信州大学工学部

学士論文

2 変数 3 次の多項式補間法による秘密分散法における秘密情報の復元条件について

指導教員　西新 幹彦 准教授

学科　電気電子工学科
学籍番号　12T2003E
氏名　石井 真範

2017 年 3 月 2 日

目次

1　はじめに

個人情報や企業の機密情報の漏洩が社会問題になっている．各々に電子情報の紛失や漏洩を防ぐことが求められている．電子情報の紛失への対策としては，コピーを作成すればよい．しかし，コピーを作成すると，電子情報の漏洩のリスクは高まる．このような電子情報の紛失と漏洩への対策を両立させることのできる方法として，秘密分散法がある．

秘密分散法の実現法の一つとして Shamir の多項式補間法が挙げられる [1]．この方法は $f(0) = S$ を満たす 1 変数 $k-1$ 次の多項式からシェアと呼ばれる鍵情報 $V_i = f(i)$ を作り，それらが k 個集まれば多項式が復元出来ることを利用し，秘密情報 $S = f(0)$ を復号する手法である．

本研究では 1 変数多項式を用いる Shamir の多項式補間法を 2 変数に拡張した方法を取り扱う．1 変数ではシェアの個数のみで復元の可否が決まり，シェアが x 軸上のどの位置にあるかは復元に際して意味を持たない．しかし 2 変数としたとき，シェアは x-y 平面上の位置により特徴付けられ，集まったシェアの個数と位置の組み合わせにより復元の可否が決定するようになる．

本研究の将来的な大きな目標は，多変数多項式による秘密分散法のアクセス構造を一般に明らかにすることである．本論文では，その目標の実現に向けて，2 変数 3 次多項式を用いる場合に，秘密情報を復元するためのいくつかの条件を明らかにする．

本論文の構成は以下の通りである．次の 2 章では秘密分散法の定義と，Shamir の多項式補間法について述べる．3 章では，2 変数多項式補間に基づく秘密分散法についてと，1 次の場合と 2 次の場合のアクセス構造について述べる．4 章では，2 変数 3 次の秘密分散法における秘密情報復元のための十分条件を，シェアの個数で場合分けして述べる．5 章では，4 章で述べた復元条件の内，シェアの個数が 7 個の時の特別な場合について述べる．最後に 6 章でまとめを述べる．

2　秘密分散法

2.1　秘密分散法の定義

紛失や漏洩から守る対象となる情報を「秘密情報」とよぶ．また，秘密情報を復元するための鍵情報を「シェア」とよぶ．秘密分散法は秘密情報の保有者であるディーラーと，シェアを管理するユーザの間で行われる．秘密分散法には秘密情報からシェアを作成しユーザに分配する分散プロセスと，ユーザが集まりユーザの保有するシェアから秘密情報を復元する復元プロセスの 2 つのプロセスがある．秘密情報を復元できるシェアの集合をアクセス集合といい，復

元できないシェアの集合を非アクセス集合という．また，この 2 つを合わせてアクセス構造と呼ぶ．あるシェアの集合があったとき，その真部分集合がアクセス集合ならば，そのシェアの集合もアクセス集合である．また，非アクセス集合の真部分集合は，非アクセス集合である．

標準的な秘密分散法の定義では，秘密情報 S およびシェア V_1 , $\cdots$, V_m を確率変数とし，これらのシェアから秘密情報が復元できることとできないことをそれぞれ

$$H\left(S|V_1,\cdots,V_m\right)=0$$
$$0<H\left(S|V_1,\cdots,V_m\right)\leqq H\left(S\right)$$

と表す．ここに，$H(\cdot)$，$H(\cdot|\cdot)$　はそれぞれシャノンエントロピーと条件付きエントロピーである．アクセス構造には完全型とランプ型の分類がある．非アクセス集合である m 個のシェアが集まったとき，秘密情報のエントロピーが $H(S|V_1,V_2,\cdots,V_m)=H(S)$ となり，秘密情報に関する情報が全く漏洩しないものを完全型と呼ぶ．一方で，$H(S|V_1,V_2,\cdots,V_m)<H(S)$ となり，いくらか秘密情報に関する情報が漏洩してしまう場合があるものをランプ型と呼ぶ．このように非アクセス集合の中には，秘密情報が全く漏洩しないものと幾分か漏洩してしまうものの二種類がある．本論文では完全なアクセス構造について論じる．

2.2 Shamir の多項式補間法

Shamir の多項式補間法では $f(0)=S$ を満たす 1 変数 $k-1$ 次の多項式を用いる．また，演算はすべて有限体 $\mathbb{F}$ 上で行う．

まず，分散プロセスについて説明する．k 個のシェアを集めたら秘密情報を復元できるようにしたいとき，ディーラーは，$k-1$ 次の多項式

$$f(x)=A_{k-1}x^{k-1}+A_{k-2}x^{k-2}+\cdots+A_1x+S \tag{1}$$

を作る．この際，秘密情報 S は任意の分布でよいが，係数 $A_1,A_2,\cdots,A_{k-1}$ は $\mathbb{F}$ 上で互いに独立で一様な分布に従う確率変数とする．次に相異なる n 個の非零の要素 $x_1,\cdots,x_n$ を選び，式 (1) を用いて，シェア $V_i=(x_i,f(x_i))$ を作り，ユーザーに配布する．ここで，x_i は公開情報とし，$f(x_i)$ は各ユーザーが管理する非公開情報とする．また，ディーラーは，シェアをユーザーに配った後，$S,A_1,\cdots,A_{k-1}$ の値を破棄する．

次に復元プロセスについて説明する．k 個のシェアを集めれば，それを用いて式 (1) を求めることができる．これより，$f(0)=S$ の値を求めれば，秘密情報 S を復元できる．$k-1$ 個以下のシェアでは多項式 $f(x)$ を一意に定めることができないため，秘密情報を復元することはできない．

