

信州大学工学部

学士論文

2変数の多項式補間法による秘密分散法の
アクセス構造について

指導教員 西新 幹彦 准教授

学科 電気電子工学科
学籍番号 06T2802D
氏名 柏倉 英明

2010年3月12日

目次

1	はじめに	1
2	2 変数の多項式補間法のアクセス集合	2
2.1	1 次の場合	2
2.2	2 次の場合	2
3	具体例	4
4	まとめ	5
	謝辞	6
	参考文献	6
	付録 A 場合分け	7
	付録 B 証明	12
B.1	アクセス集合	12
B.2	非アクセス集合	15

1 はじめに

昨今の日本は情報化社会と呼ばれ、多くの情報が行き交っている。そして情報の多くはハードディスクに保管されている。ある情報があったとき、ハードディスクの故障や破壊による情報紛失を防ぐにはコピーを多くとれば良い。しかしコピーを多くとると、それだけ人の手による漏洩の危険性が高まる。この二つの問題を同時に解決する方法として秘密分散法がある。これは秘密情報からシェアと呼ばれる鍵情報を生成し、それらを設定された組み合わせで集めることにより秘密情報を復元するものである、その実現法として Shamir の多項式補間法がある [1]。

Shamir の多項式補間法は、秘密情報が復元できるシェアの個数を k としたとき、ある秘密情報 S について $f(0) = S$ を満たす $k - 1$ 次の多項式 $f(x)$ を考えることで実現できる。各変数の係数はランダムに決定される。多項式からシェア $v_i = f(i)$ を生成し、それらをユーザーに配布する。ここでユーザーが k 人以上集まるとシェアから多項式を復元することができ、秘密情報 S が復元できる仕組みとなっている。またこの多項式の計算は有限体上にて行われる。

この方法ではシェアの個数により秘密情報の復元の可否が決定されるため、しきい値型アクセス構造と呼ばれる。アクセス構造はアクセス集合と非アクセス集合から成り、アクセス集合は秘密情報が復元可能なシェアの組み合わせの集合、非アクセス集合は秘密情報が復元できないシェアの組み合わせの集合である。

またシェアの組み合わせで復元の可否が決定されるものは一般型アクセス構造と呼ばれる。これはしきい値型アクセス構造を用いて、各ユーザーが管理するシェアの個数を調整することで部分的に実現できる。例としてシェアが 6 個あれば秘密情報が復元でき、かつユーザーが A,B,C,D,E の 5 人がいた場合を考える。各ユーザーにそれぞれ 4 個, 2 個, 2 個, 1 個, 1 個のシェアを分配する。このとき秘密情報が復元可能なユーザーの組み合わせは (A,B), (A,C), (A,D,E), (B,C,D,E) の 4 通りである。この例では A がいれば比較的少人数で秘密が復元できる代わりに、A は他のユーザーより多くのシェアを管理する必要がある。言い換えればこの方法では重要なユーザーは多くのシェアを管理しなければならない。

ところが 2 変数の多項式補間法を用いると、全てのユーザーが管理するシェアをそれぞれ 1 個としたままで一般型アクセス構造が実現可能になる。例えば、ある 8 個のシェアがあったとき、 (v_1, v_2, v_3) , $(v_1, v_2, v_4, v_5, v_6)$, $(v_1, v_3, v_4, v_5, v_7, v_8)$, $(v_1, v_3, v_4, v_6, v_7, v_8)$, $(v_1, v_3, v_5, v_6, v_7, v_8)$, $(v_1, v_4, v_5, v_6, v_7, v_8)$, $(v_3, v_4, v_5, v_6, v_7, v_8)$ を部分集合に含むシェアの集合がアクセス集合として実現可能である。本研究は 2 変数の多項式補間法について考察し、そのアクセス構造を解析することを目的とする。本稿では特に $f(x, y) = Ax + By + S$ のような 2 変数 1 次の多項式と、 $f(x, y) = ax^2 + bx + cxy + dy + ey^2 + S$ のような 2 変数 2 次の多項式について考察する。

ここで従来研究について少し触れておく．所望の一般型アクセス構造を実現する方法として [2] が知られている．一方，本研究にて考える方法は一部のアクセス構造しか実現できないが，直観的に分かりやすいものとなっている．この点が本研究の意義である．

2 2変数の多項式補間法のアクセス集合

2変数の多項式補間法を考えると，シェアは $v_i = (x_i, y_i, z_i)$ といった形で表される．ここで $z_i = f(x_i, y_i)$ である．また (x_i, y_i) をシェアの位置と呼ぶ．シェアの位置をどのように選ぶかで復元可能なシェアの組み合わせや個数が変化する点が，2変数の多項式補間を考える際の大きな特徴である．以下にどのようなアクセス集合が実現可能か示す．便宜上，ユークリッド空間での説明に見えるが，実際は位数の大きい有限体上にて考えている．シェアの場合分け，およびそれらの場合の秘密情報の復元の可否についての証明は付録に示す．

2.1 1 次の場合

この節では多項式 $f(x, y) = Ax + By + S$ について考察する．秘密情報が復元可能なシェアの組み合わせを以下に示す．

- (1) ある 3 個のシェアがあり，それら全てが x - y 平面にて直線上にならなないとき
- (2) ある 2 個のシェアがあり，それら全てが x - y 平面にて原点を通る直線上に並んでいるとき

上記の組み合わせを部分集合に含むシェアの組み合わせが，2変数 1 次の多項式補間法におけるアクセス集合である．

$f(x, y) = Ax + By + S$ で表される面は平面である．平面は直線上にならなない 3 点があれば決定される．このことから，直線上にない 3 個のシェアがあれば秘密情報を復元できる．

次に，上記の平面の断面について考えると，それは直線で表される．このことから， x - y 平面の原点を通る直線上の 2 個のシェアがあれば秘密情報が復元できる．

ここで注意すべき点は，シェアが 3 個以上集まっても，それら全てが原点を通らない直線上にあるとき，秘密情報は復元できないことである．このことに注意しなければ，本来ならアクセス集合としたいシェアの組み合わせが非アクセス集合となってしまう可能性がある．

2.2 2 次の場合

次は多項式 $f(x, y) = ax^2 + bx + cxy + dy + ey^2 + S$ について考える．秘密情報 S を復元可能なシェアの組み合わせを以下に示す．

