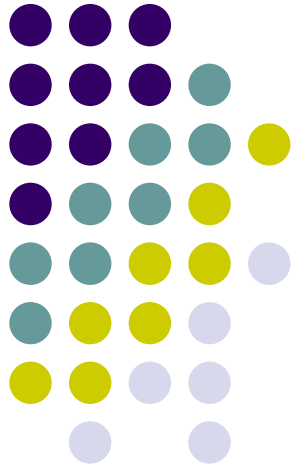
暗号理論のための格子の数学
（第3章　最近ベクトル問題）

第２８回情報セキュリティ研究会

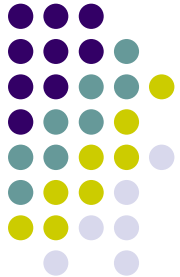
国立大学法人
北陸先端科学技術大学院大学
科学技術のフロンティアを拓く

面 和成

2010/01/05 (Tue.)

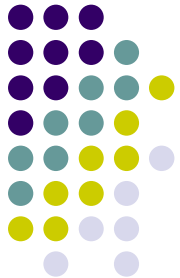


アジェンダ



- 最近ベクトル問題（CVP）とは？
- 3つの版のCVPの難しさについて
  - CVP判定版，CVP最適化版，CVP探索版
- CVPのNP完全性について
- CVPとSVP（最短ベクトル問題）の関係について

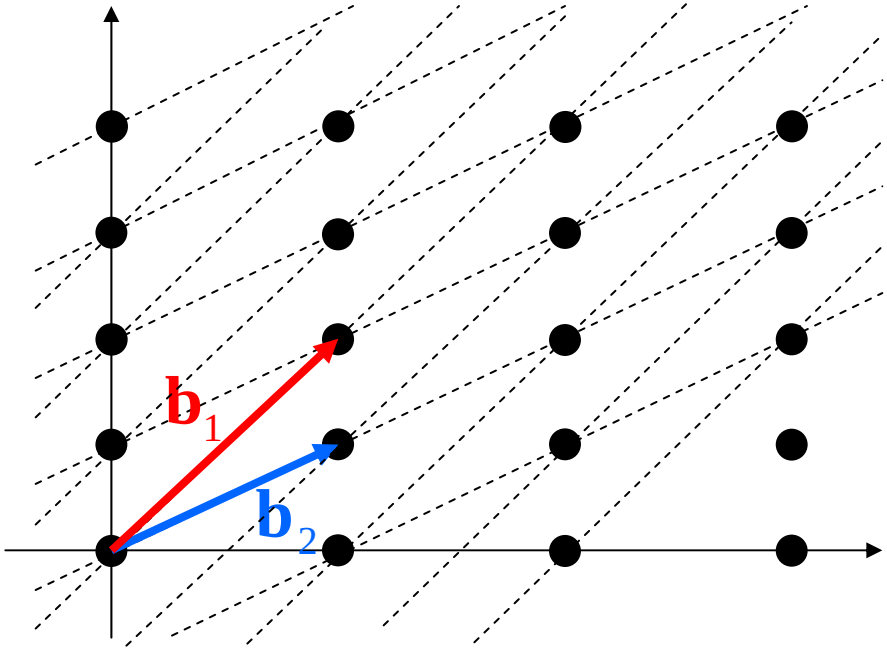
復習：最近ベクトル問題とは？



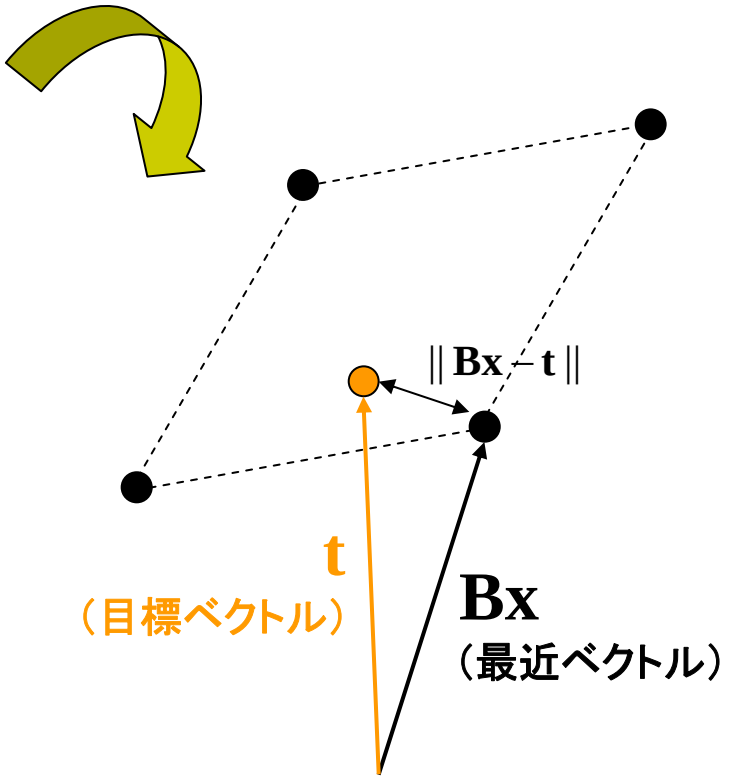
- 多項式時間解法が知られていない問題
- CVP（Closest Vector Problem）と表記する
- 定義1.2
  - 格子基底$\mathbf{B} \in Z^{m \times n}$と目標ベクトル$\mathbf{t} \in Z^{m}$が与えられたとき，目標ベクトル$\mathbf{t} \in Z^{m}$にもっとも近い格子ベクトル$\mathbf{Bx}$を見いだせ，すなわち他のいかなる$\mathbf{y} \in Z^{n}$に対しても$\| \mathbf{Bx} - \mathbf{t} \| \leq \| \mathbf{By} - \mathbf{t} \|$である整数ベクトル$\mathbf{x} \in Z^{n}$を見いだせ．
- パラメータ
  - m: 次元
  - n: 階数（格子基底の数）

復習：最近ベクトルについて（1/2）

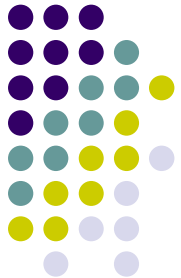
m=2, n=2の場合の格子
（2つの線形独立なベクトルの整数結合の集合）



格子基底：$\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2]$



復習：最近ベクトルについて（2/2）



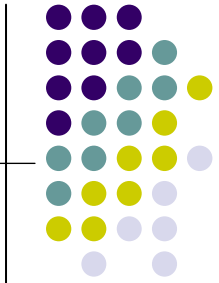
- 最近ベクトル

$$\mathbf{Bx} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_{11} & \cdots & b_{n1} \\ \vdots & & \vdots \\ b_{1m} & \cdots & b_{nm} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_{11}x_1 + \cdots + b_{n1}x_n \\ \vdots \\ b_{1m}x_1 + \cdots + b_{nm}x_n \end{bmatrix}$$

