ISSN 2186-5647

6-5

暗号における多項式連立方程式の求解問題

日大生産工　○中村 周平

1 導入

多項式連立方程式とは, 次のような多項式により表される幾つかの変数の間の関係式の組のことである.

$$\begin{cases} 4x_3+3x_2+2x_3^2+x_2x_3+x_1x_3 & =1 \\ 2x_3+3x_2+2x_1+4x_3^2+2x_2x_3+2x_1x_3 & =2 \\ x_1+x_3^2+3x_2x_3+3x_1x_3 & =3 \end{cases}$$

また, 多項式連立方程式を解くということは, ここではこの関係式たちを満たす数の組を求めることであり, そのようなものが存在しない場合は空集合を返すこととする. 例えば, 各多項式の次数が 1 次の場合の多項式連立方程式問題は, 行列に対応させることにより, 行に関する掃き出しを行うことで解を求める方法が一般に知れらている. しかしながら, 一般の次数に関する多項式連立方程式求解問題は難しく, 2 次の場合でさえ, NP-困難性を有することが知られている ([3]).

多項式連立方程式の求解問題は, その素朴さから数学の様々なところで重要となるが, 暗号においても重要な対象として考えられている. 現在, 身の回りで多く用いられている暗号は, 素因数分解問題や離散対数問題などの数学の問題に関連したものを基に設計され, 問題の効率的な解法がないことがその暗号の安全性を保障している. しかしながら, これらの数学の問題は量子計算機を用いての求解が多項式時間で可能であることが分かり, その量子計算機の急速な開発の発展から, 耐量子暗号と呼ばれる量子計算機の攻撃に耐性のある暗号を設計することが要請されている. 先ほどの多項式連立方程式の求解問題はこのような量子計算機による計算にも耐性があるものと期待され, この問題を基にした多変数暗号は耐量子暗号の候補となっている.

2 多変数暗号

ここでは, 基本的な記号や記法を導入し, 多変数暗号の定式化を行う.

体 k において k 上の n 変数の多項式のなす集合の全体を $k[x_1,\dots,x_n]$ で表す. また, 多項式環の m 個の直和 $(k[x_1,\dots,x_n])^m$ の元 $F=(f_1,\dots,f_m)$ は, k 上 n 次元線形空間 k^n から k 上 m 次元線形空間 k^m への写像 $k^n \to k^m$ を次のようにして定める:

$$(a_1,\dots,a_n) \mapsto (f_1(a_1,\dots,a_n),\dots,f_m(a_1,\dots,a_n))$$

このように定まる写像は多項式写像と呼ばれる. このような概念に対して, 次の 3 つのアルゴリズムを用いて多項式暗号が働く.

1. セキュリティパラメータ sk に対して, 秘密鍵 S,F,T が生成される.
2. $a \in k^n$ に対して, $P(a)$ を計算する. ただし, $P=(p_1,\dots,p_n)=T\circ F\circ S$ である.
3. $b=(b_1,\dots,b_m) \in k^m$ に対して, $P^{-1}(b)=T^{-1}(F^{-1}(S^{-1}(b)))$ を計算する.

暗号化方式の場合, 2 は暗号化, 3 は復号のプロセスに対応する. また, 署名方式であれば, 3 は署名, 2 は検証のプロセスに対応するものとなる. これらの方式において, 暗号文 (もしくは平文) として $b \in k^m$ が与えられたとき $P^{-1}(b)$ から平文 (もしくは署名文) を得る攻撃は, 次の多項式連立方程式の求解に対応する.

$$\begin{cases} p_1(x_1,\dots,x_n)=b_1 \\ \vdots \\ p_m(x_1,\dots,x_n)=b_m \end{cases}$$

ここで, この暗号から生じる多項式連立方程式は一般に幾つかの条件を含んでいることに注意したい. 例えば, 体 k として利用されるのは有限体であり, 多項式連立方程式の解はその体上で求める. ゆえに, その体の位数 q としたとき, 解くべき多項式連立方程式に n 個の多項式 $x_i^q-x_i$ を加えることでその解が有限個であるように設定される. また, 暗号は構成の仕方から, 必ず付随する多項式連立方程式が解をもつことも判る.

Solving systems of polynomial equations in cryptography

Shuhei NAKAMURA

3 グレブナー基底

多項式環 $k[x_1,\ldots,x_n]$ とその空でない部分集合 S に対して, 加法に関する部分群

$$\langle S\rangle := \{r_1s_1+\cdots+r_ls_l \mid r_i\in k[x_1,\ldots,x_n], s_i\in S\}$$

はイデアルと呼ばれ, S はその生成系と呼ばれた. $S=\{s_i\}_{i\geq 1}$ のとき, これを単に, $\langle s_i \mid i\geq 1\rangle$ で表す. イデアルの構造が解空間の構造を表すことはよく知られており, 多項式連立方程式 $\{f_1=b_1,\ldots,f_m=b_m\}$ が与えられたとき, その解構造はイデアル $\langle f_1-b_1,\ldots,f_m-b_m\rangle$ により表され, このイデアルの異なる生成系は同様の解空間を有する. ここでは, グレブナー基底と呼ばれる "非常に良い"生成系を導入する.

