Vol.2015-CSEC-70 No.5
Vol.2015-SPT-14 No.5
2015/7/2

格子の最短ベクトル問題において格子基底の質が探索効率に及ぼす効果について

深瀬　道晴　山口　和紀[1]

概要：格子暗号の安全性と密接に関連する格子の最短ベクトル問題 (SVP) について、本研究では、最短ベクトル探索に用いる格子基底の質が探索効率に及ぼす効果について分析する。格子基底の質を測る指標としては、基底に対応するグラム・シュミット直交ベクトル列の二乗ノルムの和を用いる。探索効率を測る指標としては、探索空間の大きさと最短ベクトルを含む確率を用いる。最短ベクトルが分かっている格子について、その格子基底のグラム・シュミット直交ベクトル列の二乗ノルムの和と、論文 [3] の方法で定めた探索空間が最短ベクトルを含む確率を求めることで、それらの関係を実験的に明らかにする。

1. はじめに

格子の最短ベクトル問題 (SVP) は、格子暗号の安全性と密接に関連する計算困難問題である。ここで、格子とは、線形独立なベクトルの組の整数係数線形結合の全ての集合である。格子を生成する線形独立なベクトルの組を、基底という。最短ベクトル問題では、与えられた格子に対して、原点を除いて原点に最も近いベクトル、すなわち、最短ベクトルが解となる。

代表的な最短ベクトル問題のアルゴリズムは、LLL アルゴリズム [7] と BKZ アルゴリズム [10] である ([4])。これらのアルゴリズムでは、与えられた格子の基底からより短いベクトルを含む基底を求める基底簡約によって、最短ベクトル問題を近似的に解くことができる。BKZ アルゴリズムは LLL アルゴリズムを拡張したアルゴリズムであり、LLL アルゴリズムよりも長い計算時間を要するが、より精度の高い近似解を得ることができる。BKZ アルゴリズムをより効率化したアルゴリズムとして、RSR アルゴリズム [11] や BKZ 2.0[1] が提案されている。これらのアルゴリズムの性能を測る指標として、NTRU[6] などの格子暗号の解読問題や Darmstadt 工科大学の Lattice challenge[8] や SVP challenge[9] を用いることができる ([1])。

本研究では、論文 [3] における最短ベクトルの探索手法について、探索に用いる基底の質が探索効率に及ぼす効果について分析する。論文 [3] においては、基底に対応するグラム・シュミット直交ベクトル列の二乗ノルムの和 (GS 和) が小さい程、探索空間に短いベクトルが含まれる確率が大きくなることが理論的に示された。しかし、論文 [3] では、基底の GS 和の大小と短いベクトルを得るために必要となる探索空間の大きさとの関係について分析されなかった。また、論文 [3] では、最短ベクトルが分かっていない SVP Challenge の格子を対象としていたため、探索空間に最短ベクトルが含まれる確率に関する実験的分析が示されなかった。そこで、本研究では、最短ベクトルが分かっている格子を対象として、基底の GS 和の大小と短いベクトルを得るために必要となる探索空間の大きさとの関係、及び、基底の GS 和の大小と探索空間が最短ベクトルを含む確率との関係を実験的に明らかにする。

本研究では、探索効率を測る指標として、探索空間の大きさと最短ベクトルを含む確率を用いる。NTRU 格子を用いた実験の結果、GS 和の小さい基底を用いることで、短いベクトルを得るために必要となる探索空間の大きさを縮小できることが示された。例えば、GS 和が小さい基底では、GS 和が大きい基底よりも 1/1913 の大きさの探索空間において、より短いベクトルが得られた。また、GS 和の異なる基底を用いて、基底の GS 和が小さい程、探索空間に最短ベクトルが含まれる確率が大きくなることを実験的に確かめた。

本研究と関連する研究として、著者等は論文 [2] において、NTRU 格子の最短ベクトルが探索空間に含まれる確率を示した。論文 [2] では短いベクトルを得るのに適した探索空間の形を求めた。しかし、同一の形の探索空間を用いた場合でも基底に対応するグラム・シュミット直交ベクトル列の二乗ノルムの傾向の違いによって短いベクトルが求まる頻度に大きな差が生じることが確認されたため、グラム・シュミット直交ベクトル列の二乗ノルムの傾向を示す

[1] 東京大学
The Uniersity of Tokyo

ⓒ 2015 Information Processing Society of Japan

GS 和の指標を論文 [3] において導入した。本研究では、論文 [3] において分析されなかった基底の GS 和の大小と短いベクトルを得るために必要となる探索空間の大きさとの関係について実験をした。