3　2 変数多項式補間に基づく秘密分散法

本研究では，2 変数多項式を次のように用いてシェアを作るような秘密分散法を考える．有限体 $\mathbb{F}$ を考える．位数は十分に大きな値とする．秘密情報 $S \in \mathbb{F}$ に対し，$\mathbb{F}$ 上の 2 変数多項式 $f(x, y)$ を定める．このとき，定数項を S とする．各係数は $\mathbb{F}$ 上の一様分布に従う確率変数であり，ほかの確率変数とも独立である．シェアは $V_i = (x_i, y_i, Z_i)$ といった形で与えられる．$Z_i = f(x_i, y_i)$ とし，これをシェアの高さと呼ぶ．また，(x_i, y_i) をシェアの位置と呼ぶ．本論文で扱う秘密分散法は各ユーザーは互いに異なるシェアを一つずつ管理する．したがってシェアとユーザーは区別されない．非公開情報としてユーザーに管理されるのはシェアの高さのみとし，シェアの位置は公開情報とする．また，秘密情報の値および多項式の係数については非公開とする．したがって，各シェアの非公開情報のサイズは秘密情報と同じである．このことから，アクセス構造によっては攻撃者に狙われやすいシェアとそうでないシェアの差が生じるが，そうした危険性の大小や対策は本論文では扱わない．もし各シェアの位置も非公開情報とすればその問題は解消されるが，非公開情報の量は 3 倍になる．なお秘密分散の目的から，原点に位置するシェアは生成しない．

以降の 3.1 節と 3.2 節では，過去の研究ですでに明らかにされている 2 変数 1 次多項式 [2] と 2 変数 2 次多項式 [3] を用いた秘密分散法のアクセス構造をそれぞれ示す．その後に 4 章で，本論文の主眼である 2 変数 3 次の多項式補間法による秘密分散法における秘密情報の復元条件について述べる．

3.1　1 次の場合のアクセス構造

1 次の場合に使用する多項式 $f(x, y)$ は

$$f(x, y) = Ax + By + S \tag{2}$$

である．

多項式の項が 3 つであることから，極小のアクセス集合のサイズは 3 以下である．従って 4 個以上のシェアからなるアクセス集合は 3 個以下からなるアクセス集合の議論に帰着される．またシェアが 1 個の場合，非アクセス集合である．以上より，以下の項ではシェアの個数が 2,3 個の場合のアクセス構造を示す．

3.1.1　シェアが 2 個の場合

定理 3.1　異なる 2 個のシェア V_1, V_2 がアクセス集合となるための必要十分条件は，行列

$$M_2 = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \tag{3}$$

の階数が 1 となることである．

（証明）まず，十分性を証明する．式 (3) に示した行列 M_2 の階数が 1 と仮定する．このとき，与えられた 2 個のシェアについて一般性を損なうことなく $y_i = \alpha x_i (i = 1, 2)$ を満たす α が一意に決定出来る．ここで $x_1 = x_2$ と仮定すると $y_1 = y_2$ が得られ，同じ位置のシェアは与えられないという仮定に矛盾する．このことから x_1, x_2 は互いに異なることが言える．今シェアの位置と Z_i について，

$$\begin{aligned}\begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} &= \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{pmatrix} \begin{pmatrix} A \\ B \\ S \end{pmatrix} \\ &= \begin{pmatrix} x_1 & \alpha x_1 & 1 \\ x_2 & \alpha x_2 & 1 \end{pmatrix} \begin{pmatrix} A \\ B \\ S \end{pmatrix} \\ &= \begin{pmatrix} x_1 & 1 \\ x_2 & 1 \end{pmatrix} \begin{pmatrix} A + \alpha B \\ S \end{pmatrix} \end{aligned} \tag{4}$$

が成り立つ．式 (4) の右辺の正方行列は Vandermonde 行列であり正則なので，逆行列が存在する．この逆行列を両辺に左からかけることで S の値を得ることが出来るため，このとき秘密情報が復元出来る．

次に，必要性を証明する．原点に位置するシェアは存在しないという仮定から，行列 M_2 の階数は 0 ではない．よって M_2 の階数を 2 と仮定して，秘密情報が復元できないことを示す．この時，M_2 は正則なので逆行列が存在するため，

$$\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}^{-1} \begin{pmatrix} Z_1 - S \\ Z_2 - S \end{pmatrix} \tag{5}$$

が成り立つ．これは，秘密情報の値を $S = s$ と固定したもとで，(Z_1, Z_2) と (A, B) の間に全単射が存在することを意味する．したがって，秘密情報の値が $S = s$ であるもとでは，(Z_1, Z_2) は $\mathbb{F}^2$ 上に一様分布する．さらにこのことから，秘密情報の値によらず (Z_1, Z_2) が一様に分布することがわかる．以上のことからベイズの定理により，シェア (V_1, V_2) を得たもとでの秘密情報の分布はシェアのないもとでの分布に等しい．具体的には，式 (5) を用いて

$$\begin{pmatrix} a \\ b \end{pmatrix} \triangleq \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}^{-1} \begin{pmatrix} z_1 - s \\ z_2 - s \end{pmatrix} \tag{6}$$

のように a, b の値を定めれば

$$Ax_1 + By_1 + s = z_1, \quad Ax_2 + By_2 + s = z_2 \tag{7}$$

と

$$A = a, \quad B = b \tag{8}$$

は等価であるため

$$\begin{aligned}\Pr\{Z_1 = z_1, Z_2 = z_2 | S = s\} &= \Pr\{Ax_1 + By_1 + S = z_1, Ax_2 + By_2 + S = z_2 | S = s\} \\ &= \Pr\{A = a\} \Pr\{B = b\} \\ &= \frac{1}{|\mathbb{F}|^2} \end{aligned} \tag{9}$$

となる．このことから

$$\begin{aligned}\Pr\{Z_1 = z_1, Z_2 = z_2\} &= \sum_s \Pr\{S = s, Z_1 = z_1, Z_2 = z_2\} \\ &= \sum_s \Pr\{S = s\} \Pr\{Z_1 = z_1, Z_2 = z_2 | S = s\} \\ &= \sum_s \Pr\{S = s\} \frac{1}{|\mathbb{F}|^2} \\ &= \frac{1}{|\mathbb{F}|^2} \end{aligned} \tag{10}$$