- (1) ある 3 個のシェアがあり，それら全てが x - y 平面にて原点を通る直線上にあるとき
- (2) ある 5 個のシェアがあり，そのうち 2 個の位置が x - y 平面にて原点を通る直線上にあり，他の 3 個が原点を通らない直線上にあり，この 2 つの直線の交点にはシェアがないとき
- (3) ある 5 個のシェアがあり，それら全てが x - y 平面にて原点を通る二次曲線上にあるとき
- (4) ある 6 個のシェアについて，次に示す行列 V がフルランクのとき

$$V = \begin{pmatrix} x_1^2 & x_1 & x_1 y_1 & y_1 & y_1^2 & 1 \\ x_2^2 & x_2 & x_2 y_2 & y_2 & y_2^2 & 1 \\ x_3^2 & x_3 & x_3 y_3 & y_3 & y_3^2 & 1 \\ x_4^2 & x_4 & x_4 y_4 & y_4 & y_4^2 & 1 \\ x_5^2 & x_5 & x_5 y_5 & y_5 & y_5^2 & 1 \\ x_6^2 & x_6 & x_6 y_6 & y_6 & y_6^2 & 1 \end{pmatrix} \quad (1)$$

上記の組み合わせを部分集合に含むシェアの組み合わせが，2 変数 2 次の多項式補間法におけるアクセス集合である．

$f(x, y) = ax^2 + bx + cxy + dy + ey^2 + S$ で表される面は二次曲面と呼ばれる．この多項式は項が 6 つあるので，シェアが 6 個集まれば秘密情報が復元出来る．ここで式 (1) に示す行列 V がフルランクにならない場合とは，冗長なシェアがある場合，全てのシェアが原点を通らない 2 直線上のどこかにある場合である．冗長なシェアについては後に触れる．

次に二次曲面の断面を考えてみると，それは二次曲線で表される．このことから， x - y 平面の原点を通る直線上のシェアが 3 個あれば秘密情報が復元できる．

また二次曲線はグラフ上の点が 3 つ与えられれば式を復元できることから，2 変数 2 次の多項式補間にて， x - y 平面上のある直線上のシェアが 3 個集まれば，その直線上の任意の位置のシェアを得られることが言える．このことから，ある 5 個のシェアについて，そのうち 2 個の位置が x - y 平面にて原点を通る直線上にあり，他の 3 個が原点を通らない直線上にあり，この 2 つの直線の交点にはシェアがないときも秘密情報が復元できることが言える．またこれに関連して，ある直線上のシェアが 4 個より多く集まると，それらは冗長なシェアになってしまう点には注意が必要である．

また x と y に媒介変数 t を用いて，2 変数の多項式を 1 変数の多項式とした場合を考えてみる．ある 5 個のシェアが x - y 平面にて原点を通る 2 次曲線上にあると秘密情報を復元できる．またこのことから，ある二次曲線上のシェアが 5 個あれば，その曲線上の任意の位置のシェアを得られることが言える．よって，ある二次曲線上のシェアが 5 個より多くあると，それらは冗長なシェアとなる．

以上が，2 変数 1 次と 2 変数 2 次の多項式補間において秘密情報が復元可能なシェアの組み合わせである．これらの組み合わせを部分集合に含むシェアの集合が，2 変数の多項式補間のアクセス集合である．非アクセス集合の証明については付録 B にて述べる．

3 具体例

この節では今までの内容を踏まえ、具体的にどのようなアクセス構造が実現可能か例を示す。

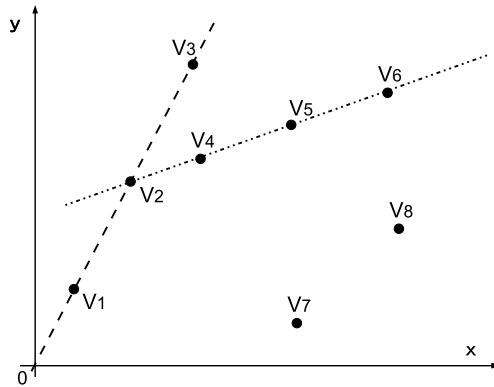


図 1 具体例 1

まずは図 1 に示すような 8 個のシェアが与えられた場合のアクセス構造について解説する。前節で述べた 4 つの場合について、場合 (1)、場合 (2)、場合 (3)、場合 (4) の順に、その条件を満たすシェアの組み合わせがあるかを探していくことがアクセス集合を探す上で合理的な手順だと思われる。

図 1 を見てみると、原点を通る直線上に v_1, v_2, v_3 の 3 個が並んでいる。また v_4, v_5, v_6 の 3 個は原点を通らない直線上にあり、二つの直線の交点には v_2 がある。以上のことからまず、場合 (1) より (v_1, v_2, v_3) 、場合 (2) より $(v_1, v_3, v_4, v_5, v_6)$ が秘密情報を復元可能な組み合わせとしてあげられる。 v_7, v_8 はどちらの直線上にもなく、また各々と原点を結んだ直線上に他のシェアは存在しない。このことから場合 (4) より V がフルランクになる条件に気をつけつつシェアを選ぶと $(v_1, v_3, v_4, v_5, v_7, v_8)$, $(v_1, v_3, v_4, v_6, v_7, v_8)$, $(v_1, v_3, v_5, v_6, v_7, v_8)$, $(v_1, v_4, v_5, v_6, v_7, v_8)$, $(v_3, v_4, v_5, v_6, v_7, v_8)$ もあげられる。以上より、図 1 のようにシェアを選んだときは、上記の 7 つの組み合わせを部分集合として含む集合がアクセス集合である。この例ではまず v_1 または v_3 は必須となっており、そこに v_2 か v_4, v_5, v_6 の 3 個が必要であり、さらに v_1, v_3, v_4, v_5, v_6 のうち 1 個が欠けていても v_7, v_8 があれば復元可能となっている。

次に特殊な例として図 2 のようなシェアのとり方について説明する。シェアは全部で k 個あり、どの 2 個も原点を通る直線上になく、ある 3 個が直線上にならんだ時、その直線は l_1, l_2, l_3 のいずれかであるとする。1 人につき 1 個のシェアを持ち、直線 l_1 上のシェアを持つ人達を A グループ、直線 l_2 上のシェアを持つ人達を B グループ、直線 l_3 上のシェアを持つ人達

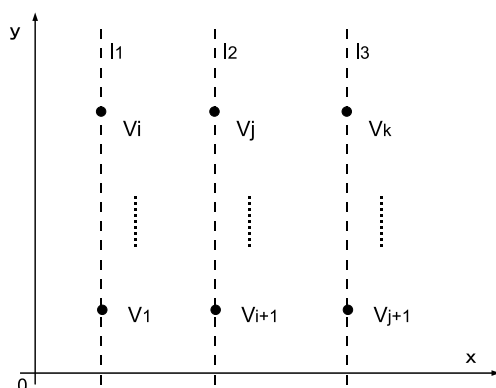


図2 具体例2

を C グループとする．どの2点も原点を通る直線上にないので場合(1)と場合(2)はここでは使用できない．また全てのシェアがとる x の値が3通りしかないので場合(3)も適用できない．よってこの例では場合(4)を満たすようにシェアを取ることがアクセス構造を調べることに繋がる．場合(4)では，同じ直線上にならぶシェアは4個目以降は冗長であること，集まった6個のシェア全てがある2つの直線上のどちらかにあるときは行列 V がフルランクにならないことが制約となっている．そのため秘密情報を復元するには最低6人集まる必要があり，かつそれぞれのグループから1人，2人，3人が集まった場合か，全グループから2人ずつ集まった場合のどちらかに限られる．この2つの条件のどちらかを満たすようなシェアの組み合わせを部分集合に持つ集合が，図2に示した例のアクセス集合である．この例では，ある1グループが何人そろっても秘密情報は復元できない．このように何人集まっても秘密情報が復元できない組み合わせが存在する点は，2変数の多項式補間法を考えるうえで大きなメリットである．