2. 探索空間と基底の質

本節では、格子に関する基本概念を説明した後、グラム・シュミット係数の自然数表現の概念と自然数表現に基づく探索空間の定義 [3] について説明する。

2.1 格子

格子 $L \subset \mathbb{R}^m$ は，n 個の線形独立なベクトル列 $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{Z}^{m\times n}$ によって，$L(B) = \{B\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^n\}$ のように定義される。ここで、整数 n を，L の次元という。$n = m$ のとき，L は全次元であるという。ベクトル列 $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{Z}^{m\times n}$ を，L の基底という。$n \geq 2$ のとき，同一の格子を生成する基底は無数に存在する。以降では，全次元整数格子 $L \subset \mathbb{Z}^n$ のみを扱う。

L において $\mathbf{0}$ を除いて最も短いベクトルを、最短ベクトルという。最短ベクトルのノルムを、$\lambda_1(L)$ によって表す。ある格子の基底 B が与えられたとき，$L(B)$ の最短ベクトルを求める問題を最短ベクトル問題 *(SVP)* という。

2.2 格子ベクトルの自然数表現

基底 $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ に対して、グラム・シュミット直交ベクトル列を $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^* \in \mathbb{R}^n$ とする：$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^*$ with $\mu_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle / \langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle$. $\mathbf{x} \in \mathbb{Z}^n$ として、$\mathbf{v} = B\mathbf{x}$ を、基底 B によって生成される格子における格子ベクトルとする。ここで、$\mathbf{v}$ を、グラム・シュミット直交ベクトル列 $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ と B のグラム・シュミット直交化の係数 $\mu_{i,j}$ とを用いて、$\mathbf{v} = \sum_{j=1}^n \nu_j \mathbf{b}_j^*$ のように表せる。$\boldsymbol{\nu} \in \mathbb{R}^n$ は、それぞれの j について $\nu_j = \sum_{i=1}^n x_i \mu_{i,j}$ である。$\mathbf{b}_j^*$ は互いに直交するため、$\|\mathbf{v}\|^2 = \sum_{j=1}^n \nu_j^2 \|\mathbf{b}_j^*\|^2$ である。以下、ν_j を $\mathbf{v}$ のグラム・シュミット係数という。

$\mathbf{v}$ のグラム・シュミット係数 ν_j は、$\mathbf{v}$ とグラム・シュミット直交ベクトル列 $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ との間の直交性の度合いを表している。$\mathbf{v}$ は、$-0.5 < \nu_j \leq 0$ または $0 < \nu_j \leq 0.5$ のとき、$\mathbf{b}_j^*$ と最も直交に近い [*1]。ここで、ν_j について 0.5 刻みで離散化した指標として、以下のように格子ベクトルの自然数表現を定義する。

定義 1 格子ベクトル $\mathbf{v} = \sum_{j=1}^n \nu_j \mathbf{b}_j^* \in L(B)$ に対して、$\mathbf{v}$ の自然数表現は、$\mathbf{z}(\mathbf{v}) \in \mathbb{N}^n$ s.t. $-(z_j(\mathbf{v}) + 1)/2 < \nu_j \leq -z_j(\mathbf{v})/2$ または $z_j(\mathbf{v})/2 < \nu_j \leq (z_j(\mathbf{v}) + 1)/2$ である。

[*1] LLL アルゴリズムによる簡約基底は、直交に近い基底であり、全ての基底ベクトルの ν_j の絶対値は、一つの j を除いて 0.5 以下である。

2.3 自然数表現を用いた探索空間の定義

格子の基底を B、B のグラム・シュミット直交ベクトル列を $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$、$L(B)$ の任意の格子ベクトルを $\mathbf{v} = \sum_{j=1}^n \nu_j \mathbf{b}_j^*$、そして、$\mathbf{v}$ の自然数表現を $\mathbf{z}(\mathbf{v})$ とする。ある $c \in \mathbb{Z}_+$ について、$\mathbf{d} \in \mathbb{N}^c$ s.t. $d_c(\mathbf{v}) = \#\{z_j(\mathbf{v}) : z_j(\mathbf{v}) = c-1, 1 \leq j \leq n\}$、$\mathbf{w} \in \mathbb{N}^c$ s.t. $w_k(\mathbf{v}) = n - \min\{j : z_j(\mathbf{v}) = c-1\} + 1$、$\mathbf{s} \in \mathbb{N}^c$,$\mathbf{t} \in \mathbb{N}^c$ とする。例えば、$d_1(\mathbf{v})$ は、$\mathbf{v}$ のグラム・シュミット係数の自然数表現における 0 の個数を表す。ここで、集合 S に対して、$\#S$ は S の要素数を表す。このとき、探索空間 $V_B(\mathbf{s}, \mathbf{t})$ を以下のように定義する。