となり，ベイズの定理から

$$\begin{aligned}\Pr\{S = s | Z_1 = z_1, Z_2 = z_2\} &= \frac{\Pr\{Z_1 = z_1, Z_2 = z_2 | S = s\} \Pr\{S = s\}}{\Pr\{Z_1 = z_1, Z_2 = z_2\}} \\ &= \Pr\{S = s\} \end{aligned} \tag{11}$$

となる．したがって以上より，

$$H(S|V_1, V_2) = H(S) \tag{12}$$

が成り立つ．□

3.1.2 シェアが 3 個の場合

定理 3.2 異なる 3 個のシェア V_1, V_2, V_3 がアクセス集合であるための必要十分条件は，ある真部分集合がアクセス集合であるか，行列

$$M_3 = \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix} \tag{13}$$

が正則となることである．

（証明）アクセス集合であるような真部分集合が存在する場合は自明なので，以降は真部分集合が非アクセス集合であると仮定して証明を進める．

まず十分性を証明する．行列 M_3 の階数を 3 と仮定する．このとき，

$$\begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \end{pmatrix} = M_3 \begin{pmatrix} A \\ B \\ S \end{pmatrix} \tag{14}$$

が成り立つ．ここで行列 M_3 は階数が 3 なので逆行列が存在し，それを両辺に左からかけることで多項式の各係数が復元できる．よってこのとき秘密情報 S が復元可能である．

次に必要性を証明する．原点に位置するシェアは存在しないという仮定から，行列 M_3 の階数は 0 ではない．よって M_3 の階数を 1 か 2 と仮定して，秘密情報が復元できないことを示す．

最初に M_3 の階数が 1 である場合を考える．M_3 の階数が 1 とすると，$x_1 = x_2 = x_3, y_1 = y_2 = y_3$ となる．これは同じ位置のシェアは作らないという前提に矛盾する．

次に，M_3 の階数が 2 である場合を考える．ここで一般性を損なうことなく，M_3 の 3 行目がほかの 2 行に線形従属であるとする．この時，一次結合の係数 α_1, α_2 が存在し，

$$\begin{aligned} \begin{pmatrix} x_3 & y_3 & 1 \end{pmatrix} &= \begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix} \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{pmatrix} \\ Z_3 &= \alpha_1 Z_1 + \alpha_2 Z_2 \end{aligned} \tag{15}$$

を満たす．

ここで式 (3) のように M_2 を定義すると，

$$\begin{pmatrix} x_3 & y_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix} M_2 \tag{16}$$

が成り立つ．今，M_2 の階数は 1 か 2 である．行列 M_2 の階数が 1 の場合，真部分集合が非アクセス集合であるという仮定に矛盾する．行列 M_2 の階数が 2 の場合，3.1.1 項の M_2 の階数が 2 の場合と同様に式 (17) が成り立つ．

$$H(S|V_1, V_2) = H(S) \tag{17}$$

一方，式 (12) より，Z_3 は (Z_1, Z_2) の関数であることがわかる．これは

$$H(S|V_1, V_2, V_3) = H(S|V_1, V_2) \tag{18}$$

を意味する．以上より，

$$H(S|V_1, V_2, V_3) = H(S) \tag{19}$$

が成り立つ．□

3.2　2 次の場合のアクセス構造

2 次の場合に使用する多項式 $f(x,y)$ は

$$f(x,y) = Ax^2 + Bx + Cxy + Dy + Ey^2 + S \tag{20}$$

である．

多項式の項が 6 つであることから，極小のアクセス集合のサイズは 6 以下である．従って 7 個以上のシェアからなるアクセス集合は 6 個以下からなるアクセス集合の議論に帰着される．またシェアが 1,2 個の場合，非アクセス集合である．以上より，以下の項ではシェアの個数が 2,3,4,5,6 個の場合のアクセス構造を示す．

3.2 節の内容は，文献 [3] で明らかにされたものである．以下では定理だけを述べる．証明は文献 [3] を参照されたい．

3.2.1　シェアが 3 個の場合

定理 3.3　異なる 3 個のシェア V_1, V_2, V_3 がアクセス集合となるための必要十分条件は，行列

$$M_3 = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \end{pmatrix} \tag{21}$$

の階数が 1 となることである．

3.2.2　シェアが 4 個の場合

定理 3.4　異なる 4 個のシェアがアクセス集合であるための必要十分条件は，ある真部分集合がアクセス集合であることである．

3.2.3　シェアが 5 個の場合

定理 3.5　異なる 5 個のシェア V_1, V_2, V_3, V_4, V_5 がアクセス集合であるための必要十分条件は，ある真部分集合がアクセス集合であるか，または行列

$$M_5 = \begin{pmatrix} x_1^2 & x_1 & x_1y_1 & y_1 & y_1^2 \\ x_2^2 & x_2 & x_2y_2 & y_2 & y_2^2 \\ x_3^2 & x_3 & x_3y_3 & y_3 & y_3^2 \\ x_4^2 & x_4 & x_4y_4 & y_4 & y_4^2 \\ x_5^2 & x_5 & x_5y_5 & y_5 & y_5^2 \end{pmatrix} \tag{22}$$

の階数が 4 でありかつ M_5 のある列の要素をすべて 1 にした行列 M_5' の階数が 5 となることである．

3.2.4 シェアが 6 個の場合

定理 3.6 異なる 6 個のシェア $V_1, V_2, V_3, V_4, V_5, V_6$ がアクセス集合であるための必要十分条件は，ある真部分集合がアクセス集合であるか，または行列

$$M_6 = \begin{pmatrix} x_1^2 & x_1 & x_1y_1 & y_1 & y_1^2 & 1 \\ x_2^2 & x_2 & x_2y_2 & y_2 & y_2^2 & 1 \\ x_3^2 & x_3 & x_3y_3 & y_3 & y_3^2 & 1 \\ x_4^2 & x_4 & x_4y_4 & y_4 & y_4^2 & 1 \\ x_5^2 & x_5 & x_5y_5 & y_5 & y_5^2 & 1 \\ x_6^2 & x_6 & x_6y_6 & y_6 & y_6^2 & 1 \end{pmatrix} \tag{23}$$