4 まとめ

2変数1次の多項式と2変数2次の多項式を用いた多項式補間方について考察し，アクセス構造を解析した．

今後の課題は，まずシェアを与えたときに復元可否の判定や秘密情報を復元するアルゴリズムの作成が挙げられる．またより大きな次数について解析をすること，所望のアクセス構造を満たすような多項式あるいはシェアの位置を選択するアルゴリズムの作成も大きな課題である．

謝辞

本研究を行うにあたり，丁寧な指導をしてくださった西新幹彦准教授に感謝の意を表する．

参考文献

- [1] A.Shamir, “How to share a secret”, Communications of the ACM, 22, pp.612-613, Nov.1979.
- [2] 岩本 貢, 山本 博資, 「一般型アクセス構造に対する強い秘密保護特性をもつランブ型秘密分散方」, 第 27 回情報理論とその応用シンポジウム予稿集, pp331-334, 2004.

付録 A 場合分け

この項では、2 変数 2 次の多項式補間におけるシェアの選び方の場合分けを示す。

シェアが 2 個の場合

要素 $A \cdots$ 原点を通る直線上に 2 個のシェアがある A が成り立つかどうかだけで場合分けが出来る。よってシェアが 2 個の場合は、以下の 2 つのどちらかになる。

1. (A) ある 2 個が原点を通る直線上にある $\cdots$ 証明 9 より非アクセス集合であることが言えた。
2. $(\bar{A})$ どの 2 点も原点を通る直線上にない $\cdots$ どの 3 個も原点を通る直線上にならないように新たにシェアを与えると、それはシェアが 3 個与えられたときの場合 (3) に帰着する。そのとき秘密情報は復元できないので、シェアを新たに与える前の場合でも秘密情報は復元できないことが言えた。

シェアが 3 個の場合

要素 $A \cdots$ ある 3 個が原点を通る直線上にある

要素 $B \cdots$ ある 3 個が原点を通らない直線上にある

要素 $C \cdots$ ある 2 個が原点を通る直線上にある

ここで A と B 、 B と C はそれぞれ同時に成立せず、 A は C を含んでいる。よって、シェアが 3 個の場合分けは以下ようになる。

1. $(A, \bar{B}, C)$ ある 3 個が原点を通る直線上にある $\cdots$ 証明 3 よりアクセス集合であることが言えた。
2. $(\bar{A}, B, \bar{C})$ ある 3 個が原点を通らない直線上にある $\cdots$ 3 個のうち 1 個を選び、そのシェアと原点を結ぶ直線上にシェアを与えることで、シェアが 4 個与えられたときの場合 (4) に帰着する。そのとき秘密情報は復元できないので、シェアを与える前の状態でも秘密情報は復元できないことが言えた。
3. $(\bar{A}, \bar{B}, C)$ ある 2 個が原点を通る直線上にある $\cdots$ 2 組の 2 個が原点を通る直線上にならないように、新たにシェアを与えた場合を考える。そのとき、シェアが 4 個集まったときの場合 (1) に帰着する。そのとき秘密情報は復元できないので、シェアを与える前の場合でも秘密情報は復元できないことが言えた。
4. $(\bar{A}, \bar{B}, \bar{C})$ どの 2 個も原点を通る直線上になく、どの 3 個も直線上にならんでいない $\cdots$ ある 2 個が原点を通る直線上に並ぶように新たにシェアを与えることで、シェアが 4 個集まったときの場合 (1) に帰着する。そのとき秘密情報は復元できないので、シェアを与える前の場合でも秘密情報は復元できないことが言えた。

シェアが 4 個の場合

要素 $A \cdots$ ある 2 個が原点を通る直線上にある

要素 $B \cdots$ ある 2 組の 2 個が、それぞれ原点を通る 2 つの直線上にある

要素 $C \cdots$ ある 3 個が原点を通る直線上にある

要素 $D \cdots$ ある 3 個が原点を通らない直線上にある

要素 $E \cdots$ 全てのシェアが原点を通る二次曲線上にある

ここで E は他のどれとも同時に成立しない。また B と C と D は同時に二つ以上成立しない。

また B と C は A を含んでいる。よって、シェアが 4 個の場合分けは以下になる。

1. $(A, \bar{B}, \bar{C}, \bar{D}, \bar{E})$ ある 2 個が原点を通る直線上にあり、他のどの 2 個も原点を通る直線上にない $\cdots$ どの 3 個も直線上に並ばないようにシェアを与えると、証明 7 に帰着する。証明 7 の場合では秘密情報は復元できないので、そこからシェアを 1 個減らした場合を考えても秘密情報は復元できないことが言えた。
2. $(A, B, \bar{C}, \bar{D}, \bar{E})$ ある 2 組の 2 個が原点を通る直線上にあり、他のどの 2 個の組も原点を通る直線上にない $\cdots$ どの 3 個も直線上に並ばないようにシェアを与えると、証明 7 に帰着する。証明 7 の場合では秘密情報は復元できないので、そこからシェアを 1 個減らした場合を考えても秘密情報は復元できないことが言えた。
3. $(A, \bar{B}, \bar{C}, \bar{D}, \bar{E})$ ある 3 個が原点を通る直線上にある $\cdots$ 証明 3 よりアクセス集合であることが言えた。
4. $(A, \bar{B}, \bar{C}, D, \bar{E})$ ある 2 個が原点を通る直線上にあり、ある 3 個が原点を通らない直線上にあり、2 直線の交点にシェアがある $\cdots$ どの 4 個も直線上に並ばず、かつどの 3 個も原点を通る直線上にないように新しいシェアを与えることで、証明 7 に帰着する。証明 7 の場合では秘密情報は復元できないので、そこからシェアを 1 個減らした場合を考えても秘密情報は復元できないことが言えた。
5. $(\bar{A}, \bar{B}, \bar{C}, D, \bar{E})$ どの 2 個も原点を通る直線上になく、ある 3 個が原点を通らない直線上にある $\cdots$ 原点を通らない直線上に並ぶ 3 点のうち一点を選び、そのシェアと原点をむすぶ直線上に新しいシェアを与えることで、証明 7 の場合に帰着する。証明 7 の場合では秘密情報は復元できないので、そこからシェアを 1 個減らした場合を考えても秘密情報は復元できないことが言えた。
6. $(\bar{A}, \bar{B}, \bar{C}, \bar{D}, \bar{E})$ どの 2 個も原点を通る直線上になく、どの 3 個も直線上にない $\cdots$ ある 2 個が原点を通る直線上に並ぶように新しいシェアを与えることで証明 7 の場合に帰着する。証明 7 の場合では秘密情報は復元できないので、そこからシェアを 1 個減らした場合を考えても秘密情報は復元できないことが言えた。
7. (E) 4 個のシェアが原点を通る二次曲線上にある $\cdots$ 証明 8 より非アクセス集合であることが言えた。