定義 2 $V_B(\mathbf{s}, \mathbf{t}) = \{\mathbf{v} \in L(B) : \mathbf{d}(\mathbf{v}) \leq \mathbf{s}, \mathbf{w}(\mathbf{v}) \leq \mathbf{t}\}$.

定義 2 において、ベクトルに関する不等号は、各成分が小さいことを表す。$V_B(\mathbf{s}, \mathbf{t})$ は、$\mathbf{s}$ によってグラム・シュミット係数の自然数表現における 0 や 1 等の個数を制限し、$\mathbf{t}$ によって 0 や 1 等が存在する範囲を規定している。$V_B(\mathbf{s}, \mathbf{t})$ の大きさ、すなわち、$\#V_B(\mathbf{s}, \mathbf{t})$ は、基底の選び方にはよらず、$\mathbf{s}$ と $\mathbf{t}$ のみによって決まることに注意されたい。

3. 探索効率の分析

本節では、基底の質が探索効率に及ぼす効果を分析する。格子基底の質を測る指標としては、基底に対応するグラム・シュミット直交ベクトル列の二乗ノルムの和、すなわち、$\sum_{j=1}^n \|\mathbf{b}_j^*\|^2$ を用いる。以降では、グラム・シュミット直交ベクトル列の二乗ノルムの和を、略して GS 和と呼ぶことにする。探索効率を測る指標としては、探索空間の大きさと最短ベクトルを含む確率を用いる。本節で示す実験においては、最短ベクトルが分かっている格子として NTRU 格子の 1 つのインスタンスを用い、NTRU の秘密鍵に相当するベクトルを最短ベクトルとみなす。NTRU の秘密鍵と NTRU 格子における最短ベクトルの関係については、論文 [6] を参照されたい。

本節で示す実験の目的と内容を、以下に示す：

3.1 節 まず、探索空間 $V_B(\mathbf{s}, \mathbf{t})$ のパラメータ $\mathbf{s}$ と $\mathbf{t}$ を変化させた場合において、探索で得られるベクトルのノルムの変化の仕方を調べるために、基底 B を固定して、探索空間 $V_B(\mathbf{s}, \mathbf{t})$ をいくつかの方法で変化させて、探索で得られるベクトルのノルムの最小値を計算する。

3.2 節 探索空間を変化させる効果と GS 和の違いによる効果とを比較するために、3.1 節と同様の実験を、GS 和の異なる別の基底 B' に対して行う。

3.4 節 探索空間が最短ベクトルを含む確率に対して GS 和の違いが及ぼす効果を調べるために、GS 和の異なる基底に対して、同一の探索空間 $V_B(\mathbf{s}, \mathbf{t})$ について、最短ベクトルが含まれる確率を計算する。

3.1 探索空間の変更による効果

ここでは、基底 B を固定して、探索空間を変化させる。以降では、格子の次元 n について $n = 214$ とする。この実験

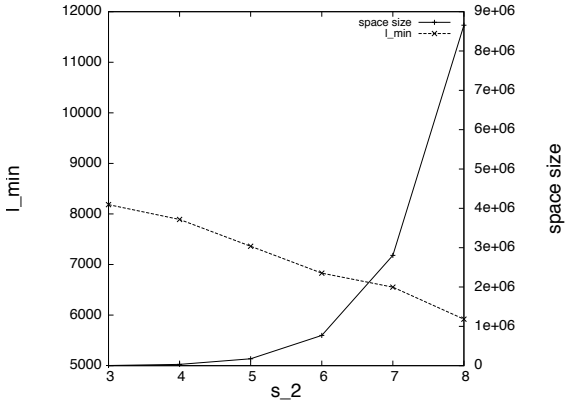

図 1　自然数表現として含む 1 の個数を変動させた場合における s_2(X 軸) と l_{min}(左側 Y 軸) 及び s_2(X 軸) と探索空間の大きさ (右側 Y 軸) の関係