の階数が 6 となることである．

4 2 変数 3 次の秘密分散法

この章では，本論文の主題である 2 変数 3 次の秘密分散法における秘密情報の復元条件について論じる．3 次の場合の多項式 $f(x, y)$ は

$$f(x, y) = A_1x^3 + A_2x^2y + A_3xy^2 + A_4y^3 + A_5x^2 + A_6xy + A_7y^2 + A_8x + A_9y + S \tag{24}$$

である．

多項式の項が 10 個あることから，極小のアクセス集合のサイズは 10 以下である．従って 11 個以上のシェアからなるアクセス集合は 10 個以下からなるアクセス集合の議論に帰着される．

以下の節では，シェアの個数が 4,7,9,10 の場合の秘密情報復元のための十分条件をそれぞれ示す．シェアが 7 個の特別な場合については，より具体的に十分条件を示すことができるので，章を改めて論じる．シェアの個数がその他の場合については今のところ明らかになっていない．

4.1 シェア 4 個で復元する条件

定理 4.1 異なる 4 個のシェア V_1, V_2, V_3, V_4 がアクセス集合であるための十分条件は，行列

$$M_4 = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \\ x_4 & y_4 \end{pmatrix} \tag{25}$$

の階数が 1 となることである．

（証明）式 (25) に示した行列 M_4 の階数が 1 と仮定する．このとき，与えられた 4 個のシェアについて一般性を損なうことなく $y_i = \alpha x_i (i = 1, 2, 3, 4)$ を満たす α が一意に決定出来る．ここで $x_1 = x_2$ と仮定すると $y_1 = y_2$ が得られ，同じ位置のシェアは与えられないという仮定に矛盾する．このことから x_1, x_2, x_3, x_4 は互いに全て異なることが言える．今シェアの位置と Z_i について，

$$
\begin{aligned}
\begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \\ Z_4 \end{pmatrix} &= \begin{pmatrix} x_1^3 & x_1^2 y_1 & x_1 y_1^2 & y_1^3 & x_1^2 & x_1 y_1 & y_1^2 & x_1 & y_1 & 1 \\ x_2^3 & x_2^2 y_2 & x_2 y_1^2 & y_2^3 & x_2^2 & x_2 y_2 & y_2^2 & x_2 & y_2 & 1 \\ x_3^3 & x_3^2 y_3 & x_3 y_1^2 & y_3^3 & x_3^2 & x_3 y_3 & y_3^2 & x_3 & y_3 & 1 \\ x_4^3 & x_4^2 y_4 & x_4 y_1^2 & y_4^3 & x_4^2 & x_4 y_4 & y_4^2 & x_4 & y_4 & 1 \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \\ A_8 \\ A_9 \\ S \end{pmatrix} \\
&= \begin{pmatrix} x_1^3 & \alpha x_1^3 & \alpha^2 x_1^3 & \alpha^3 x_1^3 & x_1^2 & \alpha x_1^2 & \alpha^2 x_1^2 & x_1 & \alpha x_1 & 1 \\ x_2^3 & \alpha x_2^3 & \alpha^2 x_2^3 & \alpha^3 x_2^3 & x_2^2 & \alpha x_2^2 & \alpha^2 x_2^2 & x_2 & \alpha x_2 & 1 \\ x_3^3 & \alpha x_3^3 & \alpha^2 x_3^3 & \alpha^3 x_3^3 & x_3^2 & \alpha x_3^2 & \alpha^2 x_3^2 & x_3 & \alpha x_3 & 1 \\ x_4^3 & \alpha x_4^3 & \alpha^2 x_4^3 & \alpha^3 x_4^3 & x_4^2 & \alpha x_4^2 & \alpha^2 x_4^2 & x_4 & \alpha x_4 & 1 \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \\ A_8 \\ A_9 \\ S \end{pmatrix} \\
&= \begin{pmatrix} x_1^3 & x_1^2 & x_1 & 1 \\ x_2^3 & x_2^2 & x_2 & 1 \\ x_3^3 & x_3^2 & x_3 & 1 \\ x_4^3 & x_4^2 & x_4 & 1 \end{pmatrix} \begin{pmatrix} A_1 + \alpha A_2 + \alpha^2 A_3 + \alpha^3 A_4 \\ A_5 + \alpha A_6 + \alpha^2 A_7 \\ A_8 + \alpha A_9 \\ S \end{pmatrix} \qquad (26)
\end{aligned}
$$

が成り立つ．式 (26) の右辺の正方行列は Vandermonde 行列であり正則なので，逆行列が存在する．この逆行列を両辺に左からかけることで S の値を得ることが出来るため，このとき秘密情報が復元出来る．□

4.2 シェア 7 個で復元する条件

定理 4.2 7 個のシェア $V_1, V_2, V_3, V_4, V_5, V_6, V_7$ がすべて，x-y 平面において原点を通る 2 次曲線

$$
g(x, y) = B_1 x^2 + B_2 x + B_3 xy + B_4 y + B_5 y^2 = 0 \qquad (27)
$$

上にあるとする．この時，行列

$$\begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \\ Z_4 \\ Z_5 \\ Z_6 \\ Z_7 \end{pmatrix} = \begin{pmatrix} x_1^3 & x_1^2y_1 & x_1y_1^2 & y_1^3 & x_1^2 & x_1y_1 & y_1^2 & x_1 & y_1 & 1 \\ x_2^3 & x_2^2y_2 & x_2y_1^2 & y_2^3 & x_2^2 & x_2y_2 & y_2^2 & x_2 & y_2 & 1 \\ x_3^3 & x_3^2y_3 & x_3y_1^2 & y_3^3 & x_3^2 & x_3y_3 & y_3^2 & x_3 & y_3 & 1 \\ x_4^3 & x_4^2y_4 & x_4y_1^2 & y_4^3 & x_4^2 & x_4y_4 & y_4^2 & x_4 & y_4 & 1 \\ x_5^3 & x_5^2y_5 & x_5y_1^2 & y_5^3 & x_5^2 & x_5y_5 & y_5^2 & x_5 & y_5 & 1 \\ x_6^3 & x_6^2y_6 & x_6y_1^2 & y_6^3 & x_6^2 & x_6y_6 & y_6^2 & x_6 & y_6 & 1 \\ x_7^3 & x_7^2y_7 & x_7y_1^2 & y_7^3 & x_7^2 & x_7y_7 & y_7^2 & x_7 & y_7 & 1 \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \\ A_8 \\ A_9 \\ S \end{pmatrix} \tag{28}$$