シェアが 5 個の場合

要素 $A \cdots$ ある 2 個が原点を通る直線上にある

要素 $B \cdots$ ある 2 組の 2 個が、それぞれ原点を通る 2 つの直線上にある

要素 $C \cdots$ ある 3 個が原点を通る直線上にある

要素 $D \cdots$ ある 3 個が原点を通らない直線上にある

要素 $E \cdots$ 全てのシェアが原点を通る二次曲線上にある

ここで E は他のどれとも同時に成立しない．また B と C は A を含む．よって、シェアが 5 個の場合分けは以下のようになる．

1. $(A, \bar{B}, \bar{C}, \bar{D}, \bar{E})$ ある 2 個が原点を通る直線上にあり、どの 3 個も直線上にない $\cdots$ 証明 7 より非アクセス集合であることが言えた．
2. $(A, \bar{B}, \bar{C}, \bar{D}, \bar{E})$ ある 2 個が原点を通る直線上にあり、他の 3 個が原点を通らない直線上にある $\cdots$ 証明 4 から、証明 3 の場合に帰着できるのでアクセス集合であることが言えた．
3. $(A, B, \bar{C}, \bar{D}, \bar{E})$ ある 2 組の 2 個が原点を通る直線上にある $\cdots$ 証明 7 より非アクセス集合であることが言えた．
4. $(A, B, \bar{C}, \bar{D}, \bar{E})$ ある 2 組の 2 個が原点を通る直線上にあり、かつ、どの 3 個も線上にない $\cdots$ 証明 7 より非アクセス集合であることが言えた．
5. $(A, B, C, \bar{D}, \bar{E})$ ある 2 組の 2 個が原点を通る直線上にあり、かつ、ある 3 個が原点を通らない直線上にある $\cdots$ 証明 7 より非アクセス集合であることが言えた．
6. (A, B, C, D) ある 2 組の 2 個が原点を通る直線上にあり、かつ、ある 3 個が原点を通る直線上にあり、かつ、ある 3 個が原点を通らない直線上にある $\cdots$ 原点を通る直線上の 3 個のシェアから、証明 3 に帰着し、アクセス集合であることが言えた．
7. $(A, \bar{B}, C, \bar{D}, \bar{E})$ ある 3 個が原点を通る直線上にあり、他のどの 3 個も直線上にない $\cdots$ 原点を通る直線上の 3 個のシェアから、証明 3 に帰着し、アクセス集合であることが言えた．
8. $(A, \bar{B}, C, D, \bar{E})$ ある 3 個が原点を通る直線上にあり、かつ、ある 3 個が原点を通らない直線上にあり、その 2 つの直線の交点にはシェアがある $\cdots$ 原点を通る直線上の 3 個のシェアから、証明 3 に帰着し、アクセス集合であることが言えた．
9. $(\bar{A}, \bar{B}, \bar{C}, D, \bar{E})$ どの 2 個も原点を通る直線上になく、ある 3 個が原点を通る直線上にある $\cdots$ 原点を通る直線上の 3 個のシェアから、証明 3 に帰着し、アクセス集合であることが言えた．
10. $(\bar{A}, \bar{B}, \bar{C}, \bar{D}, \bar{E})$ どの 2 個も原点を通る直線上になく、どの 3 個も直線上にない $\cdots$ 秘密情報 S をある任意の値としたとき、それを満たす多項式の係数が一意に決定され、これは S がとる全ての値について同様に確かである．よってこの場合では秘密情報が決定

されないため、非アクセス集合であることが言えた。

11. (E)5 個のシェアが原点を通る二次曲線上にある … 証明 5 よりアクセス集合であることが言えた。

シェアが 6 個の場合

要素 $A \cdots$ ある 2 個が原点を通る直線上にある

要素 $B \cdots$ ある 2 組の 2 個が、それぞれ原点を通る 2 つの直線上にある

要素 $C \cdots$ ある 3 組の 2 個が、それぞれ原点を通る 3 つの直線上にある

要素 $D \cdots$ ある 3 個が原点を通る直線上にある

要素 $E \cdots$ ある 2 組の 3 個が、それぞれ原点を通る 2 つの直線上にある

要素 $F \cdots$ ある 3 個が原点を通らない直線上にある

要素 $G \cdots$ ある 2 組の 3 個が、それぞれ原点を通らない 2 つの直線上にある

要素 $H \cdots$ ある 5 個のシェアだけが原点を通る二次曲線上にある

要素 $I \cdots$ 全てのシェアが原点を通らない二次曲線上にある

ここで H と I はそれぞれ他のどれとも同時に成立しない。また B は A を含み、 C は B と A を含み、 D は A を含み、 E は A と B と D を含み、 G は F を含む。また C が成立したとき D と E は成立せず、 D が成立したとき C と G は成立せず、 E が成立したとき C と F と G は成立せず、 F が成立したとき E は成立せず、 G が成立したとき D と E は成立しない。

以上より、 A 及び $\bar{A}$ について F と G を変化させた場合、 B について D と F と G を変化させた場合、 C について F と G を変化させた場合、 D について F を変化させた場合、 E が成立した場合、 H が成立した場合、 I が成立した場合についてそれぞれ場合分けを行った。ここで、場合 (2)、場合 (6)、場合 (8)、場合 (9)、場合 (15)、場合 (16)、場合 (17)、場合 (18)、場合 (19) を除く全ての場合は式 (1) に示した行列 V がフルランクになるものとし、証明は省略した。

1. $(A, \bar{B}, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ ある 2 個だけが原点を通る直線上にあり、どの 3 個も直線上にない
2. $(A, \bar{B}, \bar{C}, \bar{D}, \bar{E}, F, \bar{G}, \bar{H}, \bar{I})$ ある 2 個だけが原点を通る直線上にあり、他のある 3 個が原点を通らない直線上にある … シェアが 5 個与えられたときの場合 (2) に帰着するため、アクセス集合であることが言えた。
3. $(A, \bar{B}, \bar{C}, \bar{D}, \bar{E}, F, G, \bar{H}, \bar{I})$ ある 2 個が原点を通る直線上にあり、かつ、ある 2 組の 3 個が原点を通らない直線上にある
4. $(\bar{A}, \bar{B}, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ どの 2 個も原点を通る直線上になく、どの 3 個も直線上にない
5. $(\bar{A}, \bar{B}, \bar{C}, \bar{D}, \bar{E}, F, \bar{G}, \bar{H}, \bar{I})$ どの 2 個も原点を通る直線上になく、ある 3 個が原点を通らない直線上にある
6. $(\bar{A}, \bar{B}, \bar{C}, \bar{D}, \bar{E}, F, G, \bar{H}, \bar{I})$ どの 2 個も原点を通る直線上になく、ある 2 組の 3 個が原点

を通らない直線上にある … 証明 6 より非アクセス集合であることが言えた .