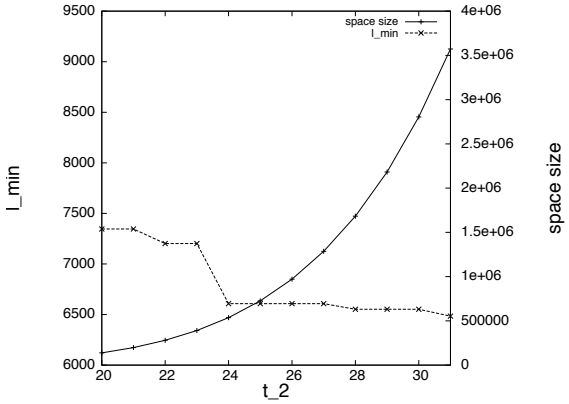

図 2　自然数表現として含む 1 の存在する範囲を変動させた場合における t_2(X 軸) と l_{min}(左側 Y 軸) 及び t_2(X 軸) と探索空間の大きさ (右側 Y 軸) の関係

では、探索空間に含まれる格子ベクトルを網羅列挙した際に得られる格子ベクトルの二乗ノルムの最小値 l_{min} を計算する。

自然数表現における 1 の個数を変更

ここでは、$\mathbf{t}$ を $(214, 30)$ に固定する。そして、$\mathbf{s}$ を $(214, 3)$ から $(214, 8)$ まで第二成分 s_2 を 1 刻みで変動させる。このときの l_{min} の変化を図 1 に示す。図 1 には、探索空間の大きさの変化も示されている。図 1 から、l_{min} は、探索空間が大きくなるにつれて小さくなる傾向が分かる。

自然数表現における 1 の存在する範囲を変更

ここでは、$\mathbf{s}$ を $(214, 7)$ に固定する。そして、$\mathbf{t}$ を $(214, 20)$ から $(214, 31)$ まで第二成分 t_2 を 1 刻みで変動させる。このときの l_{min} の変化を図 2 に示す。図 2 には、探索空間の大きさの変化も示されている。図 2 から、l_{min} は、探索空間が大きくなるにつれて小さくなる傾向はあるが、$t_2 = 24$ 以降はほとんど変化がないことが分かる。したがって、少なくとも実験で用いた t_2 の範囲では、探索空間を大きくする効果が小さいといえる。

探索空間の大きさを固定

ここでは、探索空間の大きさ $\#V_B(\mathbf{s}, \mathbf{t})$ を固定する。

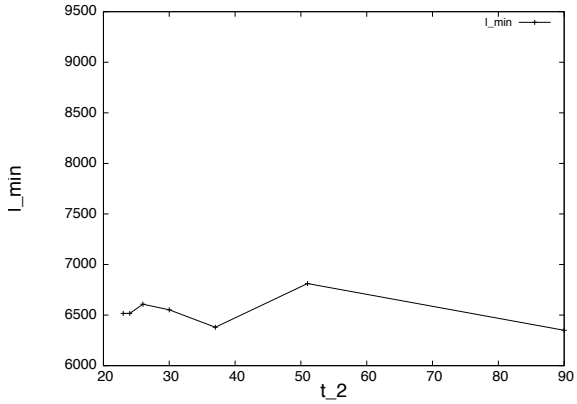

図 3　自然数表現として含む 1 の個数と存在する範囲を調整して探索空間の大きさを 2.5e + 06 に近い値に固定した場合における t_2(X 軸) と l_{min}(Y 軸) の関係

$\#V_B(\mathbf{s}, \mathbf{t})$ を完全に固定はできないので、ここでは、2.5e+06 程度になるように調整する。この実験では、自然数表現における 1 の存在する範囲を大きく変化させ、l_{min} の変化の仕方を調べる。そのため、$\mathbf{t}$ の第二成分 t_2 の値を 23 から 90 の範囲で変化させ、$\#V_B(\mathbf{s}, \mathbf{t})$ が 2.5e + 06 に近い値になるように $\mathbf{s}$ の第二成分 s_2 を調整する。このときの l_{min} の変化を、図 3 に示す。図 3 では、t_2 を横軸にとっている。図 3 から分かるように、l_{min} について、大きな変化や規則的な変化は見られなかった。

以上の実験によって、探索空間 $V_B(\mathbf{s}, \mathbf{t})$ のパラメータ $\mathbf{s}$ と $\mathbf{t}$ を変化させた場合において、探索で得られるベクトルのノルムの変化の仕方を確認した。