$k[x_1,\ldots,x_n]$ に含まれるすべての単項式全体 $\mathbb{M}$ に対して, 次の条件を満たす全順序 $\leq$ は単項式順序と呼ばれた:

1. $m_1\leq m_2\Rightarrow m_1m_3\leq m_2m_3$ $(\forall m_i\in\mathbb{M})$
2. $1\leq m$ $(\forall m\in\mathbb{M})$

例えば, 順序 $x_1^{e_1}\cdots x_n^{e_n} <_{lex} x_1^{d_1}\cdots x_n^{d_n}$ を零でない最初の値 d_i-e_i が正となるものと定め, 等号成立を単項式の一致とすれば, $\leq_{lex}$ は単項式順序となる. 多項式

$$f := \sum_{(e_1,\ldots,e_n)\in\mathbb{Z}^n_{\geq 0}} c_{(e_1,\ldots,e_n)}x_1^{e_1}\cdots x_n^{e_n}$$

に対して, ある単項式順序 $\leq$ に関する先頭単項式 $LM_{\leq}(f)$ は次のように定義される:

$$LM_{\leq}(f) := \max_{\leq}\{x_1^{e_1}\cdots x_n^{e_n} \mid c_{(e_1,\ldots,e_n)}\neq 0\}$$

このとき, あるイデアルと単項式順序 $\leq$ に対して, 次の条件を満たす生成系 $G:=\{g_1,\ldots,g_r\}$ はグレブナー基底と呼ばれる:

$$\langle LM_{\leq}(g_1),\ldots,LM_{\leq}(g_r)\rangle = \langle LM_{\leq}(f) \mid f\in\langle G\rangle\rangle$$

さらに, 各 g_i とその零でない任意の項 m に対して, $m\notin\langle LM_{\leq}(g_j) \mid g_j\in G\setminus\{g_i\}\rangle$ が成り立つとき, 簡約グレブナー基底と呼ばれる.

次の定理は暗号においてグレブナー基底の概念を導入する背景となる主張である.

定理 1. I を "$\dim I=0$"となる $k[x_1,\ldots,x_n]$ のイデアルとする. このとき, $x_i >_{lex} x_{i+1}$ $(1\leq i\leq n-1)$ となる辞書式順序 $>_{lex}$ に対してその簡約グレブナー基底は次のようになる:

$$\begin{array}{l} p_{n,1}(x_n),\\ p_{n-1,1}(x_{n-1},x_n),\ldots,p_{n-1,t_{n-1}}(x_{n-1},x_n)\\ p_{n-2,1}(x_{n-2},x_{n-1},x_n),\ldots,p_{n-2,t_{n-2}}(x_{n-2},x_{n-1},x_n)\\ \vdots\\ p_{1,1}(x_1,\ldots,x_n),\ldots,p_{1,t_1}(x_1,\ldots,x_n)\end{array}$$

ただし, 各 $1\leq j\leq n-1$ に対して $t_j\geq 1$ である.

この "$\dim I=0$"であるという仮定は, 有限体上においては n 個の多項式 $x_i^q-x_i$ を加えることで常に満たされる. このイデアルに対して, 定理を適用することで, 1 変数多項式 $p_{n,1}(x_n)=0$ を解くことにより解となるベクトルの n 次成分の有限個の候補を得ることができる. 残りの式 $p_{n-1,1},\ldots,p_{1,t_1}$ に対してその根を代入することにより, 新たに $x_1,\ldots,x_{n-1}$ からなる多項式連立方程式を得る. 再び定理を適用することで次の x_{n-1} の候補を得るが, この操作を (有限回) 繰り返すことにより, 解となるベクトルの候補を得る.

4 正則次数

このようなグレブナー基底を計算するアルゴリズムは Buchberger アルゴリズムと呼ばれるアルゴリズムから発展した F_4 や F_5 と呼ばれる Faugere のものが主である ([2]). この複雑さは, そのアルゴリズムの計算中に現れる多項式の次数の最大値により支配することができ, その値を数学的に捉える必要がある. 本講演では, この値を評価するとされる "正則次数"と呼ばれる量を導入するが, その定義には異なる 3 つの定義があることから, その関係や特性についての考察を行う ([1]).

参考文献

[1] Bardet, M., Faugére, J-C. and Salvy, B., On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations, ICPPSS International Conference on Polynomial System Solving, 2004

[2] Ding, J., Gower, J. E. and Schmidt, D. S., Multivariate Public Key Cryptosystems, Springer, New York, 2006

[3] Garey, M. R. and Johnson, D. S., Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman, 1979