7. $(A, B, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ ある 2 組の 2 個がそれぞれ原点を通る 2 つの直線上にあり , どの 3 個も直線上にない
8. $(A, B, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ ある 2 組の 2 個がそれぞれ原点を通る 2 つの直線上にあり , かつ , ある 3 個が原点を通る直線上にある … 原点を通る直線上にある 3 個についてシェアを 3 個与えたときの場合 (1) に帰着できることから , アクセス集合であることが言えた .
9. $(A, B, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ ある 2 組の 2 個がそれぞれ原点を通る 2 つの直線上にあり , かつ , ある 3 個が原点を通らない直線上にあり , かつ , ある 3 個が原点を通る直線上にある … 原点を通る直線上にある 3 個についてシェアを 3 個与えたときの場合 (1) に帰着できることから , アクセス集合であることが言えた .
10. $(A, B, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ ある 2 組の 2 個がそれぞれ原点を通る 2 つの直線上にあり , かつ , ある 3 個が原点を通らない直線上にある
11. $(A, B, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ ある 2 組の 2 個がそれぞれ原点を通る 2 つの直線上にあり , かつ , ある 2 組の 3 個が原点を通らない直線上にある
12. $(A, B, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ ある 3 組の 2 個がそれぞれ原点を通る 3 つの直線上にある
13. $(A, B, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ ある 3 組の 2 個がそれぞれ原点を通る 3 つの直線上にあり , かつ , ある 3 個が原点を通らない直線上にある
14. $(A, B, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ ある 3 組の 2 個がそれぞれ原点を通る 3 つの直線上にあり , かつ , ある 2 組の 3 個がそれぞれ原点を通らない直線上にある
15. $(A, \bar{B}, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ ある 3 個が原点を通る直線上にある … 原点を通る直線上にある 3 個についてシェアを 3 個与えたときの場合 (1) に帰着できることから , アクセス集合であることが言えた .
16. $(A, \bar{B}, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ ある 3 個が原点を通る直線上にあり , ある 3 個が原点を通らない直線上にある … 原点を通る直線上にある 3 個についてシェアを 3 個与えたときの場合 (1) に帰着できることから , アクセス集合であることが言えた .
17. $(A, B, \bar{C}, \bar{D}, \bar{E}, \bar{F}, \bar{G}, \bar{H}, \bar{I})$ 2 組の 3 個が , それぞれ原点を通る 2 つの直線上にある … 原点を通る直線上にある 3 個についてシェアを 3 個与えたときの場合 (1) に帰着できることから , アクセス集合であることが言えた .
18. (H) 5 個のシェアが原点を通る二次曲線上にある … 証明 5 より , アクセス集合であることが言えた .
19. (I) 全てのシェアが原点を通らない二次曲線上にある場合 … 証明 10 より , 6 個のシェアのうち 1 個が冗長なシェアであることが言えるので , 式 (1) はフルランクにならない . よって非アクセス集合であることが言えた .

付録 B 証明

B.1 アクセス集合

この節では、2 変数 1 次の場合のアクセス集合と、2 変数 2 次の場合のアクセス集合の証明を行う。

証明 1

1 次の多項式補間法にて直線上にない 3 個のシェアが与えられたとき秘密情報が復元できることを証明する。3 個のシェアは直線上にはないので、それぞれの位置について

$$(x_2 - x_1)(y_3 - y_1) - (x_3 - x_1)(y_2 - y_1) \neq 0 \quad (2)$$

が言える。ここで次のような行列を考える。

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix} \begin{pmatrix} A \\ B \\ S \end{pmatrix} \quad (3)$$

右辺第一項の行列式を考えると

$$\begin{aligned} \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} &= \begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ 1 & 1 & 1 \end{vmatrix} = \begin{vmatrix} 0 & x_2 - x_1 & x_3 - x_1 \\ 0 & y_2 - y_1 & y_3 - y_1 \\ 1 & 1 & 1 \end{vmatrix} \\ &= \begin{vmatrix} x_2 - x_1 & x_3 - x_1 \\ y_2 - y_1 & y_3 - y_1 \end{vmatrix} \\ &= (x_2 - x_1)(y_3 - y_1) - (x_3 - x_1)(y_2 - y_1) \end{aligned} \quad (4)$$

である。式 (2) より式 (4) の値は非零なので、式 (3) の両辺に右辺第一項の行列の逆行列を左からかけることで S の値を得られる。□

証明 2

2 変数 1 次の多項式補間を考えたとき、 x - y 平面にて原点を通る直線上にある 2 個のシェアが与えられたとき、秘密情報を復元できることを証明する。2 個のシェアは x - y 平面の原点を通る直線上の位置にあるので、媒介変数 t を用いて

$$x_i = \alpha t_i, y_i = \beta t_i$$

と表せる。また

$$t_1 \neq t_2 \quad (5)$$

このことから

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} \alpha t_1 & \beta t_1 & 1 \\ \alpha t_2 & \beta t_2 & 1 \end{pmatrix} \begin{pmatrix} A \\ B \\ S \end{pmatrix} = \begin{pmatrix} t_1 & 1 \\ t_2 & 1 \end{pmatrix} \begin{pmatrix} A\alpha + B\beta \\ S \end{pmatrix} \quad (6)$$

を得る．式 (5) より式 (6) 右辺第一項の行列は正則である．そのため，式 (6) 右辺第一項の行列の逆行列を両辺に左からかけることで S の値を得られる．□

証明 3

2 変数 2 次の多項式補間を考えたとき， x - y 平面上にで原点を通る直線上の 3 個のシェアが集まれば秘密情報が復元できることを証明する．ある 3 個のシェアがあり，それらは全て x - y 平面にて原点を通る直線上の位置にあるので

$$x_i = \alpha t_i, y_i = \beta t_i$$

と表せる．また

$$t_1 \neq t_2, t_1 \neq t_3, t_2 \neq t_3 \quad (7)$$

である．ある z_i について

$$\begin{aligned} z_i &= a(\alpha t_i)^2 + b(\alpha t_i) + c(\alpha t_i)(\beta t_i) + d(\beta t_i) + e(\beta t_i)^2 + S \\ &= (a\alpha^2 + c\alpha\beta + e\beta^2)t_i^2 + (b\alpha + d\beta)t_i + S \\ &= At_i^2 + Bt_i + S \end{aligned}$$