3.2　GS 和の違いによる効果

ここでは、3.2 節で用いた基底と異なる基底 B' を用いて、3.2 節と同様の実験をする。そして、3.2 節で用いた基底 B と基底 B' との間で結果を比較する。ここでの目的は、基底に関して、GS 和の違いが、探索で得られるベクトルのノルムに及ぼす効果を調べることである。そのため、GS 和の大きく異なる基底 B と基底 B' を用いる。3.2 節で用いた B の GS 和は、163604 である。ここでは、GS 和が 215188 の B' を新たに用いる。

自然数表現における 1 の個数を変更 (B と B' の比較)

ここでは、$\mathbf{t}$ を $(214, 30)$ に固定する。そして、$\mathbf{s}$ を $(214, 3)$ から $(214, 8)$ まで第二成分 s_2 を 1 刻みで変動させる。このときの l_{min} の変化を、B と B' のそれぞれについて、図 4 に示す。図 4 には、探索空間の大きさの変化も示されている。図 4 から、l_{min} は、B と B' のいずれの場合でも、探索空間が大きくなるにつれて小さくなる傾向が分かる。ここで、図 4 から、$s_2 = 3$ のとき $V_B(\mathbf{s}, \mathbf{t})$ において得られるベクトルのノルムの最小値は、$s_2 = 8$ のとき $V_{B'}(\mathbf{s}, \mathbf{t})$ において得られるベクトルのノルムの最小値より小さいことが分かる。$s_2 = 3$、$s_2 = 8$ のそれぞれの場合について、探索空間の大きさはそれぞれ 4525、8656936 であり、探索空

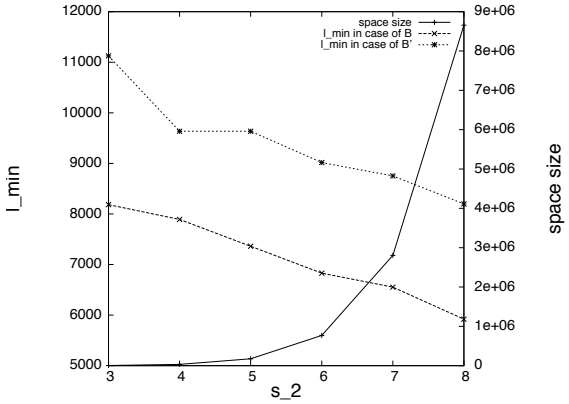

図 4　自然数表現として含む 1 の個数を変動させた場合 (B と B' の比較) における s_2(X 軸) と l_{min}(左側 Y 軸) 及び s_2(X 軸) と探索空間の大きさ (右側 Y 軸) の関係

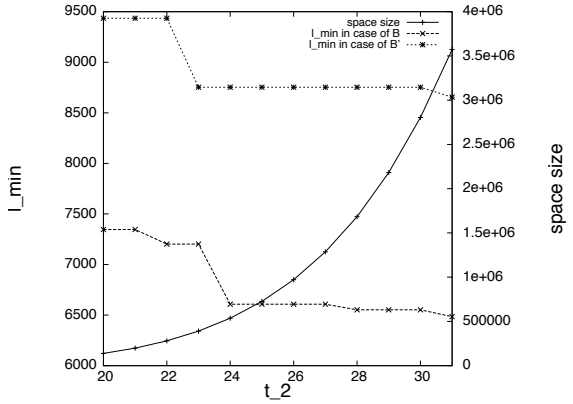

図 5　自然数表現として含む 1 の存在する範囲を変動させた場合 (B と B' の比較) における t_2(X 軸) と l_{min}(左側 Y 軸) 及び t_2(X 軸) と探索空間の大きさ (右側 Y 軸) の関係

間の大きさの比率は約 1/1913 である。このことは、GS 和の小さい B については、GS 和の大きい B' の場合に対して 1/1913 の大きさの探索空間において、より短いベクトルを得ることができることを示している。

自然数表現における 1 の存在する範囲を変更 (B と B' の比較)

ここでは、$\mathbf{s}$ を $(132, 7)$ に固定する。そして、$\mathbf{t}$ を $(132, 20)$ から $(132, 31)$ まで第二成分 t_2 を 1 刻みで変動させる。このときの l_{min} の変化を、B と B' のそれぞれについて、図 5 に示す。図 5 には、探索空間の大きさの変化も示されている。図 5 から、l_{min} は、B と B' のいずれの場合でも、探索空間が大きくなるにつれて小さくなる傾向はあるが、B の場合には $t_2 = 24$ 以降、B' の場合には $t_2 = 23$ 以降はほとんど変化がないことが分かる。ここで、図 5 から、$t_2 = 20$ のとき $V_B(\mathbf{s}, \mathbf{t})$ において得られるベクトルのノルムの最小値は、$t_2 = 31$ のとき $V_{B'}(\mathbf{s}, \mathbf{t})$ において得られるベクトルのノルムの最小値より小さいことが分かる。$t_2 = 20$、$t_2 = 31$ のそれぞれの場合について、探索空間の大きさはそれぞれ 137979、3572223 であり、探索空間の大きさの比率は約 1/25 である。このことは、GS 和の小さい B については、GS 和の大きい B' の場合に対して 1/25 の大きさの探索空間において、より短いベクトルを得ることができることを示している。