- 目標ベクトル

$$\mathbf{t} = \begin{bmatrix} t_1 \\ \vdots \\ t_m \end{bmatrix}$$

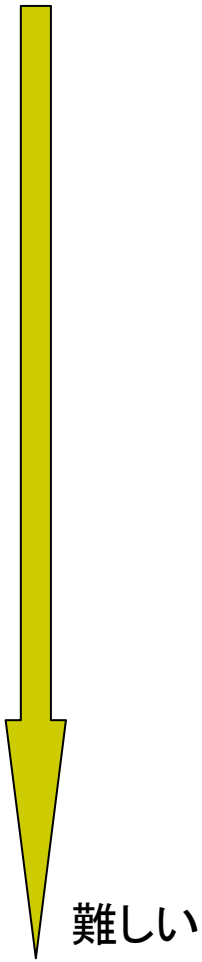
アジェンダ



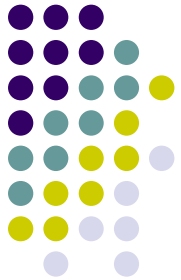
- 最近ベクトル問題（CVP）とは？
- 3つの版のCVPの難しさについて
  - CVP判定版，CVP最適化版，CVP探索版
- CVPのNP完全性について
- CVPとSVP（最短ベクトル問題）の関係について

CVPの3つの定式化

- CVP判定版
  - 整数格子 $\mathbf{B}$，目標ベクトル$\mathbf{t}$，有理数 r が与えられるとき, $\mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right) \le r$ or $\mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right) > r$ を決めよ.
- CVP最適版
  - 整数格子 $\mathbf{B}$ と目標ベクトル$\mathbf{t}$ が与えられるとき, $\mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right)$ を計算せよ.
- CVP探索版 ←本来の問題はこれ！
  - 整数格子 $\mathbf{B}$ と目標ベクトル$\mathbf{t}$ が与えられるとき, $\|\mathbf{Bx}-\mathbf{t}\|$ が最小になる格子ベクトル $\mathbf{Bx}$ を見出せ.



3つの問題の難しさの比較

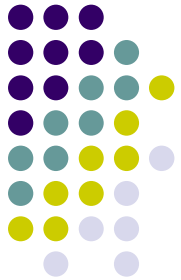


- 探索オラクルが与えられるとき，単に$\|\mathbf{Bx}-\mathbf{t}\|$を評価して$\mathbf{t}$の格子からの距離を計算できる
- 最適化オラクルが与えられるとき，$\mathrm{dist}(\mathbf{t}, L(\mathbf{B}))$と$r$を比較して，直ちに判定問題を解くことができる．

探索版が解ける　→　最適版が解ける　→　判定版が解ける
（この流れは自明）

- 以降，上記矢印の逆を多項式時間で示すことで，3つの問題が多項式同値であることを示す．
- これにより，CVPが難しい（NP困難）ことを示すためには，CVP判定版が難しいことを示すので十分となる．

「判定」対「探索」 ー 目的

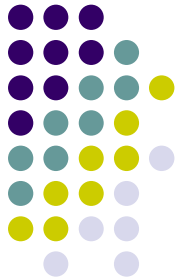


- CVP判定版を解くオラクルを多項式回呼び出すことで，CVP探索版を多項式時間で解くことができることを証明する.

言い換えると，

- $(\mathbf{B}, \mathbf{t}, r)$ を入力すると，$\mathrm{dist}(\mathbf{t}, L(\mathbf{B})) \leq r$ かどうかを答える判定オラクル A を利用できると仮定し，与えられた入力格子 $\mathbf{B}$ と目標ベクトル $\mathbf{t}$ に対してこのオラクルを使って，$\mathbf{t}$ にもっとも近い格子点 $\mathbf{Bx}$ を効率的に見出す方法を示す.

最近ベクトル Bx を見出すアイディア



最近ベクトル

$$\mathbf{Bx} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_{11} & \cdots & b_{n1} \\ \vdots & & \vdots \\ b_{1m} & \cdots & b_{nm} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_{11}x_1 + \cdots + b_{n1}x_n \\ \vdots \\ b_{1m}x_1 + \cdots + b_{nm}x_n \end{bmatrix}$$

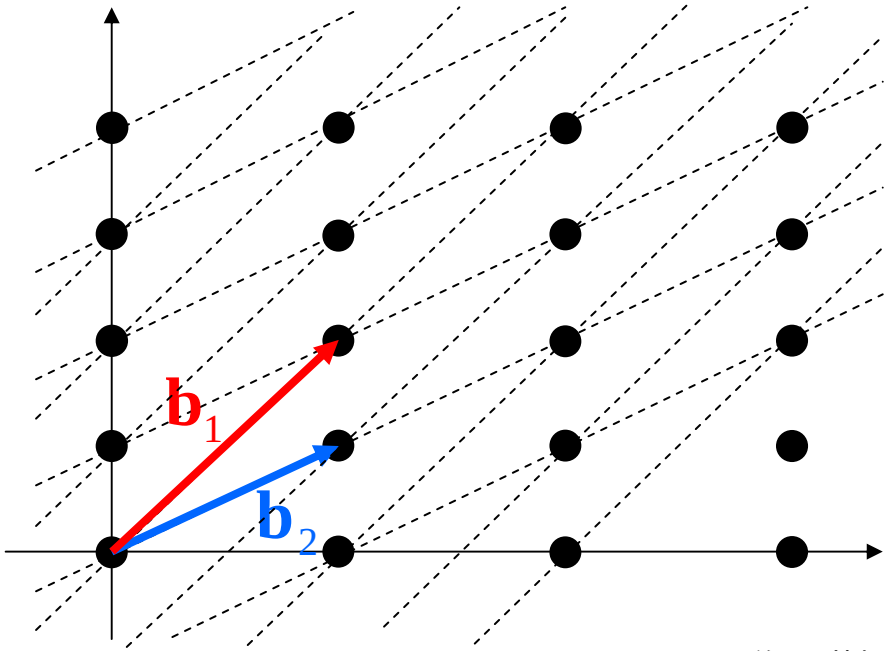
最近ベクトルを求めるメインのアイディアは，
最近ベクトルの $\mathbf{x}$ を x_1 の上位ビットから
1ビットずつ求めること．
（これが多項式時間で可能）

最近ベクトルを見出すための準備(1/3)