と書き表せる．集まった 3 個のシェアについて

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} t_1^2 & t_1 & 1 \\ t_2^2 & t_2 & 1 \\ t_3^2 & t_3 & 1 \end{pmatrix} \begin{pmatrix} A \\ B \\ S \end{pmatrix} \quad (8)$$

を得られ，式 (8) 右辺第一項の行列は vandermonde の行列で，その値は式 (7) より非零である．よって S の値を得ることができる．□ このシェアの取り方を部分集合に含む場合は，全てアクセス集合である．したがってシェアを 3 個与えた場合の 1，シェアを 4 個与えた場合の 3，シェアを 5 個与えた場合の 6，7，8，9 はアクセス集合である．

証明 4

2 変数 2 次の多項式補間法にて 3 個のシェアが直線上にあったとき，その直線上の任意の位置のシェアを得られることを証明する． x - y 平面上のある直線上にある 3 個のシェアが集まったとき

$$x_i = \alpha_x t_i + \beta_x \quad (9)$$

$$y_i = \alpha_y t_i + \beta_y \quad (10)$$

を満たす $\alpha_x, \beta_x, \alpha_y, \beta_y$ を得られる．ここで $(\alpha_x, \alpha_y) \neq (0, 0)$ である．式 (9), (10) を多項式 $f(x, y)$ に代入すると，

$$\begin{aligned}
z_i &= a(\alpha_x t_i + \beta_x)^2 + b(\alpha_x t_i + \beta_x) + c(\alpha_x t_i + \beta_x)(\alpha_y t_i + \beta_y) \\
&\quad + d(\alpha_y t_i + \beta_y) + e(\alpha_y t_i + \beta_y)^2 + S \\
&= t_i^2(a\alpha_x^2 + c\alpha_x\alpha_y + e\alpha_y^2) \\
&\quad + t_i(2a\alpha_x\beta_x + b\alpha_x + c\alpha_x\beta_y + c\alpha_y\beta_x + d\alpha_y + 2e\alpha_y\beta_y) \\
&\quad + (a\beta_x^2 + b\beta_x + c\beta_x\beta_y + d\beta_y + e\beta_y^2 + S) \\
&= At_i^2 + Bt_i + C
\end{aligned} \tag{11}$$

と書き表せる．このとき証明 3 より， A, B, C を得られることが言える．式 (11) は t の関数となっており，式 (9), (10) から今考えている直線上の任意の位置の t_i を得ることで，その位置の z_i の値を得ることが出来る．□

証明 5

2 変数 2 次の多項式補間にて， x - y 平面の原点を通る二次曲線上にある 5 個のシェアが集まったとき，秘密情報が復元できることを証明する．ある 5 個のシェアがあり，その位置は

$$x_i = t_i, y = \alpha t_i^2 + \beta t_i$$

を満たす．これを多項式 $f(x, y)$ に代入すると

$$\begin{aligned}
z_i &= at_i^2 + bt_i + ct_i(\alpha t_i^2 + \beta t_i) + d(\alpha t_i^2 + \beta t_i) + e(\alpha t_i^2 + \beta t_i)^2 + S \\
&= at_i^2 + bt_i + c\alpha t_i^3 + c\beta t_i^2 + d\alpha t_i^2 + d\beta t_i + e\alpha^2 t_i^4 + 2e\alpha\beta t_i^3 + e\beta^2 t_i^2 + S \\
&= t_i^4(e\alpha^2) + t_i^3(c\alpha + 2e\alpha\beta) + t_i^2(a + c\beta + d\alpha + e\beta) \\
&\quad + t_i(b + d\beta) + S \\
&= At_i^4 + Bt_i^3 + Ct_i^2 + Dt_i + S
\end{aligned} \tag{12}$$

となる．集まった 5 個のシェアと式 (12) から

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \end{pmatrix} = \begin{pmatrix} t_1^4 & t_1^3 & t_1^2 & t_1 & 1 \\ t_2^4 & t_2^3 & t_2^2 & t_2 & 1 \\ t_3^4 & t_3^3 & t_3^2 & t_3 & 1 \\ t_4^4 & t_4^3 & t_4^2 & t_4 & 1 \\ t_5^4 & t_5^3 & t_5^2 & t_5 & 1 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \\ D \\ S \end{pmatrix} \tag{13}$$

を得る．式 (13) の右辺第一項の行列は vandermonde の行列から正則である．よって S の値を得ることが出来る．□

B.2 非アクセス集合

この節では 2 変数 2 次の多項式補間法において，先に証明した場合以外は非アクセス集合であることを証明する．

証明 6

2 変数 2 次の多項式補間法にて 6 個のシェアが与えられたとき，そのうち 3 個が原点を通らない直線上にあり，他の 3 個も原点を通らない別の直線上にあったとき，秘密情報が復元できないことを証明する．まず原点を通らない直線上のシェアの位置について媒介変数 t を用いて

$$x = \alpha_x t + \beta_x, y = \alpha_y t + \beta_y$$

が言える．このことから，6 個のシェアの位置を

$$x_i = \alpha_{x1} t_i + \beta_{x1}, y_i = \alpha_{y1} t_i + \beta_{y1} \quad i = 1, 2, 3 \quad (14)$$

$$x_j = \alpha_{x2} t_j + \beta_{x2}, y_j = \alpha_{y2} t_j + \beta_{y2} \quad j = 4, 5, 6 \quad (15)$$

と表せる．ここで t_1 から t_6 は全て異なる値を持ち，かつ非零である．式 (14) と式 (15) より，それぞれ z_1, z_2, z_3 と z_4, z_5, z_6 について

$$\begin{aligned} z_i &= a(\alpha_{x1} t_i + \beta_{x1})^2 + b(\alpha_{x1} t_i + \beta_{x1}) + c(\alpha_{x1} t_i + \beta_{x1})(\alpha_{y1} t_i + \beta_{y1}) \\ &\quad + d(\alpha_{y1} t_i + \beta_{y1}) + e(\alpha_{y1} t_i + \beta_{y1})^2 + S \\ &= t_i^2 (a\alpha_{x1}^2 + c\alpha_{x1}\alpha_{y1} + e\alpha_{y1}^2) \\ &\quad + t_i (2a\alpha_{x1}\beta_{x1} + b\alpha_{x1} + c\alpha_{x1}\beta_{y1} + c\alpha_{y1}\beta_{x1} + d\alpha_{y1} + 2e\alpha_{y1}\beta_{y1}) \\ &\quad + (a\beta_{x1}^2 + b\beta_{x1} + c\beta_{x1}\beta_{y1} + d\beta_{y1} + e\beta_{y1}^2 + S) \end{aligned} \quad (16)$$

$$\begin{aligned} z_j &= a(\alpha_{x2} t_j + \beta_{x2})^2 + b(\alpha_{x2} t_j + \beta_{x2}) + c(\alpha_{x2} t_j + \beta_{x2})(\alpha_{y2} t_j + \beta_{y2}) \\ &\quad + d(\alpha_{y2} t_j + \beta_{y2}) + e(\alpha_{y2} t_j + \beta_{y2})^2 + S \\ &= t_j^2 (a\alpha_{x2}^2 + c\alpha_{x2}\alpha_{y2} + e\alpha_{y2}^2) \\ &\quad + t_j (2a\alpha_{x2}\beta_{x2} + b\alpha_{x2} + c\alpha_{x2}\beta_{y2} + c\alpha_{y2}\beta_{x2} + d\alpha_{y2} + 2e\alpha_{y2}\beta_{y2}) \\ &\quad + (a\beta_{x2}^2 + b\beta_{x2} + c\beta_{x2}\beta_{y2} + d\beta_{y2} + e\beta_{y2}^2 + S) \end{aligned} \quad (17)$$