の右辺の 7×10 行列を，式 (27) を用いて 10 列の内 3 列を他の 7 列で表すことにより，7×7 行列の M_7 にすることができる．M_7 に逆行列が存在すれば，秘密情報 S を復元することができる．

（証明）式 (27) は 2 次曲線なので，2 次の項の係数は $(B_1, B_3, B_5) \neq (0, 0, 0)$ である．よって，x^2, xy, y^2 のいずれか 1 つの項は他の項の線形結合で表すことができるため，消すことができる．また，その 2 次の項に x, y を上手くかけ合わせれば，3 次の項 2 つを他の項で表すことができるため，消すことができる．

例として，$B_1 \neq 0, B_3 = 0, B_5 = 0$ の場合について説明する．この時，式 (27) は

$$g(x, y) = B_1x^2 + B_2x + B_4y = 0 \tag{29}$$

となる．式 (29) から次の 3 式

$$x^2 = -\frac{B_2}{B_1}x - \frac{B_4}{B_1}y \tag{30}$$

$$x^2y = -\frac{B_2}{B_1}xy - \frac{B_4}{B_1}y^2 \tag{31}$$

$$x^3 = -\frac{B_2}{B_1}x^2 - \frac{B_4}{B_1}xy = \frac{B_2}{B_1}(\frac{B_2}{B_1}x + \frac{B_4}{B_1}y) - \frac{B_4}{B_1}xy \tag{32}$$

を得ることができる．式 (30) (31) (32) を用いて式 (28) を変形すると，

$$\begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \\ Z_4 \\ Z_5 \\ Z_6 \\ Z_7 \end{pmatrix} = \begin{pmatrix} x_1y_1^2 & y_1^3 & x_1y_1 & y_1^2 & x_1 & y_1 & 1 \\ x_2y_1^2 & y_2^3 & x_2y_2 & y_2^2 & x_2 & y_2 & 1 \\ x_3y_1^2 & y_3^3 & x_3y_3 & y_3^2 & x_3 & y_3 & 1 \\ x_4y_1^2 & y_4^3 & x_4y_4 & y_4^2 & x_4 & y_4 & 1 \\ x_5y_1^2 & y_5^3 & x_5y_5 & y_5^2 & x_5 & y_5 & 1 \\ x_6y_1^2 & y_6^3 & x_6y_6 & y_6^2 & x_6 & y_6 & 1 \\ x_7y_1^2 & y_7^3 & x_7y_7 & y_7^2 & x_7 & y_7 & 1 \end{pmatrix} \begin{pmatrix} A_3 \\ A_4 \\ A_6 - \frac{B_4}{B_1} - \frac{B_2}{B_1} \\ A_7 - \frac{B_4}{B_1} \\ A_8 - \frac{B_2}{B_1} + \frac{B_2^2}{B_1^2} \\ A_9 - \frac{B_4}{B_1} \\ S \end{pmatrix} \tag{33}$$

となる．以上より，式 (28) の右辺の 7×10 行列を，式 (29) を用いることにより 7×7 行列にすることができた．式 (33) の右辺の 7×7 行列に逆行列が存在すれば，秘密情報 S を復元することができることがわかる．$B_1\neq0, B_3=0, B_5=0$ 以外の場合についても同様にして 7×7 行列を求めることができる．各場合についてどの項が消えるかの一覧を付録 A.3 に示した．□

定理 4.2 により M_7 を作ることのできる例として，原点を通る 2 次曲線が $g(x,y)=y-\alpha x^2$ である場合があげられるが，この時，M_7 は必ず正則となる．これを特殊な例として 5.1 節で紹介する．

$g(x.y)$ が因数分解できる時，2 次曲線ではなく 2 本の直線となる．この時，シェアの位置によっては 7 個のシェアで秘密を復元することができる．これを 5.2 節に示す．

また，2 次曲線の分類について，付録 A.1 で述べる．

4.3 シェア 9 個で復元する条件

定理 4.3 9 個のシェア $V_1,V_2,V_3,V_4,V_5,V_6,V_7,V_8,V_9$ がすべて，x-y 平面において原点を通る 3 次曲線

$$h(x,y)=C_1x^3+C_2x^2y+C_3xy^2+C_4y^3+C_5x^2+C_6xy+C_7y^2+C_8x+C_9y=0 \quad (34)$$

上にあるとする．この時，行列

$$\begin{pmatrix}Z_1\\Z_2\\Z_3\\Z_4\\Z_5\\Z_6\\Z_7\\Z_8\\Z_9\end{pmatrix}=\begin{pmatrix}x_1^3&x_1^2y_1&x_1y_1^2&y_1^3&x_1^2&x_1y_1&y_1^2&x_1&y_1&1\\x_2^3&x_2^2y_2&x_2y_1^2&y_2^3&x_2^2&x_2y_2&y_2^2&x_2&y_2&1\\x_3^3&x_3^2y_3&x_3y_1^2&y_3^3&x_3^2&x_3y_3&y_3^2&x_3&y_3&1\\x_4^3&x_4^2y_4&x_4y_1^2&y_4^3&x_4^2&x_4y_4&y_4^2&x_4&y_4&1\\x_5^3&x_5^2y_5&x_5y_1^2&y_5^3&x_5^2&x_5y_5&y_5^2&x_5&y_5&1\\x_6^3&x_6^2y_6&x_6y_1^2&y_6^3&x_6^2&x_6y_6&y_6^2&x_6&y_6&1\\x_7^3&x_7^2y_7&x_7y_1^2&y_7^3&x_7^2&x_7y_7&y_7^2&x_7&y_7&1\\x_8^3&x_8^2y_8&x_8y_1^2&y_8^3&x_8^2&x_8y_8&y_8^2&x_8&y_8&1\\x_9^3&x_9^2y_9&x_9y_1^2&y_9^3&x_9^2&x_9y_9&y_9^2&x_9&y_9&1\end{pmatrix}\begin{pmatrix}A_1\\A_2\\A_3\\A_4\\A_5\\A_6\\A_7\\A_8\\A_9\\S\end{pmatrix} \quad (35)$$

