\mathbf{B}$がコルキン-ゾルタレフ (KZ) 簡約されている

def ⇔

- $\mathbf{b}_i^*$は$\pi_i(\mathcal{L}(\mathbf{B}))$の最短非零ベクトル　($\gamma$近似KZの場合, $||\mathbf{b}_i^*|| \leq \gamma \cdot \lambda_i$)
- 全ての$j < i$に対し, $\mathbf{B}$のグラム-シュミット係数$\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}$が$|\mu_{i,j}| \leq \frac{1}{2}$

コルキン―ゾルタレフ簡約
Korkin-Zolotarev reduction

- 注意
  - $\pi_i(\mathbf{x})$ の定義で $\mathbf{x}$ はベクトルにもかかわらず, KZ 簡約基底の定義に $\pi_i(\mathcal{L}(\mathbf{B}))$ と格子 $\mathcal{L}(\mathbf{B})$ に対して π_i を作用させている ???
  - 以下の論文で定義を再確認しました
    - J. C. Lagarias, H. W. Lenstra, Jr., and C.-P. Schnorr. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. Combinatorica, 10(4):333–348, 1990.

$$\pi_i(\mathcal{L}(\mathbf{B})) : \text{ a lattice of rank } n-i+1 \text{ with basis } [\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_n)]$$

  - （どうでもいいですが）本ではKorkineとなっているが, 実際はKorkinさんのようです

γ近似コルキン-ゾルタレフ問題

Korkin-Zolotarev Problem (KZPγ)

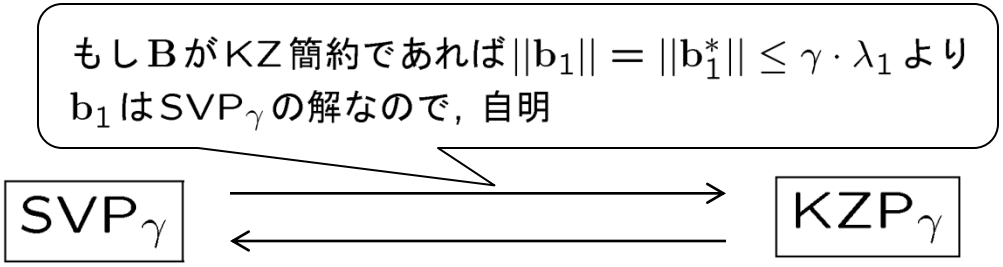
- KZPγ
  - Input

    基底 $\mathbf{B} \in \mathbb{Z}^{m \times n}$
  - Output

    $\mathbf{B}$と同値な（＝同じ格子を生成する）KZ_γ簡約基底

- 定理7.6

任意の近似因子γに対し，SVP_γとKZP_γはCook帰着の下で同値である

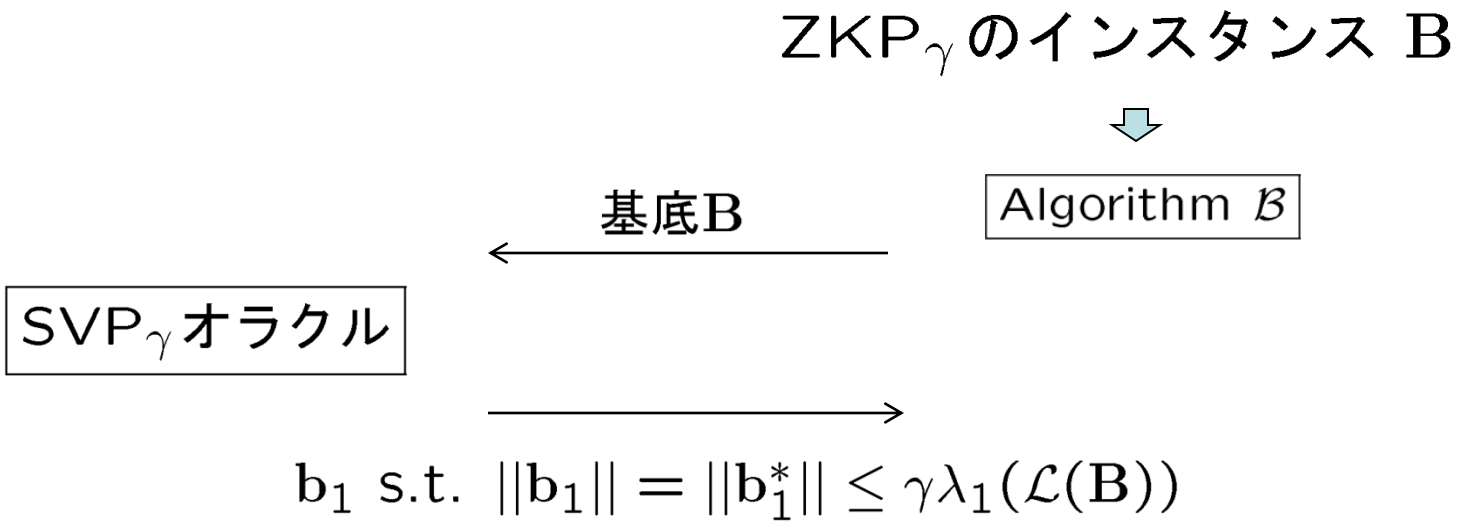


以下, SVP←KZPを見ていく

SVP←KZP

- 証明

  SVP_γオラクルを利用してKZP_γを解く



SVP←KZP

$\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$ が得られた後, $\mathbf{b}_i$ を次のように決定していく

$\Lambda_i = \pi_i(\mathcal{L}(\mathbf{B}))$: $\Lambda = \mathcal{L}(\mathbf{B})$ の $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$ の直交補空間への写像

(ややこしいが) 定義では$\mathrm{span}(\mathbf{b}_i, \ldots, \mathbf{b}_n)$となっていたものを$\mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})$で考えるということ.