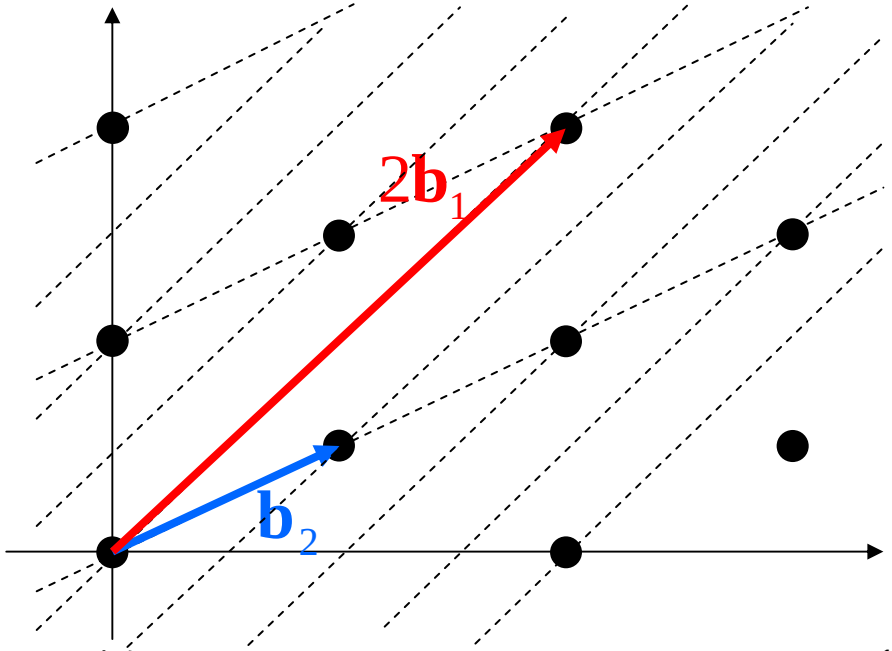
元の格子 $L(\mathbf{B})$ とその部分格子 $L(\mathbf{B}')$ を用意し，
それぞれの格子から目標ベクトルまでの距離
を比較する

$$\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n], \ \mathbf{B}' = [2\mathbf{b}_1, \ldots, \mathbf{b}_n]$$

$\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2]$ の例



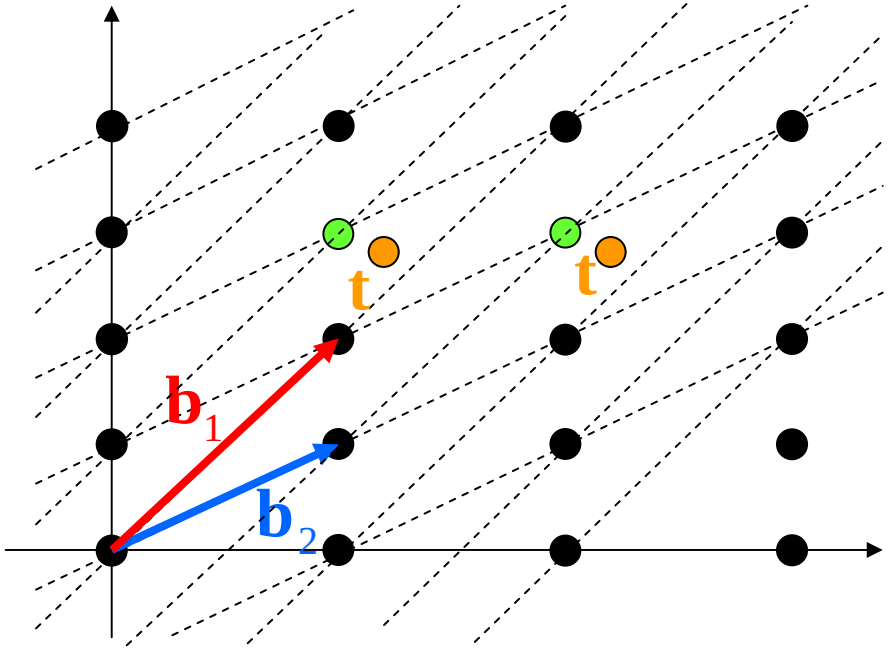
$\mathbf{B}' = [2\mathbf{b}_1, \mathbf{b}_2]$ の例



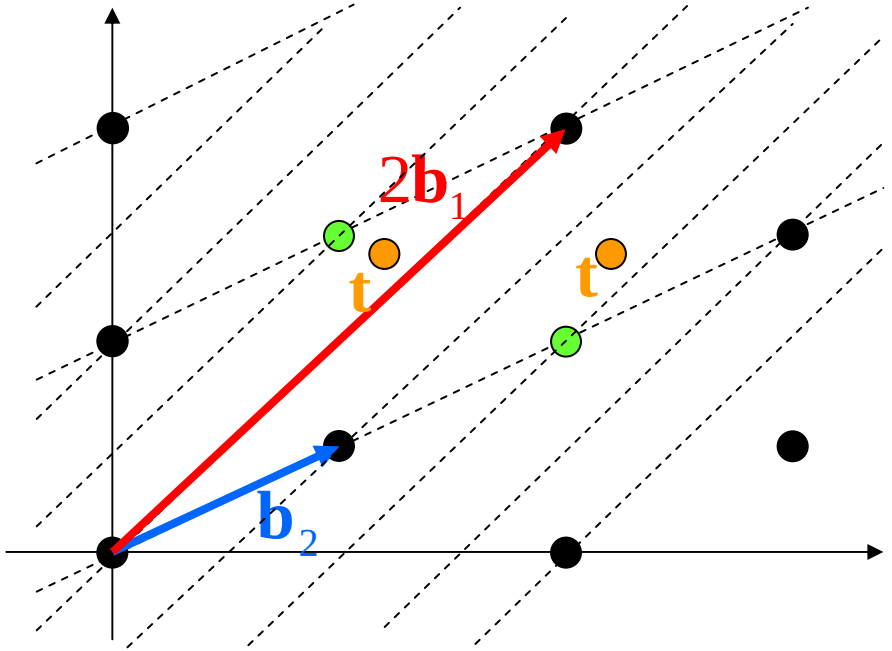
最近ベクトルを見出すための準備(2/3)

$$\mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right) \leq \mathrm{dist}\left(\mathbf{t}, L(\mathbf{B}')\right)$$

$\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2]$ の例



$\mathbf{B}' = [2\mathbf{b}_1, \mathbf{b}_2]$ の例



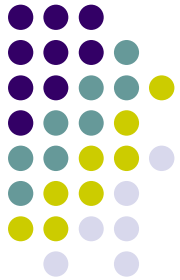
最近ベクトルを見出すための準備(3/3)

格子間距離の最大値(上界)を導出する.
格子間距離が最大になるのは, 各基底が直交しているとき. すなわち, 格子間距離の平方の上界 R は以下になる.

$$R = \sum_i \| \mathbf{b}_i \|^2$$

なぜ格子間距離の上界を考えるか？
最近ベクトルの位置を探索するのに2分探索を行うが, その範囲を求めるため.
この場合, [0,R]の範囲で2分探索を行う.