を得る．式 (16) と式 (17) より 6 個のシェアについて次のような行列を得る．

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \end{pmatrix} = \begin{pmatrix} t_1^2 & t_1 & 1 & 0 & 0 & 0 \\ t_2^2 & t_2 & 1 & 0 & 0 & 0 \\ t_3^2 & t_3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & t_4^2 & t_4 & 1 \\ 0 & 0 & 0 & t_5^2 & t_5 & 1 \\ 0 & 0 & 0 & t_6^2 & t_6 & 1 \end{pmatrix} \begin{pmatrix} a\alpha_{x1}^2 + c\alpha_{x1}\alpha_{y1} + e\alpha_{y1}^2 \\ 2a\alpha_{x1}\beta_{x1} + b\alpha_{x1} + c\alpha_{x1}\beta_{y1} + c\alpha_{y1}\beta_{x1} + d\alpha_{y1} + 2e\alpha_{y1}\beta_{y1} \\ a\beta_{x1}^2 + b\beta_{x1} + c\beta_{x1}\beta_{y1} + d\beta_{y1} + e\beta_{y1}^2 + S \\ a\alpha_{x2}^2 + c\alpha_{x2}\alpha_{y2} + e\alpha_{y2}^2 \\ 2a\alpha_{x2}\beta_{x2} + b\alpha_{x2} + c\alpha_{x2}\beta_{y2} + c\alpha_{y2}\beta_{x2} + d\alpha_{y2} + 2e\alpha_{y2}\beta_{y2} \\ a\beta_{x2}^2 + b\beta_{x2} + c\beta_{x2}\beta_{y2} + d\beta_{y2} + e\beta_{y2}^2 + S \end{pmatrix}$$

t_1 から t_6 は全て異なる値を持つので，上式の右辺第一行列は非零である．また右辺第二行列から次の行列を得る．

$$= \begin{pmatrix} a\alpha_{x1}^2 + c\alpha_{x1}\alpha_{y1} + e\alpha_{y1}^2 \\ 2a\alpha_{x1}\beta_{x1} + b\alpha_{x1} + c\alpha_{x1}\beta_{y1} + c\alpha_{y1}\beta_{x1} + d\alpha_{y1} + 2e\alpha_{y1}\beta_{y1} \\ a\beta_{x1}^2 + b\beta_{x1} + c\beta_{x1}\beta_{y1} + d\beta_{y1} + e\beta_{y1}^2 + S \\ a\alpha_{x2}^2 + c\alpha_{x2}\alpha_{y2} + e\alpha_{y2}^2 \\ 2a\alpha_{x2}\beta_{x2} + b\alpha_{x2} + c\alpha_{x2}\beta_{y2} + c\alpha_{y2}\beta_{x2} + d\alpha_{y2} + 2e\alpha_{y2}\beta_{y2} \\ a\beta_{x2}^2 + b\beta_{x2} + c\beta_{x2}\beta_{y2} + d\beta_{y2} + e\beta_{y2}^2 + S \end{pmatrix} = \begin{pmatrix} \alpha_{x1}^2 & 0 & \alpha_{x1}\alpha_{y1} & 0 & \alpha_{y1}^2 & 0 \\ 2\alpha_{x1}\beta_{x1} & \alpha_{x1} & \alpha_{x1}\beta_{y1} + \alpha_{y1}\beta_{x1} & \alpha_{y1} & 2\alpha_{y1}\beta_{y1} & 0 \\ \beta_{x1}^2 & \beta_{x1} & \beta_{x1}\beta_{y1} & \beta_{y1} & \beta_{y1}^2 & 1 \\ \alpha_{x2}^2 & 0 & \alpha_{x2}\alpha_{y2} & 0 & \alpha_{y2}^2 & 0 \\ 2\alpha_{x2}\beta_{x2} & \alpha_{x2} & \alpha_{x2}\beta_{y2} + \alpha_{y2}\beta_{x2} & \alpha_{y2} & 2\alpha_{y2}\beta_{y2} & 0 \\ \beta_{x2}^2 & \beta_{x2} & \beta_{x2}\beta_{y2} & \beta_{y2} & \beta_{y2}^2 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ S \end{pmatrix}$$

上式の右辺第一行列はフルランクで無いため，多項式の係数を計算より得ることが出来ない．これは，二次曲面の断面を 2 つ得ても二次曲面全体を復元することは出来ないことを意味していると思われる．

以上より，2 変数 2 次の多項式補間法にて 6 個のシェアが与えられたとき，そのうち 3 個が原点を通らない直線上にあり，他の 3 個も原点を通らない別の直線上にあったとき，秘密情報が復元できないことが言えた．□

証明 7 シェアが 5 個与えられ、ある 2 個は x - y 平面にて原点を通る直線上に並び，他の 3 個はどの直線上にもないとき秘密情報が復元できないことを証明する．図にそのイメージを示す．原点を通る直線上のシェアの位置はそれぞれ

$$x_i = \alpha t_i, y_i = \beta t_i$$

と表すことが出来る． v_1 と v_3 は原点を通る直線上にならんでいないことから

$$x_1y_3 - x_3y_1 \neq 0$$

を得る．他の組み合わせについても同様に考え，またそれらを α や β を用いて表すと，最終的に

$$\alpha y_3 - \beta x_3 \neq 0 \quad (18)$$

$$\alpha y_4 - \beta x_4 \neq 0 \quad (19)$$

$$\alpha y_5 - \beta x_5 \neq 0 \quad (20)$$

を得る．また v_3 と v_4 と v_5 は直線上に並んでいないことから

$$(x_5 - x_3)(y_4 - y_3) - (x_4 - x_3)(y_5 - y_3) \neq 0 \quad (21)$$

である． v_1 と v_2 について考えると，ある任意の S について

$$\begin{pmatrix} z_1 - S \\ z_2 - S \end{pmatrix} = \begin{pmatrix} (\alpha t_1)^2 & \alpha t_1 & \alpha t_1 \beta t_1 & \beta t_1 & (\beta t_1)^2 \\ (\alpha t_2)^2 & \alpha t_2 & \alpha t_2 \beta t_2 & \beta t_2 & (\beta t_2)^2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} \\ = \begin{pmatrix} t_1^2 & t_1 \\ t_2^2 & t_2 \end{pmatrix} \begin{pmatrix} a\alpha^2 + c\alpha\beta + e\beta^2 \\ b\alpha + d\beta \end{pmatrix}$$