の右辺の 9×10 行列を，式 (34) を用いて 10 列の内 1 列を他の 9 列で表すことにより，9×9 行列 M_9 にすることができる．M_9 に逆行列が存在すれば，秘密情報 S を復元することができる．

（証明）式 (34) は 3 次曲線なので，3 次の項の係数 $(C_1,C_2,C_3,C_4)\neq(0,0,0,0)$ である．よって，x^3,x^2y,xy^2,y^3 のいずれか 1 つの項は他の項の線形結合で表すことができる．これを踏まえて式 (35) 右辺の 9×10 行列と 10×1 行列を変形することにより，9×9 行列と 9×1 行列にすることができる．□

n 次曲線を決定する点の条件について，付録 A.2 で述べる．

4.4　シェア 10 個で復元する条件

定理 4.4　異なる 10 個のシェア $V_1, V_2, V_3, V_4, V_5, V_6, V_7, V_8, V_9, V_{10}$ がアクセス集合であるための十分条件は，行列

$$M_{10} = \begin{pmatrix} x_1^3 & x_1^2y_1 & x_1y_1^2 & y_1^3 & x_1^2 & x_1y_1 & y_1^2 & x_1 & y_1 & 1 \\ x_2^3 & x_2^2y_2 & x_2y_2^2 & y_2^3 & x_2^2 & x_2y_2 & y_2^2 & x_2 & y_2 & 1 \\ x_3^3 & x_3^2y_3 & x_3y_3^2 & y_3^3 & x_3^2 & x_3y_3 & y_3^2 & x_3 & y_3 & 1 \\ x_4^3 & x_4^2y_4 & x_4y_4^2 & y_4^3 & x_4^2 & x_4y_4 & y_4^2 & x_4 & y_4 & 1 \\ x_5^3 & x_5^2y_5 & x_5y_5^2 & y_5^3 & x_5^2 & x_5y_5 & y_5^2 & x_5 & y_5 & 1 \\ x_6^3 & x_6^2y_6 & x_6y_6^2 & y_6^3 & x_6^2 & x_6y_6 & y_6^2 & x_6 & y_6 & 1 \\ x_7^3 & x_7^2y_7 & x_7y_7^2 & y_7^3 & x_7^2 & x_7y_7 & y_7^2 & x_7 & y_7 & 1 \\ x_8^3 & x_8^2y_8 & x_8y_8^2 & y_8^3 & x_8^2 & x_8y_8 & y_8^2 & x_8 & y_8 & 1 \\ x_9^3 & x_9^2y_9 & x_9y_9^2 & y_9^3 & x_9^2 & x_9y_9 & y_9^2 & x_9 & y_9 & 1 \\ x_{10}^3 & x_{10}^2y_{10} & x_{10}y_{10}^2 & y_{10}^3 & x_{10}^2 & x_{10}y_{10} & y_{10}^2 & x_{10} & y_{10} & 1 \end{pmatrix} \tag{36}$$

が正則であることである．

（証明）行列 M_{10} が正則と仮定する．このとき，

$$\begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \\ Z_4 \\ Z_5 \\ Z_6 \\ Z_7 \\ Z_8 \\ Z_9 \\ Z_{10} \end{pmatrix} = M_{10} \begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \\ A_8 \\ A_9 \\ S \end{pmatrix} \tag{37}$$

が成り立つ．ここで行列 M_{10} が正則なので逆行列が存在し，それを両辺に左からかけることで多項式の各係数が復元できる．よってこのとき秘密情報 S が復元可能である．□

5　シェア 7 個の特別な場合

4.2 節において，シェア 7 個の場合に秘密情報を復元することができる十分条件を示した．この時，M_7 に逆行列が存在すれば秘密情報を復元できるとしたが，式 (27) が $g(x, y) = y - \alpha x^2$ の時は，M_7 に逆行列が存在する．これを 5.1 節で示す．

また 4.2 節において，式 (27) が 2 本の直線となるときがあると述べた．この時，シェアの位置によっては秘密情報を復元できる．これを 5.2 節で示す．

5.1 $y = \alpha x^2$ 上にある場合

定理 5.1 *x-y 平面において，7 個のシェア $V_1, V_2, V_3, V_4, V_5, V_6, V_7$ がすべて，原点を通る 2 次曲線 $g(x, y) = y - \alpha x^2 = 0$ 上にあるとき，この 7 個のシェアはアクセス集合となる．*

（証明）7 個のシェア $V_1, V_2, V_3, V_4, V_5, V_6, V_7$ がすべて，原点を通る 2 次曲線 $g(x, y) = y - \alpha x^2 = 0$ 上にあるとする．ここで $x_1 = x_2$ と仮定すると $y_1 = y_2$ が得られ，同じ位置のシェアは与えられないという仮定に矛盾する．このことから $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ は互いに全て異なることが言える．今シェアの位置と Z_i について，