最近ベクトルを見出す(1/4)

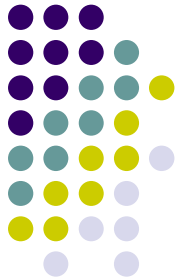


- $r < \mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right)^2 \le r+1$ のような整数 r を見出すまで [0,R] の範囲で2分探索を実行する
- $\left(\mathbf{B}', \mathbf{t}, \sqrt{r+1}\right)$ が入力されると，判定オラクルAを呼び出す．
  - NOを返した場合：
    $$\mathrm{dist}\left(\mathbf{t}, L(\mathbf{B}')\right) > \sqrt{\mathrm{r}+1} \ge \mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right)$$
  - YESを返した場合：
    $$\sqrt{\mathrm{r}} < \mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right) \le \mathrm{dist}\left(\mathbf{t}, L(\mathbf{B}')\right) \le \sqrt{\mathrm{r}+1}$$
    $$\Rightarrow \mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right) = \mathrm{dist}\left(\mathbf{t}, L(\mathbf{B}')\right)$$

$\left(\mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right)^2 \text{も} \mathrm{dist}\left(\mathbf{t}, L(\mathbf{B}')\right)^2 \text{も整数}\right)$

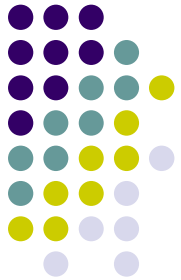
判定オラクルA：
$(\mathbf{B}, \mathbf{t}, r)$ を入力すると，$\mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right) \le r$ かどうかを答える

最近ベクトルを見出す(2/4)



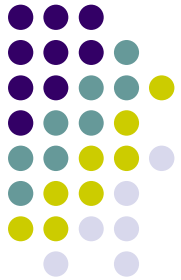
- ある最近ベクトル $\mathbf{Bx}$ に対して x_1 が偶数なら,
$$\mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right) = \mathrm{dist}\left(\mathbf{t}, L(\mathbf{B}')\right)$$
- ある最近ベクトル $\mathbf{Bx}$ に対して x_1 が奇数なら,
$$\mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right) < \mathrm{dist}\left(\mathbf{t}, L(\mathbf{B}')\right)$$
- これは, $\mathrm{dist}\left(\mathbf{t}, L(\mathbf{B})\right)$ と $\mathrm{dist}\left(\mathbf{t}, L(\mathbf{B}')\right)$ を比較すれば, ある最近ベクトル $\mathbf{Bx}$ に対して x_1 の偶数・奇数を決めることができることを意味する
- 以下の処理をして, 次の2分木探索を実行する
  - x_1 が偶数のときは目標ベクトルはそのまま
  - x_1 が奇数のときは目標ベクトルを $\mathbf{b}_1$ 分だけ移動
$$\mathbf{t}' = \mathbf{t} - \mathbf{b}_1$$

最近ベクトルを見出す(3/4)



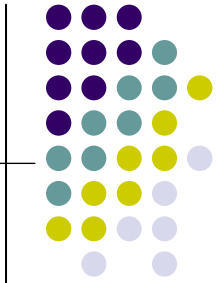
- 最初は，2分木探索を実行していくことで，上位ビットから順番に最初の係数 x_1 を完全に復元する.（多項式回数の反復）
- 次に，入力例題を少し修正する.
  - 格子: $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \rightarrow \mathbf{B} = [\mathbf{b}_2, \ldots, \mathbf{b}_n]$
  - 目標ベクトル: $\mathbf{t} \rightarrow \mathbf{t} - x_1 \mathbf{b}_1$
- これを繰り返して階数を減らし，x_1 から x_n まで順番に復元していく.
- 最終的に，得られた格子ベクトル $\mathbf{Bx} = \sum_{i=1}^{n} x_i \mathbf{b}_i$ はCVP問題 $(\mathbf{B}, \mathbf{t})$ への解である.

最近ベクトルを見出す(4/4)



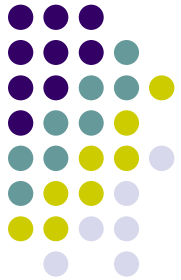
- 以上により，(厳密な)CVP判定版，CVP最適化版およびCVP探索版は多項式同値であり，判定版CVPはすでにこの問題の困難性を捉えていることを示している.
- これ以降，CVP判定版に集中する.
- 次は，CVP判定版がNP完全であることを示す.

アジェンダ



- 最近ベクトル問題（CVP）とは？
- 3つの版のCVPの難しさについて
  - CVP判定版，CVP最適化版，CVP探索版
- CVPのNP完全性について
- CVPとSVP（最短ベクトル問題）の関係について

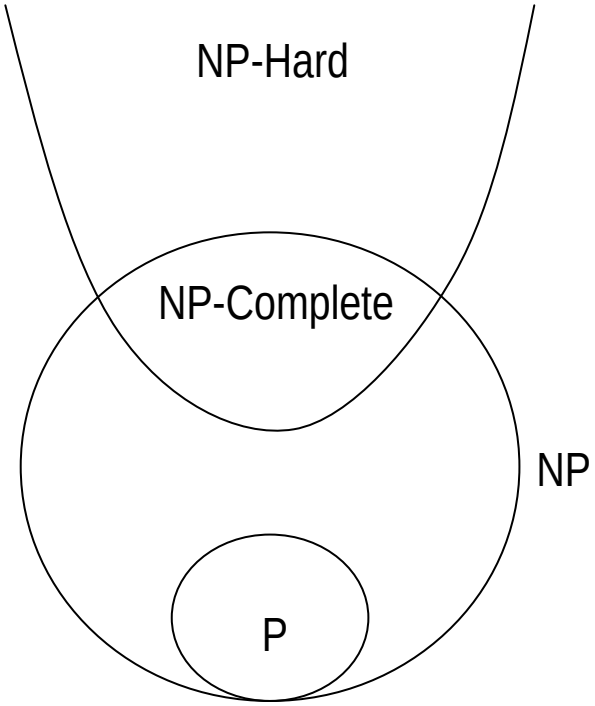
クラスPとクラスNPについて



- 判定問題（yes/noで答えられる問題）のクラス
- クラスP（Polynomial）
  - 決定性チューリングマシンによって多項式で解くことができる問題の集合.
  - 決められた手順通りに処理を進めれば解ける問題の集合.
- クラスNP（Non-deterministic Polynomial）
  - 非決定性チューリングマシンによって多項式解くことができる問題の集合.
  - 処理の手順に膨大な選択肢があり，その中から1つの手順を選んで，運が良ければ解けるというような問題の集合.

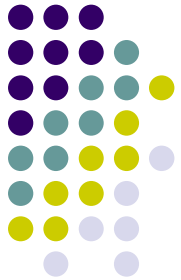
NP困難（NP-Hard）とNP完全（NP-Complete）

- NP困難
  - NPに属する最も難しい問題と比べて，少なくとも同等以上に難しい問題のクラス
- NP完全
  - NPに属する問題のうちでNP困難なクラス．
  - クラスNPに属する問題で，かつクラスNPのすべての問題から多項式時間帰着可能な問題



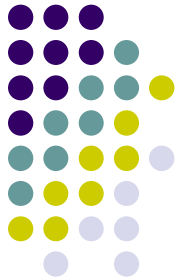
NP≠P の場合

CVPのNP完全性



- CVP判定版がNP完全であることを示す.
- 定理3.1
  - 任意の$p \geq 1$ ($p = \infty$も含む) に対して，ℓ_pノルムでの GAPCVP_1（すなわちCVPを厳密に解くことに付随する判定問題）はNP完全である.
- 証明手順
  - ① GAPCVP_1 がNPに属することを示す.
  - ② GAPCVP_1 がNP困難であることを示す.
  - ①②より，NP完全であることを示す.

