アルゴリズム 33－8
（1993．5．28）

集合族における極小集合決定アルゴリズムとその応用

土井 洋　　岡本 栄司
北陸先端科学技術大学院大学 情報科学研究科

本論文では、集合族における極小集合決定アルゴリズムに基づき、モノトーン性の判定をも行なうアルゴリズムを提案する。

秘密情報分散方式においては、秘密情報を復元できるグループの集合族（アクセス構造）はモノトーン性を持ち、その極小集合により特徴づけられる。提案する極小集合決定アルゴリズムは、秘密情報分散方式に応用することができ、アクセス構造のモノトーン性の判定を効率よく行なう。

A Decision Algorithm for Minimal Sets and its Application

Hiroshi DOI　　Eiji OKAMOTO
School of Information Science
JAIST(Japan Advanced Institute of Science and Technology)

This paper presents a decision algorithm for monotone sets based on an algorithm for finding minimal sets in a family of sets.

A family of access groups in secret sharing systems has a monotone property, and its minimal sets characterize its access structure. The algorithm for finding the minimal sets is applied to secret sharing systems so that the monotone property of the access structure is effectively decided.

1 はじめに

有限集合 N に対し、N の部分集合から成る集合族 $\mathcal{A}$ が与えられた場合、その極小集合を決定する必要が多々ある。その検索には色々なアルゴリズムが考えられるが、本論文では「エラトステネスのふるい」を利用した方式を与える。このアルゴリズムは他の条件を付加すると、集合のモノトーン性を判定する効率的なアルゴリズムとなる。

ある集合族 $\mathcal{A}$ がモノトーン性を持つとは、「$\mathcal{A}$ に含まれる集合 A を含む N の任意の部分集合は、やはり $\mathcal{A}$ に含まれる」という性質である。この性質は、情報セキュリティにおける秘密情報分散方式と密接に関係している。

本論文では、集合族の極小集合の決定、特にモノトーン性の判定も条件に加えた極小集合の決定アルゴリズムを提案する。

2 極小集合と決定アルゴリズム

有限集合 $N = \{1, 2, \cdots, n\}$ に対し、Nの部分集合から成る集合族 $\mathcal{A} \subset 2^N$ が与えられたとする。極小集合の定義と、その例を以下に示す。

定義 1 (極小集合) 与えられた集合族 $\mathcal{A}$ に対し、その部分集合 $\mathcal{F} \subset \mathcal{A}$ が

$$\mathcal{F} = \{P \in \mathcal{F} : \forall Q \in \mathcal{A}, P \neq Q \Rightarrow Q \not\subset P\} \quad (1)$$

となるとき、$\mathcal{F}$ を $\mathcal{A}$ の極小集合と定義する。 □

例 1 集合族 $\mathcal{A}$ が
$\mathcal{A} = \{\{1,2\}, \{2,3\}, \{1,3,4\}, \{1,2,3\}, \{1,2,3,4\}\}$
で与えられた時、極小集合は
$\{\{1,2\}, \{2,3\}, \{1,3,4\}\}$ である。 □

単に極小集合を決定するには、「エラトステネスのふるい」を利用したアルゴリズムが考えられる。アルゴリズムを以下に示す。

なお、本論文では混乱を避けるため、元、集合、集合族を次のように記号、または字体を区別して使用する。

元 $1, 2, \cdots, p, q$

集合 A, B, N, P

集合族 $\mathcal{A}, \mathcal{B}, \mathcal{F}$

アルゴリズム 1 (極小集合の決定)
【定義】
$\mathcal{A}$: 与えられた集合族
$\mathcal{B}$: 求める極小集合

【手続き】
$\mathcal{A}$ に含まれる集合を、その集合が含む元の数の昇順にソートする。
$\mathcal{B} = \emptyset$;
while $(\mathcal{A} \neq \emptyset)$ {
  $A = \mathcal{A}$ に含まれる元の数が最小の集合;
  $\mathcal{B} = \mathcal{B} \cup A$;
  $\mathcal{A} = \mathcal{A} - A$;
  for ($X \in \mathcal{A}$ となる X 全て) {
    if $(A \subset X)$
      $\mathcal{A} = \mathcal{A} - X$;
  }
}

□

ここで、$\mathcal{B} - A$ は、集合族 $\mathcal{B}$ から集合 A を取り除く演算を意味する。

与えられた集合族の構造に制限がない場合、極小集合を決定するには、アルゴリズム 1に示す「エラトステネスのふるい」的な手法が適切と考えられる。

3 集合族のモノトーン性

3.1 モノトーン性の定義

極小集合を決定する際、与えられた集合族にモノトーン性を要求する場合がある。モノトーン性の定義とその例を以下に示す。

定義 2 (モノトーン性) 有限集合 N に対し、N の部分集合から成る集合族 $\mathcal{A} \subset 2^N$ が与えられた場合、$\mathcal{A}$ がモノトーン性を持つとは、

$$\forall A \in \mathcal{A}, A \subset \forall B \subset N \Rightarrow B \in \mathcal{A} \quad (2)$$