$$
\begin{aligned}
\begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \\ Z_4 \\ Z_5 \\ Z_6 \\ Z_7 \end{pmatrix}
&= \begin{pmatrix}
x_1^3 & x_1^2 y_1 & x_1 y_1^2 & y_1^3 & x_1^2 & x_1 y_1 & y_1^2 & x_1 & y_1 & 1 \\
x_2^3 & x_2^2 y_2 & x_2 y_1^2 & y_2^3 & x_2^2 & x_2 y_2 & y_2^2 & x_2 & y_2 & 1 \\
x_3^3 & x_3^2 y_3 & x_3 y_1^2 & y_3^3 & x_3^2 & x_3 y_3 & y_3^2 & x_3 & y_3 & 1 \\
x_4^3 & x_4^2 y_4 & x_4 y_1^2 & y_4^3 & x_4^2 & x_4 y_4 & y_4^2 & x_4 & y_4 & 1 \\
x_5^3 & x_5^2 y_5 & x_5 y_1^2 & y_5^3 & x_5^2 & x_5 y_5 & y_5^2 & x_5 & y_5 & 1 \\
x_6^3 & x_6^2 y_6 & x_6 y_1^2 & y_6^3 & x_6^2 & x_6 y_6 & y_6^2 & x_6 & y_6 & 1 \\
x_7^3 & x_7^2 y_7 & x_7 y_1^2 & y_7^3 & x_7^2 & x_7 y_7 & y_7^2 & x_7 & y_7 & 1
\end{pmatrix}
\begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \\ A_8 \\ A_9 \\ S \end{pmatrix} \\
&= \begin{pmatrix}
x_1^3 & \alpha x_1^4 & \alpha^2 x_1^5 & \alpha^3 x_1^6 & x_1^2 & \alpha x_1^3 & \alpha^2 x_1^4 & x_1 & \alpha x_1^2 & 1 \\
x_2^3 & \alpha x_2^4 & \alpha^2 x_2^5 & \alpha^3 x_2^6 & x_2^2 & \alpha x_2^3 & \alpha^2 x_2^4 & x_2 & \alpha x_2^2 & 1 \\
x_3^3 & \alpha x_3^4 & \alpha^2 x_3^5 & \alpha^3 x_3^6 & x_3^2 & \alpha x_3^3 & \alpha^2 x_3^4 & x_3 & \alpha x_3^2 & 1 \\
x_4^3 & \alpha x_4^4 & \alpha^2 x_4^5 & \alpha^3 x_4^6 & x_4^2 & \alpha x_4^3 & \alpha^2 x_4^4 & x_4 & \alpha x_4^2 & 1 \\
x_5^3 & \alpha x_5^4 & \alpha^2 x_5^5 & \alpha^3 x_5^6 & x_5^2 & \alpha x_5^3 & \alpha^2 x_5^4 & x_5 & \alpha x_5^2 & 1 \\
x_6^3 & \alpha x_6^4 & \alpha^2 x_6^5 & \alpha^3 x_6^6 & x_6^2 & \alpha x_6^3 & \alpha^2 x_6^4 & x_6 & \alpha x_6^2 & 1 \\
x_7^3 & \alpha x_7^4 & \alpha^2 x_7^5 & \alpha^3 x_7^6 & x_7^2 & \alpha x_7^3 & \alpha^2 x_7^4 & x_7 & \alpha x_7^2 & 1
\end{pmatrix}
\begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \\ A_8 \\ A_9 \\ S \end{pmatrix} \\
&= \begin{pmatrix}
x_1^6 & x_1^5 & x_1^4 & x_1^3 & x_1^2 & x_1 & 1 \\
x_2^6 & x_2^5 & x_2^4 & x_2^3 & x_2^2 & x_2 & 1 \\
x_3^6 & x_3^5 & x_3^4 & x_3^3 & x_3^2 & x_3 & 1 \\
x_4^6 & x_4^5 & x_4^4 & x_4^3 & x_4^2 & x_4 & 1 \\
x_5^6 & x_5^5 & x_5^4 & x_5^3 & x_5^2 & x_5 & 1 \\
x_6^6 & x_6^5 & x_6^4 & x_6^3 & x_6^2 & x_6 & 1 \\
x_7^6 & x_7^5 & x_7^4 & x_7^3 & x_7^2 & x_7 & 1
\end{pmatrix}
\begin{pmatrix} \alpha^3 A_4 \\ \alpha^2 A_3 \\ \alpha A_2 + \alpha^2 A_7 \\ A_1 + \alpha A_6 \\ A_5 + \alpha A_9 \\ A_8 \\ S \end{pmatrix}
\end{aligned}
\tag{38}
$$

が成り立つ．式 (38) の右辺の正方行列は Vandermonde 行列であり正則なので，逆行列が存在する．この逆行列を両辺に左からかけることで，秘密情報 S を復元出来る．□

5.2　2 本の直線上にある場合

定理 5.2　x-y 平面において，7 個のシェア $V_1, V_2, V_3, V_4, V_5, V_6, V_7$ の内，V_1, V_2, V_3, V_4 が原点を通らない直線 $y = ax + b$ 上にあり，V_5, V_6, V_7 が原点を通る直線 $y = cx$ 上にあるとき，7 個のシェアはアクセス集合となる．なお，$a \neq c, b \neq 0$ とする．

（証明）x-y 平面において，7 個のシェア $V_1, V_2, V_3, V_4, V_5, V_6, V_7$ の内，V_1, V_2, V_3, V_4 が原点を通らない直線 $y = ax + b$ 上にあり，V_5, V_6, V_7 が原点を通る直線 $y = cx$ 上にあるとする．なお，$a \neq c, b \neq 0$ とする．この時，$(x_i, y_i), i = 1, 2, 3, 4$ は $y_i = ax_i + b$ を満たす．よって，

$$\begin{aligned} Z_i &= A_1 x_i^3 + A_2 x_i^2 y_i + A_3 x y_i^2 + A_4 y_i^3 + A_5 x_i^2 + A_6 x_i y_i + A_7 y_i^2 + A_8 x_i + A_9 y_i + S \\ &= B_1 x_i^3 + B_2 x_i^2 + B_3 x_i + B_4 \end{aligned} \tag{39}$$

というように，$B_1, \ldots, B_4$ は $A_1, \ldots, A_9, S$ で書くことができる．これより，

$$\begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \\ Z_4 \end{pmatrix} = \begin{pmatrix} x_1^3 & x_1^2 & x_1 & 1 \\ x_2^3 & x_2^2 & x_2 & 1 \\ x_3^3 & x_3^2 & x_3 & 1 \\ x_4^3 & x_4^2 & x_4 & 1 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \end{pmatrix} \tag{40}$$

となる．式 (40) の右辺の正方行列は Vandermonde 行列であり正則なので，逆行列が存在する．この逆行列を両辺に左からかけることで $B_1, \cdots, B_4$ の値を得ることが出来る．よって，シェアの位置が $y = ax + b$ 上であるシェアがとる Z の値がわかる．2 本の直線の交点は $(\frac{b}{c-a}, \frac{bc}{c-a})$ である．この交点に位置するシェア (x_8, y_8, Z_8) を新たに考えると，$x_8 = \frac{b}{c-a}$, $y_8 = \frac{bc}{c-a}$ であるから，$Z_8 = f(\frac{b}{c-a}, \frac{bc}{c-a})$ と求めることができる．