と表すことが出来る． $t_1 \neq t_2$ より，ある A, B が存在して，

$$\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} \alpha^2 & 0 & \alpha\beta & 0 & \beta^2 \\ 0 & \alpha & 0 & \beta & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix}$$

と書ける．このことから，例にあげた 5 個のシェアについて

$$\begin{pmatrix} A \\ B \\ z_3 - S \\ z_4 - S \\ z_5 - S \end{pmatrix} = \begin{pmatrix} \alpha^2 & 0 & \alpha\beta & 0 & \beta^2 \\ 0 & \alpha & 0 & \beta & 0 \\ x_3^2 & x_3 & x_3 y_3 & y_3 & y_3^2 \\ x_4^2 & x_4 & x_4 y_4 & y_4 & y_4^2 \\ x_5^2 & x_5 & x_5 y_5 & y_5 & y_5^2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix}$$

を得る．式 (18)，式 (19)，式 (20)，式 (21) より，

$$\begin{vmatrix} \alpha^2 & 0 & \alpha\beta & 0 & \beta^2 \\ 0 & \alpha & 0 & \beta & 0 \\ x_3^2 & x_3 & x_3 y_3 & y_3 & y_3^2 \\ x_4^2 & x_4 & x_4 y_4 & y_4 & y_4^2 \\ x_5^2 & x_5 & x_5 y_5 & y_5 & y_5^2 \end{vmatrix} = (\alpha y_3 - \beta x_3)(\alpha y_4 - \beta x_4)(\alpha y_5 - \beta x_5) \\ \cdot ((x_5 - x_3)(y_4 - y_3) - (x_4 - x_3)(y_5 - y_3)) \neq 0$$

を得る．よって，どのような S についてもそれを満たす a, b, c, d, e が存在することになり，この 5 個のシェアからは S に対する情報は得られないことが分かる．

以上よりシェアが 5 個与えられ，そのうち 2 個は原点を通る直線上にあり，他の 3 個は直線上にないとき秘密情報が復元できないことが言えた．□

証明 8

シェアが 4 個与えられ，全てのシェアが x - y 平面にて原点を通る二次曲線上にある場合，秘密情報が復元できないことを証明する．今ある 4 個のシェアの位置は

$$\begin{aligned} x &= t \\ y &= \alpha t^2 + \beta t \end{aligned}$$

を満たす．これより

$$\begin{aligned}
f(x, y) &= ax^2 + bx + cxy + dy + ey^2 + S \\
&= at^2 + bt + ct(\alpha t^2 + \beta t) + d(\alpha t^2 + \beta t) + e(\alpha t^2 + \beta t)^2 + S \\
&= t^4(e\alpha^2) + t^3(c\alpha + 2e\alpha\beta) + t^2(a + c\beta + d\alpha + e\beta^2) + t(b + d\beta) + S \\
&= At^4 + Bt^3 + Ct^2 + Dt + S
\end{aligned}$$

となり，1 変数 4 次の多項式を得る．この多項式はしきい値 5 の秘密分散法と同じ形をしており，シェアが 5 個なければ秘密情報が復元できない．よって今ある 4 個のシェアからは秘密情報についての情報を得られない．

以上より，シェアが 4 個与えられ，全てのシェアが x - y 平面にて原点を通る二次曲線上にある場合，秘密情報が復元できないことが証明できた．□

証明 9

x - y 平面にて原点を通る直線上のシェアが 2 個あったとき，秘密情報が復元できないことを証明する．2 個のシェアの位置について

$$x = \alpha t, y = \beta t$$

が言える．このことから任意の S について

$$\begin{aligned}
&\begin{pmatrix} z_1 - S \\ z_2 - S \end{pmatrix} \\
&= \begin{pmatrix} (\alpha t_1)^2 & \alpha t_1 & \alpha t_1 \beta t_1 & \beta t_1 & (\beta t_1)^2 \\ (\alpha t_2)^2 & \alpha t_2 & \alpha t_2 \beta t_2 & \beta t_2 & (\beta t_2)^2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} \\
&= \begin{pmatrix} t_1^2 & t_1 \\ t_2^2 & t_2 \end{pmatrix} \begin{pmatrix} a\alpha^2 + c\alpha\beta + e\beta^2 \\ b\alpha + d\beta \end{pmatrix}
\end{aligned}$$

$t_1 \neq t_2$ かつ $t_1 \neq 0, t_2 \neq 0$ より，上式右辺の第一行列の行列式の値は非零である．よって，どのような S についてもそれを満たす a, b, c, d, e が一意に決定されるため，多項式に関する情報は得られない．

以上より， x - y 平面にて原点を通る直線上のシェアを 2 個得た場合，秘密情報は復元できないことが言えた．□

証明 10

2 変数 2 次の多項式補間法にて，ある二次曲線上のシェアが 5 個あったとき，その曲線上の任

意の位置のシェアを得られることを証明する．今考える全てのシェアの位置について

$$x = t, y = \alpha t^2 + \beta t + \gamma \quad (22)$$

が言える．これを多項式 $f(x, y)$ に代入すると次式を得る．

$$\begin{aligned} f(x, y) &= ax^2 + bx + cxy + dy + ey^2 + S \\ &= at^2 + bt + ct(\alpha t^2 + \beta t + \gamma) + d(\alpha t^2 + \beta t + \gamma) + e(\alpha t^2 + \beta t + \gamma)^2 + S \\ &= at^2 + bt + c\alpha t^3 + c\beta t^2 + c\gamma t + d\alpha t^2 + d\beta t + d\gamma \\ &\quad + e\alpha^2 t^4 + 2e\alpha\beta t^3 + 2e\alpha\gamma t^2 + e\beta^2 t^2 + 2e\beta\gamma t + \gamma^2 + S \\ &= t^4(e\alpha^2) \\ &\quad + t^3(c\alpha + 2e\alpha\beta) \\ &\quad + t^2(a + c\beta + d\alpha + 2e\alpha\gamma + e\beta^2) \\ &\quad + t(b + c\gamma + d\beta + 2e\beta\gamma) \\ &\quad + d\gamma + \gamma^2 + S \\ &= At^4 + Bt^3 + Ct^2 + Dt + E \end{aligned} \quad (23)$$

上式は 1 変数 4 次の多項式となっている．式 (22) より，今考えている二次曲線上の任意の位置の t を得ることで，式 (23) よりその位置の z の値を得ることが出来る．

以上より，2 変数 2 次の多項式補間法にて，ある二次曲線上のシェアが 5 個あったとき，その曲線上の任意の位置のシェアを得られることが言えた．□