を満たすことをいう。 □

次に、モノトーン性を持つ集合族の例を示す。

例 2 $N = \{1,2,3,4\}$ とすると、次の集合族 $\mathcal{A}$ はモノトーン性を持つ。

$$\mathcal{A} = \{\{1,2\}, \{2,3\}, \{1,3,4\}, \{1,2,3\}, \{1,2,4\}, \{2,3,4\}, \{1,2,3,4\}\}$$

なお、この例では、$\{\{1,2\},\{2,3\},\{1,3,4\}\}$ が極小集合になる。 □

3.2 応用例

集合族のモノトーン性は秘密情報分散方式と密接な関係がある。秘密情報分散方式とは、秘密情報を複数に分割し、各々適切なユーザに秘密を分散保管させる方法である。もっとも基本的な方式である (k,n) しきい値法 [Sha79] では、秘密情報を n 人に分割し、n 人で分散保管する。分散情報のうち、k 個の情報が集まれば秘密が復元されるが、k個未満の情報からは秘密に関する情報は全く得られない。この方式は、ネットワーク内で秘密鍵を分散管理する際に利用できる。

秘密情報分散方式において、メンバーの全体集合を

$$N = \{1, 2, \cdots, n\}$$

とする。秘密情報を復元できるメンバーのグループ（アクセス集合）の集合族を $\mathcal{A}$ とおき、アクセス構造と呼ぶ。アクセス構造の本質を意味する性質として、次の定理1が成り立つ。

定理 1 秘密情報分散方式において、アクセス構造はモノトーン性を持つ。逆に、与えられた集合族 $\mathcal{A}$ がモノトーン性を持つならば、$\mathcal{A}$ をアクセス構造とする秘密情報分散方式が存在する [ISN87]。 □

本論文では秘密情報分散方式を念頭におき、次の2項目を満足するアルゴリズムについて考察する。

- 与えられた集合族がモノトーン性を持つこと
- モノトーン性を持つ条件の下で極小集合を決定すること

4 モノトーン性判定アルゴリズム

4.1 モノトーン性の判定

先に示したアルゴリズム1は、極小集合を決定することはできるが、モノトーン性を確認することはできない。実際、例1で与えられた集合族 $\mathcal{A}$ の極小集合を決定することはできるが、$\mathcal{A}$ はモノトーン性を持たない。

そこで、モノトーン性の判定を行なうアルゴリズムを考える。

アルゴリズム 2 (モノトーン性の判定)

【定義】

$N = \{1, 2, \cdots, n\}$: メンバーの全体集合

$\mathcal{A}$: 与えられた Nの部分集合族

$\mathcal{A}[i]$: $\mathcal{A}$ に含まれる集合の中で、
i 個の元を持つ集合から成る集合族

【手続き】

$\mathcal{A}$ に含まれる集合を、その集合が含む元の数の昇順にソートする。

```
while (A ≠ ∅){
  A = A に含まれる元の数が最小の集合;
    (元の数を i とする)
  A = A − A;
  P = N − A;
  while (P ≠ ∅){
    p ∈ P;
    P = P − p;
    if (A ∪ p ∉ A[i + 1]){
      A はモノトーン集合でない;
      エラー終了;
    }
  }
}
```

□

アルゴリズム 2の計算量を簡単な例で求めてみる。極小集合が単一の元から成る集合1つの場合、例えば、$\{\{1\}\}$ のような場合を考えると、計算量は以下のようになる。

$$\begin{aligned} \text{計算量} &= 1 + (n-1) + (n-1)(n-2) + \cdots \\ &= \sum_{k=1}^{n-1} {}_{n-1}P_k \end{aligned}$$

アルゴリズム 2は、極小集合に含まれる集合がいかなるパターンでもモノトーン性の確認ができるが、計算量が多すぎる。

4.2 モノトーン性の特徴

次に、集合族 $\mathcal{A}$ がモノトーン性を持つことに着目してその性質を調べる。極小集合に含まれる任意の集合に対して、それを含む N の部分集合がまた $\mathcal{A}$ に含まれているはずであるから、組合せによる集合数によってモノトーン集合族の特徴を示すことができる。

定理 2 集合族 $\mathcal{A}$ がモノトーン性を持つための必要十分条件は、任意の集合 A に対して

$$|\{B : A \subseteq B\}| = 2^{n-|A|} \tag{3}$$

が成り立つことである。ここで、集合 X に対して $|X|$ は X の元の数を意味する。

(証明) $\mathcal{A}$ がモノトーン性を持てば上式が成立するのは当然である。A を含む部分集合は全部で $2^{n-|A|}$ 個しか存在しないので、逆に上式が成立すれば A を含む全ての部分集合は $\mathcal{A}$ に含まれる。 □

次に、$\mathcal{A}$ がモノトーン性を持つ場合、A を含む $\mathcal{A}[i]$ の集合数を考える。ただし、$A \in \mathcal{A}$ で、$|A| < i$ とする。すると、定理2から、次の定理が得られる。