復習：ℓ_pノルムとは何か？

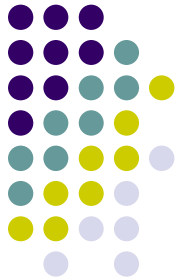


- p次平均ノルム，またはp-ノルムと呼ばれる
- 任意の $p \geq 1$ に対し，ベクトル $\mathbf{x} \in R^n$ の ℓ_p ノルム：

$$\| \mathbf{x} \|_p = \left(\sum_{i=1}^{n} | x_i |^p \right)^{\frac{1}{p}}$$

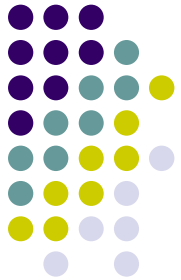
- p=2のときはユークリッドノルム
- p=∞のときは最大ノルム

復習：GAPCVP_γとは何か？



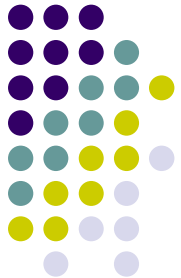
- 判定問題のCVPを一般化した約定問題
  - 約定問題は判定問題の一般化
  - 判定問題がCVP，約定問題がGAPCVP_γ
  - γ はギャップ関数
- 定義1.6　約定問題 GAPCVP_γ は，γ を階数の関数として次のように定義される：
  - YES例題は，ある $\mathbf{z} \in Z^m$ に対して $\| \mathbf{Bz} - \mathbf{t} \| \leq r$ のような $(\mathbf{B}, \mathbf{t}, r)$ である．
  - NO例題は，すべての $\mathbf{z} \in Z^m$ に対して $\| \mathbf{Bz} - \mathbf{t} \| > \gamma r$ のような $(\mathbf{B}, \mathbf{t}, r)$ である．
- 近似因子が $\gamma = 1$ に等しいとき，約定問題 GAPCVP_γ は厳密なCVPに付随する判定問題と同値である

① GAPCVP_1がNPに属することを示す



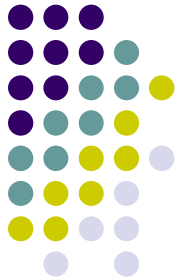
- $\mathrm{dist}(\mathbf{t}, L(\mathbf{B})) \le r$ であるすべての例題 $(\mathbf{B}, \mathbf{t}, r)$ に対し，$\mathrm{dist}(\mathbf{t}, L(\mathbf{B}))$ が高々 r であることを証明する短い証拠が存在することを示せばよい.
- 証拠は探索問題の解（$\| \mathbf{Bx} - \mathbf{t} \| \le r$ である格子点 $\mathbf{x}$ ）である.
- $\mathbf{x}$ の大きさは多項式である.
- 格子におけるベクトルの所属が多項式時間で決定できることから，証拠は多項式時間で検査することができる.

② $GAPCVP_1$がNP困難であることを示す（1/3）



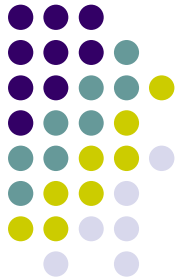
- 問題AがNP困難であることを示す標準的技法は，ある他のNP困難問題BをAに帰着することである．
- ここでは部分集合和問題からの帰着により証明する．
- 部分集合和問題はNP困難である
（NP完全であることも知られている）

部分集合和問題(SS)



- 定義3.1
  - 部分集合和問題(SS)とは次のようなものである．n+1個の整数 $(a_1,\ldots,a_n,s)$ が与えられるとき，足し合わせるとsになる a_i の部分集合を(もし存在すれば)見出せ．同じことであるが，$\sum_i a_i x_i = s$ である係数 $x_i \in \{0,1\}$ を見出せ．問題の判定版では $(a_1,\ldots,a_n,s)$ が与えられ，$\sum_i a_i x_i = s$ となる係数 $x_i \in \{0,1\}$ が存在するか，を決定しなければならない．
- SSの例
  - 問題：{2,4,6,8,10}の部分和で，和が19になるものは存在するか？
  - 答え：存在しない(偶数の和は偶数なので)

② GAPCVP_1がNP困難であることを示す(2/3)

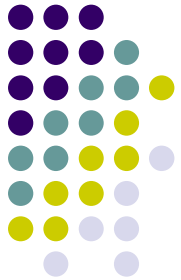


- 部分集合和例題 $(a_1,\ldots,a_n,s)$ が与えられるとき，各部分集合和係数 a_i に対し一つの列 b_i を持つ格子基底 **B** を定義する. **t** を和 s に付随させる.

$$\mathbf{B}=[\mathbf{b}_1,\ldots,\mathbf{b}_n]=\begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ 2 & 0 & \cdots & 0 \\ 0 & 2 & & \\ \vdots & & \ddots & \\ 0 & & & 2 \end{bmatrix}=\begin{bmatrix} \mathbf{a} \\ 2\mathbf{I}_n \end{bmatrix} \qquad \mathbf{t}=\begin{bmatrix} s \\ 1 \\ \vdots \\ 1 \end{bmatrix}\Big\}n$$

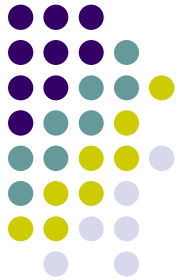
- 帰着の出力 $\left(\mathbf{B},\mathbf{t},\sqrt[p]{n}\right)$

② GAPCVP_1がNP困難であることを示す(3/3)



- 帰着が正しいことを証明する，すなわち以下の2つを証明する.
- (a) $(\mathbf{a}, s)$ が YES SS 例題
  → $\left(\mathbf{B}, \mathbf{t}, \sqrt[p]{n}\right)$ は YES CVP 例題
- (b) $(\mathbf{a}, s)$ が NO SS 例題
  → $\left(\mathbf{B}, \mathbf{t}, \sqrt[p]{n}\right)$ は NO CVP 例題

$(\mathbf{a}, s)$ が YES SS 例題 → $(\mathbf{B}, \mathbf{t}, \sqrt[p]{n})$は YES CVP 例題



- 部分集合和問題の解が存在すること，すなわち $\sum_{i=1}^{n} x_i a_i = s$ であるような $x_i \in \{0,1\}$ が存在することを仮定する.
- 距離ベクトル:

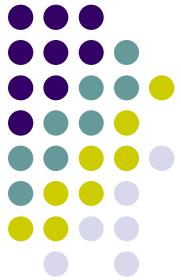
$$\mathbf{Bx} - \mathbf{t} = \begin{bmatrix} \sum_i a_i x_i - s \\ 2x_1 - 1 \\ \vdots \\ 2x_n - 1 \end{bmatrix}$$

- ℓ_p 距離の p 乗べき:

$$\|\mathbf{Bx} - \mathbf{t}\|_p^p = \underbrace{\left|\sum_{i=1}^{n} a_i x_i - s\right|^p}_{=0} + \sum_{i=1}^{n} \underbrace{\left|2x_i - 1\right|^p}_{=\pm 1} = n$$

- これは $\mathbf{t}$ の $L(\mathbf{B})$からの距離が高々 $\sqrt[p]{n}$ であり，$(\mathbf{B}, \mathbf{t}, \sqrt[p]{n})$ はCVPのYES例題である.