探索空間の大きさを固定 (B と B' の比較)

ここでは、$\mathbf{t}$ の第二成分 t_2 の値を 23 から 90 の範囲で大きく変化させ、$\#V_B(\mathbf{s}, \mathbf{t})$ が $2.5\mathrm{e}+06$ に近い値になるように $\mathbf{s}$ の第二成分 t_2 を調整する。このときの l_{min} の変化を、B と B' のそれぞれについて、図 6 に示す。図 6 では、t_2 を横軸にとっている。図 6 から分かるように、B と B' のいずれの場合でも、l_{min} は、大きな変化や規則的な変化は見られなかった。

以上の実験から、GS 和の小さい基底では、GS 和が大きい基底に対して非常に小さい探索空間において、より短いベクトルが得られることが分かった。

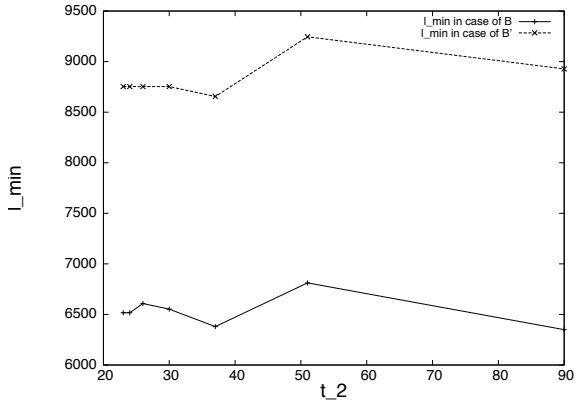

図 6　自然数表現として含む 1 の個数と存在する範囲を調整して探索空間の大きさを $2.5\mathrm{e}+06$ に近い値に固定した場合 (B と B' の比較) における t_2(X 軸) と l_{min}(Y 軸) の関係

3.3　GS 和の指標を用いる意義について

3.2 節において、基底 B と B' に関する実験条件として、それぞれの基底の GS 和を示した。ここで、より詳細な実験条件として、B と B' のそれぞれについて、基底に対応するグラム・シュミット直交ベクトル列 $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ の二乗ノルムを、図 7 に示す。図 7 においては、Y 軸のスケールの問題で後半のインデックスにおいて二乗ノルムの差が視認できなくなることを防ぐために、二乗ノルムについて 10 を底とした対数値を表示している。

図 7 から、$j = 1$ から $j = 20$ 辺りにおいては二乗ノルムはほとんど等しいが、$j = 20$ から $j = 50$ 辺りまでにおいては、B の二乗ノルムの方が小さいことが分かる。一方で、$j = 50$ 以降、後半のインデックスにおいては、B' の二乗ノルムの方が小さい傾向が読み取れる。後半のインデックスにおける $\mathbf{b}_j^*$ より、前半のインデックスにおける $\mathbf{b}_j^*$ の方が二乗ノルムの値が大きいため、探索で得られるベクトルのノルムの大きさに与える寄与が大きい ([11])。そのため、前半のインデックスにおいてより二乗ノルムが短い B を用いた方が、探索において有利である。GS 和の指標を導入する利点は、個々の $\mathbf{b}_j^*$ の二乗ノルムの大小ではな

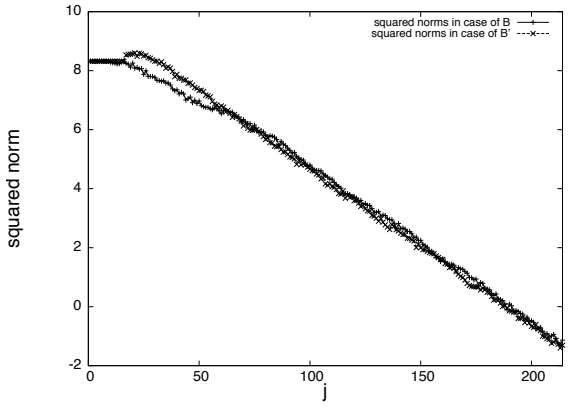

図 7　B と B' のグラムシュミット直交ベクトル列に関するベクトルのインデックス j(X 軸) と二乗ノルム $\log \mathbf{b}_j^*$(Y 軸) の関係