$[\pi_i(\mathbf{b}_1), \ldots, \pi_i(\mathbf{b}_{i-1})]$ をSVPオラクルへの入力基底とし, 返答されたベクトルを $\mathbf{b}_i$ とする

$\mathbf{b}_i$ はSVP_γの解なので, その $\mathbf{b}_i$ を π_i で写した $\mathbf{b}_i^* = \pi_i(\mathbf{b}_i)$ は, 格子 Λ_i における (γ 近似の意味で) shortest vector

$\Lambda = \mathcal{L}(\mathbf{B})$ は（逐次最小の定義から）高々長さが $\lambda_i(\Lambda)$ な i 個の線型独立なベクトルを含み, これらの少なくとも一個は$\mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})$に直交する非零成分を持つ.

Λ_i は（長さが高々$\lambda_i(\Lambda)$ な）非零ベクトルを含む.

$$||\mathbf{b}_i^*|| \leq ||\pi_i(\mathbf{b}_i)|| \leq \gamma \cdot \lambda_i(\Lambda)$$

SVP←KZP

- 繰り返していくと

$$||\mathbf{b}_i^*|| \leq \gamma\lambda_i \text{ な列 } (\mathbf{b}_1, \ldots, \mathbf{b}_n)$$

を得る.

- グラムシュミット系数の条件 (1/2以下) は, (CVPを解く)最近平面アルゴリズム(the nearest plane algorithm , 2章参照)を利用することでみたされる

格子 $(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})$ に対し，目標ベクトル $\mathbf{b}_i$ として最近平面アルゴリズムを実行，返ってきたベクトル $\mathbf{v}$ に対し，$\mathbf{b}_i$ を $\mathbf{b}_i - \mathbf{v}$ に置き換える.

Conclusion

- 本章では, 主に格子に対する (基底の簡約に関連した) 問題を種々定義し, それぞれの関係性 (他方が解けると他方が解ける, 同値であるなど) を示した

- 今回紹介した計算量仮定と実際の暗号で使われている計算量仮定 (例えばLWE) との関係性としては以下などが参考になる
  - Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In STOC 2005.
  - Chris Peikert and Brent Waters, Lossy Trapdoor Functions and Their Applications. In STOC 2008.
    - Regev showed that LWE is indeed hard on the average if standard lattice problems (like approximating the shortest vector problem) are hard in the worst case for quantum algorithms. No efficient (or even subexponential-time) quantum algorithms are known for the associated worst-case lattice problems, despite significant research efforts.

余談：LWE (Leaning With Error)

- $\mathbb{Z}_q^n \times \mathbb{Z}_q$上の確率分布$A_{\mathbf{z},\chi}$

整数$q \geq 2$，ある確率分布 $\chi : \mathbb{Z}_q \to \mathbb{R}^+$，次元$n \in \mathbb{Z}^+$及びベクトル$\mathbf{z} \in \mathbb{Z}_q^n$に対し，
$\mathbb{Z}_q^n \times \mathbb{Z}_q$上の変数 $(\mathbf{a}, \langle \mathbf{a}, \mathbf{z} \rangle + e)$ の確率分布を$A_{\mathbf{z},\chi}$と定義する．

演算は$\mathbb{Z}_q$上

$\mathbf{a} \leftarrow \mathbb{Z}_q^n$ (一様ランダムに選択)
$e \leftarrow \chi$ ($\mathbf{a}$とは独立)

- Leaning With Error (LWE)

$q = q(n)$及びχ：$\mathbb{Z}_q$上の確率分布に対し，uniformly randomに選ばれた$\mathbf{z} \leftarrow \mathbb{Z}_q^n$に対し，
$A_{\mathbf{z},\chi}$ と $\mathbb{Z}_q^n \times \mathbb{Z}_q$上の一様分布とを区別する問題をLWE問題$\mathrm{LWE}_{q,\chi}$と定義する．

$A_{\mathbf{z},\chi}$: $\mathbf{a} \leftarrow \mathbb{Z}_q^n,\ e \leftarrow \chi,\ (\mathbf{a}, \langle \mathbf{a}, \mathbf{z} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$

$\mathbb{Z}_q^n \times \mathbb{Z}_q$上の一様分布 : $\mathbf{b} \leftarrow \mathbb{Z}_q^n,\ c \leftarrow \mathbb{Z}_q,\ (\mathbf{b}, c) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$

識別