$(\mathbf{a}, s)$ が NO SS 例題 → $(\mathbf{B}, \mathbf{t}, \sqrt[p]{n})$ は NO CVP 例題



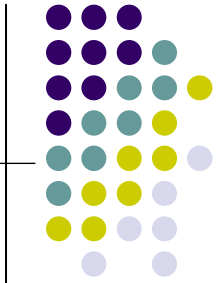
- 対偶をとって示す.
- $(\mathbf{B}, \mathbf{t}, \sqrt[p]{n})$ が YES CVP 例題であると仮定する
  - すなわち $\mathbf{y}$ の格子からの距離が高々 $\sqrt[p]{n}$ であると仮定し, $\mathbf{x}$ を $\|\mathbf{Bx}-\mathbf{y}\| \le \sqrt[p]{n}$ のような整数ベクトルとする.
- ℓ_p 距離の p 乗べき: $\|\mathbf{Bx}-\mathbf{t}\|_p^p = \left|\sum_{i=1}^{n} a_i x_i - s\right|^p + \sum_{i=1}^{n} |2x_i - 1|^p$
- すべての $2x_i - 1$ は奇数であるから以下を満たす

$$\sum_{i=1}^{n} |2x_i - 1|^p \ge n$$

- したがって, $\|\mathbf{Bx}-\mathbf{y}\| \le \sqrt[p]{n}$ が可能であるのは以下に限る $\sum_{i=1}^{n} a_i x_i - s = 0$ and $|2x_i - 1|^p = 1$ ←判定可能！
- 以下は部分集合和問題の解である

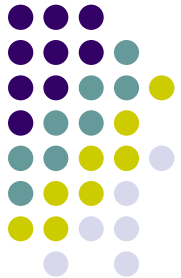
$$\sum_{i=1}^{n} a_i x_i = s \text{ and } x_i \in \{0,1\}$$

アジェンダ



- 最近ベクトル問題（CVP）とは？
- 3つの版のCVPの難しさについて
  - CVP判定版，CVP最適化版，CVP探索版
- CVPのNP完全性について
- CVPとSVP（最短ベクトル問題）の関係について

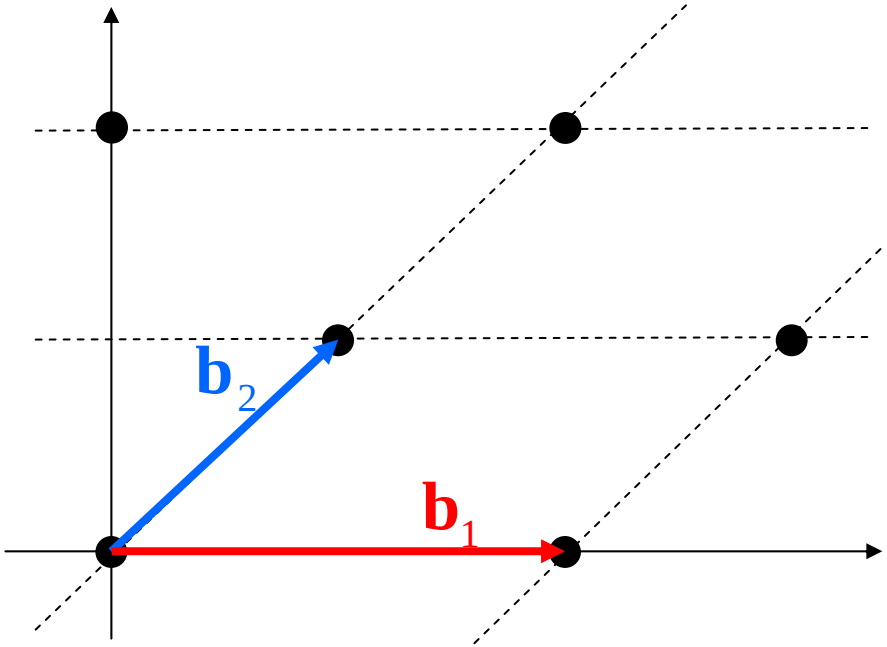
最短ベクトル問題とは？



- 多項式時間解法が知られていない問題
- SVP（Shortest Vector Problem）と表記する
- 定義1.1
  - 格子基底$\mathbf{B} \in Z^{m \times n}$ が与えられるとき，非零格子ベクトル$\mathbf{Bx}$ $(\mathbf{x} \in Z^n \setminus \{0\})$ で他のいかなる$\mathbf{y} \in Z^n \setminus \{0\}$に対しても$\| \mathbf{Bx} \| \leq \| \mathbf{By} \|$ であるものを見出せ.

最短ベクトルについて

m=2, n=2の場合の格子



$$\mathbf{b}_1 = \begin{bmatrix} 2 \\ 0 \end{bmatrix} \quad \mathbf{b}_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

- ℓ_1 ノルムでは, $\lambda_1 = \|\mathbf{b}_1\|_1 = \|\mathbf{b}_2\|_1 = 2$
- ℓ_2 ノルムでは, $\lambda_1 = \|\mathbf{b}_2\|_2 = \sqrt{2}$
- ℓ_∞ ノルムでは, $\lambda_1 = \|\mathbf{b}_2\|_\infty = 1$

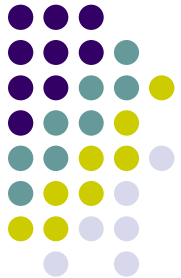
$$\|\mathbf{x}\|_\infty = \lim_{p\to\infty} \|\mathbf{x}\|_p = \max_{i=1}^{n} |x_i|$$

SVPのNP完全性について

- 定理3.2
  - GAPSVP_1（すなわちSVPを厳密に解くことに付随する判定問題）は，ℓ_∞ノルムでNP完全である．

- CVPのNP困難性を確立するのは易しい
- SVPがℓ_2 ノルムでNP困難であるかは，ほぼ20年間未解決問題であった．
- SVPのNP困難性は，1996年にAjtaiによってランダム帰着に対してのみ解決された
- 以降，SVPのCVPへの帰着について議論する