く、上記で示したような全ての $\mathbf{b}_j^*$ の二乗ノルムの傾向を、1 つの数値で提示できることである。基底に関する全ての $\mathbf{b}_j^*$ の二乗ノルムの傾向を 1 つの数値で提示する指標としては、全ての $\mathbf{b}_j^*$ の二乗ノルムを等比数列で近似した場合の公比 q がある (論文 [11])。しかし、公比 q は二乗ノルムの傾向を近似的に示すものであり、特に、NTRU では先頭周辺のインデックスにおける二乗ノルムを等比数列で近似することができないため、公比 q によって全ての二乗のルムの傾向を示すことは難しいと考えられる。一方、GS 和は、全ての二乗ノルムの和であり計算過程に誤差が生じないため、より精緻に全ての二乗ノルムの傾向を提示することができるという利点がある。

3.4　最短ベクトルを含む確率の分析

$n = 214$ の NTRU 格子について、NTRU の秘密鍵に相当するベクトルが $n/2 = 107$ 個含まれている。ここでは、これらの 107 個のベクトルを最短ベクトルとみなす。実験では、探索空間のパラメータ $\mathbf{s}, \mathbf{t}$ を固定して、GS 和の異なる 45 個の基底について、探索空間が最短ベクトルを 107 個のうち何個含むかを計算する。ここで、探索空間が最短ベクトルを含む確率として、最短ベクトルが探索空間に含まれる頻度（探索空間に含まれる最短ベクトルの個数を探索空間の大きさで割った値）を計算する。

最初に、$\mathbf{s}$ を $(214, 5)$、$\mathbf{t}$ を $(214, 50)$ に固定する。これらの $\mathbf{s}$ と $\mathbf{t}$ に対して、$\#V_B(\mathbf{s}, \mathbf{t}) = 2369935$ である。このとき GS 和の異なる 45 個の基底について、最短ベクトルが探索空間に含まれる頻度を図 8 に示す。ここで、GS 和を説明変数、最短ベクトルが探索空間に含まれる頻度を非説明変数として、線形回帰をして、傾きが 0 であるという帰無仮説を検定した。統計ソフト R を用いた検定の結果、p 値が 0.003596 で 0.05 より小さいので、有意水準 5% において帰無仮説が棄却された。

次に、$\mathbf{s}$ を $(214, 10)$、$\mathbf{t}$ を $(214, 60)$ に固定する。これらの $\mathbf{s}$ と $\mathbf{t}$ に対して、$\#V_B(\mathbf{s}, \mathbf{t}) = 93178047048$ である。このとき GS 和の異なる 45 個の基底について、最短ベクトルが探索空間に含まれる頻度を図 8 に示す。図 8 の場合と同様に、GS 和を説明変数、最短ベクトルが探索空間に含まれる頻度を非説明変数として、線形回帰をして、傾きが 0 であるという帰無仮説を検定した。統計ソフト R を用いた検定の結果、p 値が 0.00459 で 0.05 より小さいので、有意水準 5% において帰無仮説が棄却された。

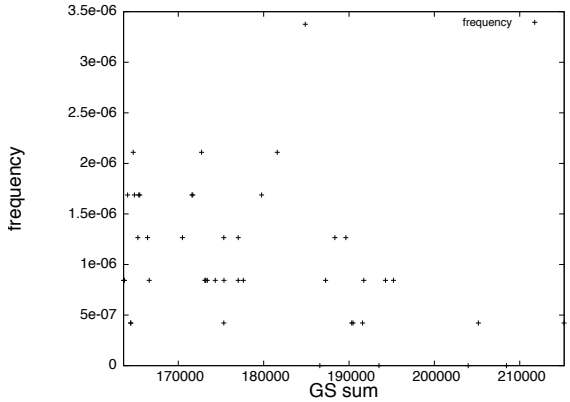

図 8　$\mathbf{s} = (214, 5)$、$\mathbf{t} = (214, 50)$ の場合における GS 和 (X 軸) と最短ベクトルが探索空間に含まれる頻度 (Y 軸) の関係

