部分和問題と格子簡約

大庭 翔介
北海道大学大学院 情報科学研究科 修士1年

背景

- **部分和問題**を解くのが困難であることを安全性の根拠にしている暗号を**ナップサック暗号**という
- 量子コンピュータでも効率的に解けるアルゴリズムが見つかっていないことから、耐量子暗号としても注目されている
- このタイプの暗号への攻撃として、**格子簡約**を利用した「低密度攻撃」が存在する

部分和問題

- $a_1, \dots, a_n, S \in \mathbb{N}$ が与えられたとき、

$$\sum_i a_i x_i = S$$

となる $x_i \in \{0,1\}$ を見つける問題

- **NP完全問題**である
- 与えられた部分和問題に対して、
  密度 $d = \frac{n}{\max(log\ a_i)}$ を定義
  一般に$d = 1$ のときが最も難しく、$d > 1$では多数の解が存在する

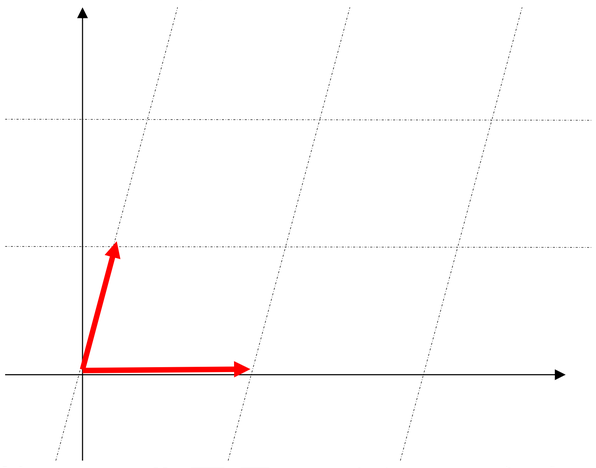
格子

- ベクトル $\mathrm{b}_1, \dots, b_n \in \mathbb{R}^n$ に対して、

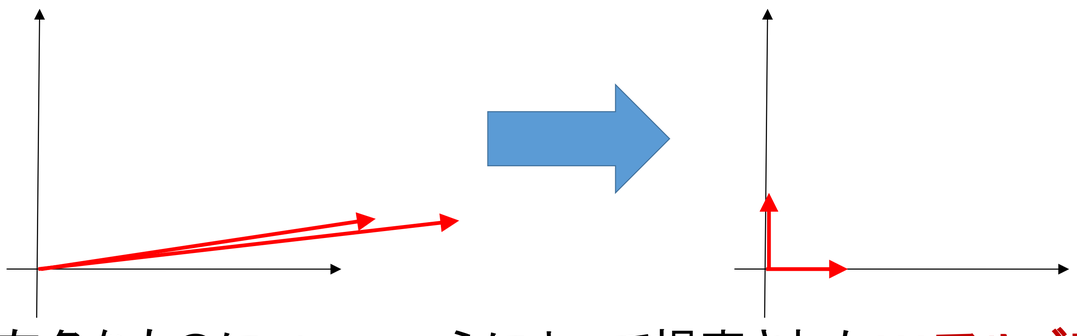
$$\mathrm{L}(b_1, \dots, b_n) = \{ \sum x_i b_i \mid x_i \in \mathbb{Z} \}$$

を**基底** $b_1, \dots, b_n$ によって構成される格子という

- 直感的には、グリッド線の交点の集合



- 与えられた格子の非零最小ベクトルを求める問題（**最小ベクトル問題：SVP**）は**NP困難**
- **格子簡約**：格子の基底を、同じ格子を構成する短い基底に変換すること



- 有名なものに、Lenstra らによって提案された**LLLアルゴリズム** [1]がある
- 最小のベクトルを求める代わりに、基底簡約によって小さいベクトルを求める