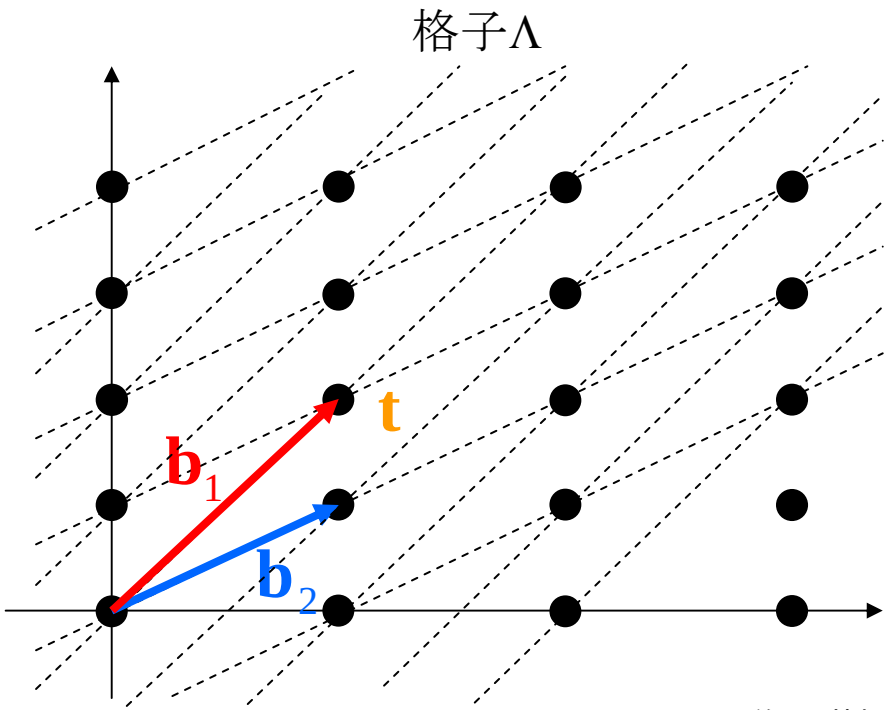
SVPとCVPの違いについて

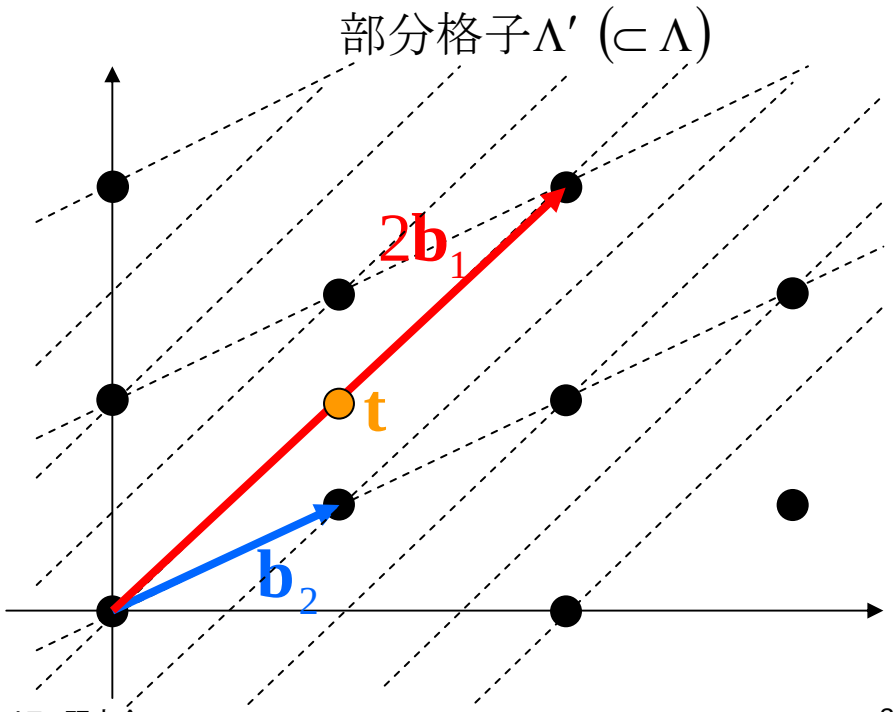


- SVP
  - 全零ベクトルに近い格子点を求める
  - 全零解を許さない
- CVP
  - 任意の目標ベクトルに近い格子点を求める
  - 許容解として目標ベクトルを受け入れる
- したがって，2つの問題の関連は自明ではない．
- SVPからCVPへの明らかな帰着は，CVPオラクルが常に全零ベクトルを返すので機能しない

CVPオラクルが全零ベクトルを返すことを避けるアイディア

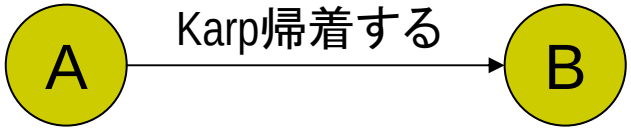
- 全零ベクトルに近い格子点を探す代わりに，ある他のベクトル $\mathbf{t} \in \Lambda \ (\text{e.g.}, \mathbf{t} = \mathbf{b}_1)$ に近い格子点を探す
- $\mathbf{t}$ が解として解されるのを避けるため，$\mathbf{t}$ を含まない部分格子 Λ' に対しCVPオラクルを実行
- 部分格子の選び方がポイント



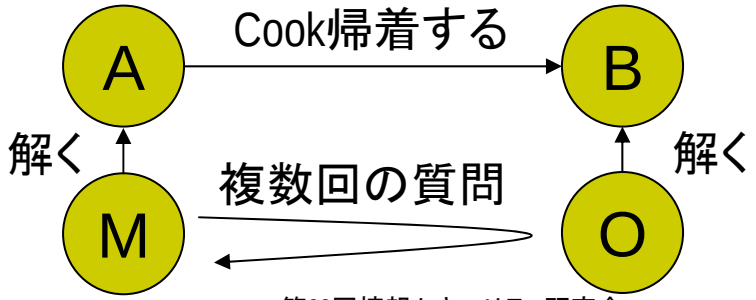


準備：帰着について

- AからBへ（Karp）帰着するとは
  - Bが多項式時間で解けるなら，Aもまた多項式時間で解くことができる（単一の例題に帰着）



- AからBへCook帰着するとは
  - 問題Bを正しく解くオラクルOが与えられるとき，Oを利用できる多項式チューリング機械Mが正しく問題Aを解くならば，MはAをBに帰着する．



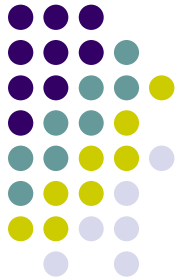
決定性帰着

- SVPをCVPのn個の例題の解に帰着させる（Cook帰着）
- 決定性帰着の概要
  - 基底 $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ が与えられるとき，CVPのn個の例題を次のように構成する．j番目の例題は次の基底

$$\mathbf{B}^{(j)} \stackrel{\text{def}}{=} [\mathbf{b}_1, \ldots, \mathbf{b}_{j-1}, 2\mathbf{b}_j, \mathbf{b}_{j+1}, \ldots, \mathbf{b}_n]$$

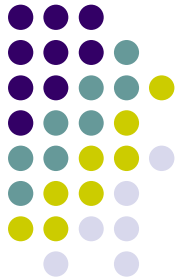
    と目標ベクトル $\mathbf{b}_j$ からなる．
  - CVP_γ オラクルへのn個の対応する質問において，これらn個のCVP例題を使って出力する