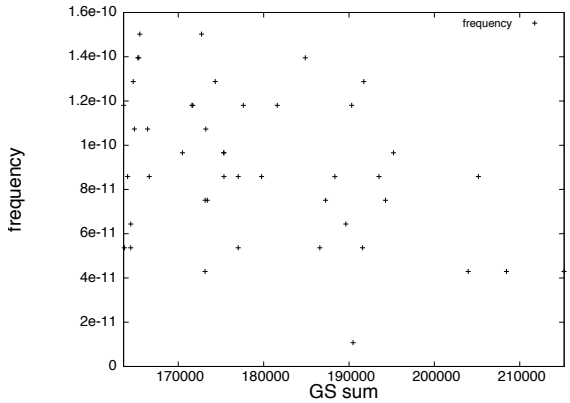

図 9　$\mathbf{s} = (214, 10)$、$\mathbf{t} = (214, 60)$ の場合における GS 和 (X 軸) と最短ベクトルが探索空間に含まれる頻度 (Y 軸) の関係

以上の実験から、基底の GS 和は探索空間に最短ベクトルが含まれる頻度の要因として認められるという結論を得た。図 8 と図 9 の場合それぞれにおいて、線形回帰の結果、傾きの符号は負であり、このことから、基底の GS 和が小さい程、探索空間に最短ベクトルが含まれる頻度が大きくなると判断できる。したがって、最短ベクトルを探索する上では、基底の GS 和を可能な限り下げてから探索を行うべきであると考えられる。

4.　まとめ

本研究では、基底の GS 和を基底の質を測る指標として、GS 和が探索効率に及ぼす効果について分析した。最短ベクトルの分かっている NTRU 格子を用いた実験の結果、GS 和の小さい基底を用いることで、より小さい探索空間で短いベクトルを求め得ることが示された。また、基底の GS 和が小さい程、探索空間に最短ベクトルが含まれる確

率が大きくなることを実験的に示した。

5. 今後の課題

関連研究の論文 [2] における実験では NTRU 格子の多数のインスタンスを用いており、NTRU 格子の最短ベクトルを実際に探索する実験を行っている。一方、本研究の実験では NTRU 格子の 1 つのインスタンスのみを用いており、NTRU 格子の最短ベクトルを実際に探索する実験を行っていない。今後の課題は、NTRU 格子の十分に多くのインスタンスを用いて実験を行うこと、及び、実験により導出した探索空間の最適パラメータを用いて NTRU 格子の最短ベクトルを実際に探索する実験を行うことである。

謝辞　本研究は，電気通信普及財団助成によるものである．

参考文献

[1] Chen, Y., Nguyen, P.Q.: BKZ 2.0: Better Lattice Security Estimates. Proceedings of ASIACRYPT 2011, vol. 7073 of LNCS, pp. 1-20, (2011).
[2] Fukase, M., Yamaguchi, K.: Exhaustive Search for Finding a Very Short Vector in High-Dimensional Lattices. Proceedings (short papers) of IWSEC 2010, pp. 26-41, (2010).
[3] Fukase, M., Kashiwabara, K.: An Accelerated Algorithm for Solving SVP Based on Statistical Analysis, JIP, vol.23, no.1, pp. 67-80, (2015).
[4] Gama, N., Nguyen, P.Q.: Predicting Lattice Reduction. EUROCRYPT 2008, vol. 4965 of LNCS, pp. 31-51, (2008).
[5] Gama, N., Nguyen, P.Q., Regev, O.: Lattice Enumeration Using Extreme Pruning. EUROCRYPT 2010, vol. 6110 of LNCS, pp. 257-278, (2010).
[6] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A Ring-Based Public Key Cryptosystem. Proceedings of ANTS III, vol. 1423 of LNCS, Springer-Verlag, pp. 267-288, (1998).
[7] Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring Polynomials with Rational Coefficients. Mathematische Ann., vol. 261, pp. 513-534, (1982).
[8] Lindner, R., Rückert, M.: Lattice challenge. Available at `http://www.latticechallenge.org/`.
[9] Schneider, M., Gama, N.: SVP challenge. Available at `http://www.latticechallenge.org/svp-challenge/`.
[10] Schnorr, C.P., Euchner, M.: Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems. Math. Programming, vol. 66, pp. 181-199, (1994).
[11] Schnorr, C.P.: Lattice Reduction by Random Sampling and Birthday Methods. STACS 2003, vol. 2607 of LNCS, Springer-Verlag, pp. 145-156, (2003).

ⓒ 2015 Information Processing Society of Japan