最近ベクトル問題の**NP**困難性

後藤 達哉
筑波大学理工学群数学類 3 年

2019/3/3

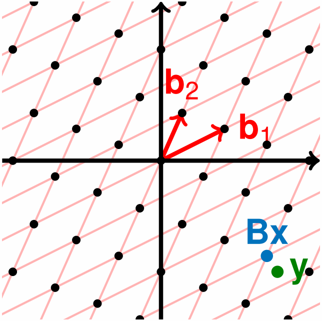
1. 最近ベクトル問題 (CVP)
2. P 問題と NP 問題
3. 部分和問題 (SS)
4. CVP が NP 困難なことの証明

1. 最近ベクトル問題 (CVP)
2. P 問題と NP 問題
3. 部分和問題 (SS)
4. CVP が NP 困難なことの証明

最近ベクトル問題 (CVP) とは？

最近ベクトル問題 (Closest Vector Problem; CVP) とは以下の問題である

- 入力: $\mathbb{R}$ 上線形独立なベクトル $\mathbf{b}_1, \ldots, \mathbf{b}_m \in \mathbb{Q}^n$ と $\mathbf{y} \in \mathbb{Q}^n$
- 出力: $||\mathbf{Bx} - \mathbf{y}||$ を最小にする $\mathbf{x} \in \mathbb{Z}^m$ (ただし $\mathbf{B} = (\mathbf{b}_1 \ldots \mathbf{b}_m)$)



CVP の応用例

- いわば暗号攻撃に応用がある
- 線形合同法

$$x_{n+1} = (ax_n + b) \bmod m$$

において $[0, c)$ の範囲の疑似乱数の列 $\lfloor cx_n/m \rfloor$ が外部から観測できるとする。このとき種 x_0 を復元したいなど

CVPのNP困難性

- CVPはNP困難である

1. 最近ベクトル問題 (CVP)
2. P 問題と NP 問題
3. 部分和問題 (SS)
4. CVP が NP 困難なことの証明

P問題

- 計算問題が **P問題** であるとは、(通常の計算機で)それを解くアルゴリズムであってその実行時間が入力サイズの多項式で抑えられるものが存在するときをいう

NP 問題

- **NP 問題**とは計算問題であって
  “非決定性チューリング機械”において実行時間が
  入力サイズの多項式で抑えられるアルゴリズムが
  存在するものを言う

NP 問題 (別の定義)

- 集合 X の元が入力されたら Yes、そうでなければ No を答えなければいけない計算問題 (集合 X によって規定される決定問題) を考える。
- この問題が **NP 問題**であるとは、多項式 q と多項式時間アルゴリズム R があって

$$x \in X \iff (\exists w)(|w| \leq q(|x|) \wedge R(x, w) = 1)$$

となること
- 大ざっぱに言えば、解の候補が与えられてそれが本当に解か確かめる多項式時間のアルゴリズムが存在することが条件

NP 問題 (例)

- 自然数が与えられたとき合成数か判定する問題 (X = 合成数の全体)
- $R(x, w) =$ (w が x の真の約数なら 1、そうでなければ 0), $q(n) = n$ とおけば NP 問題の条件

$$x \in X \iff (\exists w)(|w| \leq q(|x|) \wedge R(x, w) = 1)$$

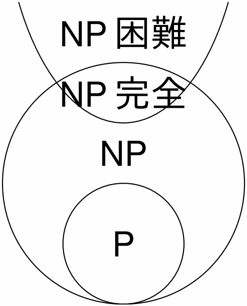
をみたす。
- よって合成数判定問題は NP 問題

多項式時間還元

- 決定問題 Y が定数時間で解ける機械があるような仮想的な世界において、それを (好きな回数だけ) 呼び出すことで決定問題 X が多項式時間で解けるとき、X は Y に多項式時間還元可能といい、$X \leq_p Y$ と書く

NP困難とNP完全

- 問題 X について、どんなNP問題も X に多項式時間還元できるとき X は **NP困難**な問題という
- NP困難かつNPな問題を **NP完全**な問題という



- 注: $\mathrm{P} \subseteq \mathrm{NP}$ は証明されているが、$\mathrm{P} \neq \mathrm{NP}$ かどうかは未解決問題。

1. 最近ベクトル問題 (CVP)
2. P 問題と NP 問題
3. 部分和問題 (SS)
4. CVP が NP 困難なことの証明

部分和問題

次の問題を部分和問題 (Subset Sum; SS) という

- 入力: 任意有限個の自然数 $a_1, \ldots, a_n$ と自然数 s
- 出力: $I \subseteq \{1, \ldots, n\}$ があって $\sum_{i \in I} a_i = s$ とできるか？