決定性帰着に関する3つの命題



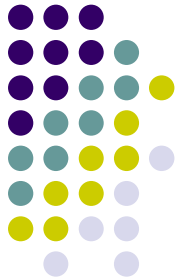
- 命題3.3
  - $\mathbf{v} = \sum_{i=1}^{n} c_i \mathbf{b}_i$ を $\Lambda = L(\mathbf{B})$ の最短非零ベクトルとする．このとき，c_i が奇数であるような i が存在する．
- 命題3.4
  - $\mathbf{v} = \sum_{i=1}^{n} c_i \mathbf{b}_i$ を c_j が奇数である$L(\mathbf{B})$ の格子ベクトルとする．このとき $\mathbf{u} = \frac{c_j + 1}{2}(2\mathbf{b}_j) + \sum_{i \neq j} c_i \mathbf{b}_i$ は $L(\mathbf{B}^{(j)})$ の格子ベクトルで，目標 $\mathbf{b}_j$ から $\mathbf{u}$ までの距離は $\mathbf{v}$ の長さに等しい
- 命題3.5
  - $\mathbf{u} = c'_j(2\mathbf{b}_j) + \sum_{i \neq j} c_i \mathbf{b}_i$ を $L(\mathbf{B}^{(j)})$ のベクトルとする．このとき $\mathbf{v} = (2c'_j - 1)\mathbf{b}_j + \sum_{i \neq j} c_i \mathbf{b}_i$ は $L(\mathbf{B})$ の非零格子ベクトルであり，$\mathbf{v}$ の長さは目標 $\mathbf{b}_j$ から $\mathbf{u}$ までの距離に等しい

決定性帰着による証明(1/3)



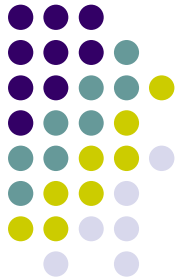
- 定理3.6
  - すべての関数$\gamma : N \mapsto \{r \in R : r \geq 1\}$に対して, SVP_γ $\left(\text{or } \mathrm{GAPSVP}_\gamma\right)$ はCVP_γ $\left(\text{or } \mathrm{GAPCVP}_\gamma\right)$ にCook帰着可能である. さらに, 帰着は非適応型であり, すべての質問は入力例題の階数を保つ.
- 証明の方針
  - 判定版(あるいは約定版)について, (a),(b)を示す
  - $(\mathbf{B}, r)$ をGAPSVP_γ 例題とする
  - $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$ をGAPCVP_γ 例題とする
  - (a) $(\mathbf{B}, r)$ がYES例題
    → $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$ があるjに対してYES例題
  - (b) $(\mathbf{B}, r)$ がNO例題
    → $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$ がすべてのjに対してNO例題

決定性帰着による証明(2/3)



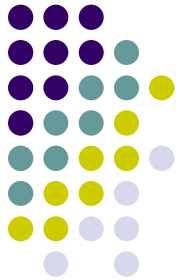
- (a) $(\mathbf{B}, r)$ がYES例題 → $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$ がYES例題
  - $(\mathbf{B}, r)$ をYES例題と仮定し, $\mathbf{v} = \sum_{i=1}^{n} c_i \mathbf{b}_i$ を $L(\mathbf{B})$ の最短非零格子ベクトルとする.
  - $\|\mathbf{v}\| \le r$ であり, 命題3.3より, あるjについて c_j は奇数であることを知っている.
  - ベクトル$\mathbf{u}$(命題3.4で定義)は $L(\mathbf{B}^{(j)})$ に属し, $\|\mathbf{u} - \mathbf{b}_j\| = \|\mathbf{v}\| \le r$ を満たす.
  - これにより, $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$ がYES例題であることがいえる.

決定性帰着による証明(3/3)



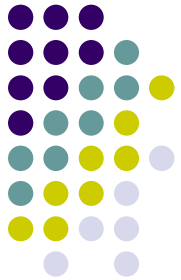
- (b) $(\mathbf{B}, r)$ がNO例題 → $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$ がNO例題
  - 対偶をとって示す
  - $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$ があるjに対してNO例題でない，すなわち $\|\mathbf{u}-\mathbf{b}_j\| \le \gamma(n)\cdot r$ である $L(\mathbf{B}^{(j)})$ のベクトル $\mathbf{u}$ が存在すると仮定する.
  - ベクトル $\mathbf{v}$（命題3.5で定義）は $L(\mathbf{B})$ の非零格子ベクトルであり，$\|\mathbf{v}\| = \|\mathbf{u}-\mathbf{b}_j\| \le \gamma(n)\cdot r$ を満たす.
  - これにより，$(\mathbf{B}, r)$ がNO例題でないことがいえる.

ランダム帰着に向けて



- 決定性帰着では，任意の GAPSVP_γ 例題は，GAPCVP_γ のn個の例題を解くことに，決定的に帰着できる（Cook帰着）ことを示した
- 次は，GAPSVP問題を GAPCVP の単一の例題に帰着することが可能かどうか，すなわち，2つの問題の間にKarp帰着が存在するかどうかにチャレンジする.
- より具体的には，写像関数 $f:\mathrm{GAPSVP}_\gamma \to \mathrm{GAPCVP}_\gamma$ が，確率アルゴリズムによって多項式時間で計算可能であることを許してKarp帰着を一般化する（→ランダム帰着）.

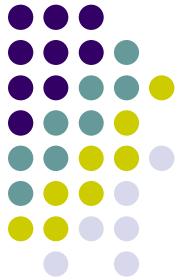
ランダム帰着



- YES例題あるいはNO例題のどちらかは，常に正しく写像される確率帰着である

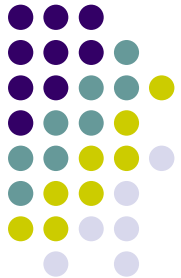
- 不誠実ランダム帰着
  （Unfaithful random reduction: UR帰着）
  - YES例題を常にYES例題に，NO例題を確率 p でNO例題に写像する帰着である．1－p を健全性誤差と呼ぶ．
- 逆不誠実ランダム帰着（RUR帰着）
  - YES例題を確率 p でYES例題に，NO例題を常にNO例題に写像する帰着である．1－p を完全性誤差と呼ぶ．

ランダム帰着による証明



- 定理3.7
  - すべての関数$\gamma : N \mapsto \{r \in R : r \geq 1\}$に対して，上から1/2で抑えられる完全性誤差を有する，SVP_γ $(\text{or } \mathrm{GAPSVP}_\gamma)$ から CVP_γ $(\text{or } \mathrm{GAPCVP}_\gamma)$ へのRUR帰着がある．さらに，作られたCVP例題はもとのSVP例題と同じ次元と階数を持つ．
- （証明略）

CVPの近似不可能性



- たとえ最適から小さな因子内での解を許したとしても，CVPはなおNP困難であることが示されている．
  - 任意のℓ_pノルムに対して，CVPをある対数多項式因子$\mathrm{O}\left(\log^{1/p} n\right)$内で近似することはNP困難である．
  - さらに，任意の対数多項式因子 $\mathrm{O}\left(\log^{c} n\right)$ に対し，ℓ_p ノルムでCVPがNP困難である．

ご清聴ありがとうございました.