一方，$(x_i, y_i), i = 5, 6, 7$ は $y_i = cx_i$ を満たす．さらに，(x_8, y_8) も同様であることに注意されたい．よって $i = 5, 6, 7, 8$ に対して

$$\begin{aligned} Z_i &= A_1 x_i^3 + A_2 x_i^2 y_i + A_3 x y_i^2 + A_4 y_i^3 + A_5 x_i^2 + A_6 x_i y_i + A_7 y_i^2 + A_8 x_i + A_9 y_i + S \\ &= C_1 x_i^3 + C_2 x_i^2 + C_3 x_i + S \end{aligned} \tag{41}$$

というように，$C_1, \ldots, C_3$ は $A_1, \ldots, A_9$ で書くことができる．これより，

$$\begin{pmatrix} Z_5 \\ Z_6 \\ Z_7 \\ Z_8 \end{pmatrix} = \begin{pmatrix} x_5^3 & x_5^2 & x_5 & 1 \\ x_6^3 & x_6^2 & x_6 & 1 \\ x_7^3 & x_7^2 & x_7 & 1 \\ x_8^3 & x_8^2 & x_8 & 1 \end{pmatrix} \begin{pmatrix} C_1 \\ C_2 \\ C_3 \\ S \end{pmatrix} \tag{42}$$

となる．式 (42) の右辺の正方行列は Vandermonde 行列であり正則なので，逆行列が存在する．この逆行列を両辺に左からかけることで，S の値を求めることができる．□

6　まとめ

本研究では，Shamir の多項式補間法を多変数に拡張した秘密分散法について，2 変数 3 次の場合のアクセス集合の十分条件を調べた．シェアが 7 個および 9 個の場合については，逆行列が存在するのか確かめる必要がある．また，秘密分散法の安全性の観点から，シェアの配り方によって慮外に秘密が復元できてしまうと問題がある．よって，アクセス構造を明らかにすること，つまり秘密情報を復元できる条件とできない条件についてエントロピーを用いて明らかにすることが課題である．

次数や変数の数の一般化が，今後の大きな課題である．

謝辞

この研究を進めるにあたり指導して下さった，西新幹彦准教授に感謝する．

参考文献

[1] A. Shamir, “How to share a secret,” Communications of the ACM, no.22, pp.612–613, Nov. 1979.

[2] 柏倉英明，「2 変数 2 次の多項式補完法による秘密分散法のアクセス構造について」，信州大学工学部，学士論文，2010 年．

[3] 柏倉英明，「2 変数 2 次の多項式補完法による秘密分散法のアクセス構造」，信州大学大学院工学系研究科修士論文，2012 年．

[4] Leonhard Euler,“On an Apparent Contradiction in the Doctrine of Curved Lines,” English translation of “Sur une contradiction apparente dans la doctrine des lignes courbes,” Mémoire de l’Académie des sciences de Berlin , 1750, pp. 219–233,The Eular Archive index number : E147.

付録 A　付録

A.1　2 次曲線の分類について

定理 4.2 において，シェアの位置を x-y 平面上で見て，原点を通る 2 次曲線上にあるかどうかということが一つのポイントとなっていることが分かった．そこで，ここでは 2 次曲線の分類についてまとめる．

平面上の 2 次曲線は，

$$f(x,y) = B_1x^2 + B_2xy + B_3y^2 + B_4x + B_5y + B_6 \tag{43}$$

で表される．2 次曲線が 2 直線でないとき，次が成り立つ．

$B_2^2 - 4B_1B_3 < 0$ のとき，2 次曲線は楕円である．

$B_2^2 - 4B_1B_3 = 0$ のとき，2 次曲線は放物線である．

$B_2^2 - 4B_1B_3 > 0$ のとき，2 次曲線は双曲線である．

また，式 (43) が 2 直線を表す判定条件は，式 (44) で表される．

$$\begin{vmatrix} B_1 & 2B_2 & 2B_4 \\ 2B_2 & B_3 & 2B_5 \\ 2B_4 & 2B_5 & B_6 \end{vmatrix} = 0 \tag{44}$$

式 (43) が因数分解できるとき，これを「可約 2 次曲線」という．また，因数分解できないとき，「既約 2 次曲線」という．可約 2 次曲線は，2 本の直線（重なって 1 本となる場合もある）となる．

A.2　n 次曲線を決定する点の数

今後，多変数多項式を用いた秘密分散法の次数や変数の数の一般化をするにあたり，シェアの位置が n 次曲線上にあるかないか，ということがポイントになると思われる．平面上の n 次曲線を決定するための点の条件として次のことが知られている [4]．

$\frac{n(n+3)}{2}$ 個の独立な点が，n 次の平面代数曲線を決定する．

A.3　4.2 節の補足

表 1 に，2 次曲線 $f(x,y)$ の 2 次の項の各係数 (B_1, B_3, B_5) において，シェアの位置を表す式の各項の内，他の項（表中に $*$ で示した）の線形結合で表すことができる項（表中に//で示した）の組み合わせの一例を示す．

表 1 から，7 個のシェアがすべて 2 次曲線上にあったとき，式 (28) の右辺の 7×10 行列を，7×7 行列の M_7 にすることができることがわかる．

表 1　7 個のシェアがすべて 2 次曲線上にある時の B_1, B_3, B_5 と他の項の線形結合で表すことのできる項の組み合わせの 1 例

B_1	B_3	B_5	x^3	x^2y	xy^2	y^3	x^2	xy	y^2	x	y	1
0	0	B_5	$*$	$*$	//	//	$*$	$*$	//	$*$	$*$	$*$
0	B_3	B_5	//	$*$	$*$	//	$*$	//	$*$	$*$	$*$	$*$
0	B_3	0	$*$	//	//	$*$	$*$	//	$*$	$*$	$*$	$*$
B_1	B_3	0	$*$	//	//	$*$	$*$	//	$*$	$*$	$*$	$*$
B_1	B_3	B_5	//	//	$*$	$*$	//	$*$	$*$	$*$	$*$	$*$
B_1	0	B_5	//	//	$*$	$*$	//	$*$	$*$	$*$	$*$	$*$
B_1	0	0	//	//	$*$	$*$	//	$*$	$*$	$*$	$*$	$*$