部分和問題

部分和問題については次が知られている:

- 部分和問題は NP 完全である

1. 最近ベクトル問題 (CVP)
2. P 問題と NP 問題
3. 部分和問題 (SS)
4. CVP が NP 困難なことの証明

CVP の NP 困難性

- SS が CVP に多項式時間還元できることを示せばよい

CVP の NP 困難性

SS のインスタンス $(a_1, \ldots, a_n, s)$ に対して CVP のインスタンス $\mathbf{B}, \mathbf{y}$ を決めて

$$\begin{aligned} &\text{SS のインスタンス } (a_1, \ldots, a_n, s) \text{ に解がある} \\ &\quad \iff \text{CVP のインスタンス } \mathbf{B}, \mathbf{y} \text{ に対して} \\ &\quad\ \sqrt{n} \text{ 以下の解がある} \end{aligned}$$

を示す。

CVP の NP 困難性

具体的には $(a_1, \dots, a_n, s)$ に対し $\mathbf{B}, \mathbf{y}$ を次で定める:

$$\mathbf{B} = \begin{pmatrix} \mathbf{a}^{\mathrm{T}} \\ \hline 2\mathbf{I}_n \end{pmatrix} \in M(\mathbb{Z}, (n+1) \times n)$$

$$(\text{where } \mathbf{a}^{\mathrm{T}} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix})$$

$$\mathbf{y} = \begin{pmatrix} s \\ 1 \\ \vdots \\ 1 \end{pmatrix} \in \mathbb{Z}^{n+1}$$

CVP の NP 困難性

仮に $(a_1, \dots, a_n, s)$ に解 $I \subseteq \{1, \dots, n\}$ があれば

$$x_i = \begin{cases} 1 & i \in I \\ 0 & \text{otherwise} \end{cases}$$

とおけば、$\sum_{i=1}^{n} x_i a_i = s$ なので

$$\|\mathbf{B}\mathbf{x} - \mathbf{y}\|^2 = \left\| \begin{pmatrix} \mathbf{a}^\mathrm{T} \\ \hline 2\mathbf{I}_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} - \begin{pmatrix} s \\ 1 \\ \vdots \\ 1 \end{pmatrix} \right\|^2$$

$$= \left| \sum_{i=1}^{n} x_i a_i - s \right|^2 + \sum_{i=1}^{n} |2x_i - 1|^2 = n$$

CVP の NP 困難性

また任意の $\mathbf{x} \in \mathbb{Z}^n$ に対し、

$$\|\mathbf{B}\mathbf{x} - \mathbf{y}\|^2 = \left| \sum_{i=1}^{n} x_i a_i - s \right|^2 + \sum_{i=1}^{n} |2x_i - 1|^2 \geq n$$

であり等号が成り立つのは $\sum_{i=1}^{n} x_i a_i = s$ かつ $x_i \in \{0, 1\}$ のとき。
よって $\|\mathbf{B}\mathbf{x} - \mathbf{y}\| \leq \sqrt{n}$ となる $\mathbf{x}$ があれば SS の解がある

以上より SS を CVP に多項式時間還元できた！ $\square$

まとめと補足1

- 最近ベクトル問題 (CVP) は NP 困難である。その証明は部分和問題 (SS) を還元することによる
- したがって、P=NP でない限り、CVP は効率的に解けそうにないということになる
- 今回はユークリッドノルムに関して CVP の NP 困難性を示したが、他の p 乗ノルムや max ノルムでも NP 困難なことが知られている
- なお厳密解でなく近似解を求めるなら多項式時間で解けるものもある

まとめと補足 2

- 行列 **B** があらかじめ分かっている場合、前処理をする (行列を扱いやすい形に変形しておくなど) ことによって入力 **y** に対して CVP を解く問題 (CVPP; CVP with preprocessing という) は効率的に解けるのではないか？ →これも不可能
- また、CVP が NP 困難だからといって最初に紹介した疑似乱数、線形合同法への効率的な攻撃ができないと分かったわけではない

参考文献

- D. Micciancio. The hardness of the closest vector problem with preprocessing. *IEEE Transactions on Information Theory*, 47(3):1212–1215, March 2001.
- 渡辺治. 今度こそわかる $P \neq NP$ 予想. 今度こそわかるシリーズ. 講談社, 2014.