既存研究

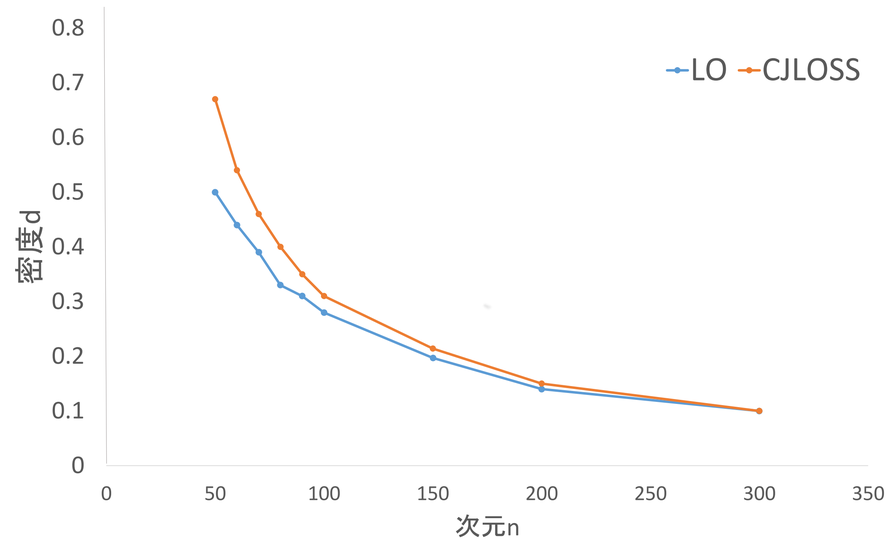
- Lagarias らによって、部分和問題を格子の最短ベクトル問題に帰着する方法 [2]が示された
- この方法によって、密度が $d < 0.6463$ である部分和問題は**格子オラクルを仮定すれば**効率よく解けることを示した
- 後に Coster らの改良[3]により、$d < 0.9408$ の場合にも適用できるようになる
- Coster らの方法では、Nを十分大きな数として、

$$b_1 = (2, 0, 0, \dots, 0, \mathrm{N}a_1)$$
$$b_2 = (0, 2, 0, \dots, 0, \mathrm{N}a_2)$$
$$\vdots$$
$$b_n = (0, 0, 0, \dots, 2, \mathrm{N}a_n)$$
$$b_{n+1} = (1, 1, 1, \dots, 1, \mathrm{N}S\ )$$

とすることで、このベクトルからなる格子の最小ベクトルが部分和問題の解を表すベクトルとなる

計算機実験

- Lagarias や Coster らが実験した部分和問題は次元があまり大きくない。高次元ではどうだろうか？
- まずランダムな部分和問題を生成
- Lagariasらの基底構成法、Costerらの基底構成法によって基底を構成し、LLLアルゴリズムで簡約化する
- 与えたすべての問題で解が求められる密度は次元nが大きくなるとnの逆数程度の速度で小さくなる



現在の研究(今後の課題)

- 理論的には格子オラクルが存在すれば解ける密度でも、簡約化を使用した方法では解けていない
- LLLアルゴリズムの他にも、いくつかの格子簡約アルゴリズムが提案されている
  それらを組み合わせて利用したり、部分的に変更することによって高次元での性能を上げられないか
- もしくは同程度の性能ならばより高速にできないか

参考文献

[1] A. K. Lenstra, H. W. jun. Lenstra, and Lovász Laszlo. Factoring polynomials with rational coefficients. Mathematische Annalen, 261(4):515-534, 1982
[2] J. C. Lagarias and A.M. Odlyzko. Solving low-density subset sum problems. Journal of the Association for Computing Machinery, 32(1):229-246, 1985.
[3] M. J. Coster, A. Joux, B. A. LaMacchia, A. M. Odlyzko, C. P. Schnorr, and J. Stern. Improved low-density subset sum algorithms. computational complexity, 2(2):111-128, 1992.