定理 3 $\mathcal{A}[i]$ を i 個の要素を持つ集合から成る $\mathcal{A}$ の部分集合とすると、$\mathcal{A}[i]$ において $\forall A \in \mathcal{A}$ を含む集合の数 $(= gnum(A,i))$ は以下の式で計算できる。

$$gnum(A,i) = \binom{n-|A|}{i-|A|}$$

(証明) 定理2の証明と同様。 □

この議論を一般化することにより、次の組合せ理論的性質が導かれる。

定理 4 $\mathcal{A}$ の極小集合を $\{A_1, A_2, \cdots, A_L\}$ とする。このとき、$\mathcal{A}$ がモノトーン性を持つための必要十分条件は、

$$|\mathcal{A}| = \sum_{k=1}^{L} \sum_{i_1,i_2,\cdots,i_k} (-1)^{k+1} 2^{n-|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_k}|} \tag{4}$$

である。

(証明) 前記定理2から、極小集合が1個の集合から成るときは成立する。2個のとき、$2^{n-|A_1|} + 2^{n-|A_2|}$ は $A_1 \cup A_2$ を含む部分集合が二重に数えられているので、その分を差し引く必要がある。3個以上でも同様にすると、包除原理により上式が得られる。

逆は、定理2の証明と同様である。例えば極小集合が2個の集合 A_1 と A_2 から成るとき、それらを含む部分集合は全部で $2^{n-|A_1|} + 2^{n-|A_2|} - 2^{n-|A_1 \cup A_2|}$ 個存在し、一方 $\mathcal{A}$ は A_1 と A_2 を含む部分集合を $2^{n-|A_1|} + 2^{n-|A_2|} - 2^{n-|A_1 \cup A_2|}$ 個含むので、$\mathcal{A}$ は A_1 と A_2 を含む部分集合を全て持つ。 □

なお、上式では k に関する和 $\sum_{k=1}^{L}$ を途中で打ち切れば、$|\mathcal{A}|$ の近似式となる。近似は $|\mathcal{A}|$ を挟む形で精度が上がっていく。

このように、モノトーン性を組合せ論的性質を用いて、特徴づけることができた。

4.3 改良アルゴリズム

定理2、定理3を利用してアルゴリズム2を改良し、次のアルゴリズムを得る。

アルゴリズム 3 (要素数チェック方式)

【定義】

$N = \{1, 2, \cdots, n\}$: メンバーの全体集合

$\mathcal{A}$: 与えられた N の部分集合族

$\mathcal{A}[i]$: $\mathcal{A}$ に含まれる集合の中で、i 個の元を持つ集合から成る集合族

$\mathcal{A}[i][k]$: $\mathcal{A}[i]$ に含まれる集合の中で、k 番目の集合

$\mathcal{B}$: 求める極小集合

【手続き】

```
A に含まれる集合を、その集合が含む元の数の
  昇順にソートする。
for(i = 1; i < n; i++){
  B = B + {A[i] で一度も参照されていないもの}
  while (B ∈ Bとなる B 全て){
    count = 0;
    for (k = 1; k ≤ |A[i+1]|; k++){
      if (B ⊂ A[i+1][k]){
        count++;
        A[i+1][k] に参照マークをつける
      }
    }
    if (count ≠ gnum(B, i+1)){
      アクセス集合ではない;
      エラー終了;
    }
  }
}
```

□

ここで、$A[i+1]$ において、極小集合に含まれる集合 B を含む集合数 $(= gnum(B,i))$ を定理3を利用して求めている。

アルゴリズム3は極小集合を決定しつつ、モノトーン性をも判定している。更に、「参照マークをつける」処理を「削除する」処理に変更すれば、最初に示したアルゴリズム1と同様の処理を行なうことがわかる。

5 計算量について

まず、極小集合が単一の元から成る集合1つの場合、すなわち極小集合 $\mathcal{B} = \{\{1\}\}$ のような場合を考えると、アルゴリズム3の計算量は以下のようになる。

$$\begin{aligned} \text{計算量} &= \binom{n-1}{1} + \binom{n-1}{2} + \cdots + \binom{n-1}{n-1} \\ &= 2^{n-1} \end{aligned}$$

これは、集合族に含まれる集合数と等しい検索数であり、「極小集合が単一の元から成る集合1つ」である場合は最速と考えられる。ただ、この検索を実現するためにはあらかじめ集合族を集合が含む元の個数の順にソートしなくてはならない。元の数は1以上 n 以下であるから、元の数ごとに探索できるようなソートで十分である。従ってソートの計算量はやはり集合の数に比例すると考えられる。

次に極小集合が複数個 ($A_1, A_2, \cdots, A_m$) ある場合を考える。各々の集合に含まれる元の数を $b[i]$ 個 $(i = 1, 2, \cdots, m)$ とする。アルゴリズム3では 各 A_i に対し、$b[i]$ 個より多くの元を含む集合族 $\mathcal{A}$ の集合すべてに対し、1回だけ包含関係を調べることになる。従って計算量は次の式となる。

$$\begin{aligned} \text{計算量} &= \sum_{i=b[1]+1}^{n} |\mathcal{A}[i]| + \sum_{i=b[2]+1}^{n} |\mathcal{A}[i]| + \cdots \\ &= \sum_{j=1}^{m} \sum_{i=b[j]+1}^{n} |\mathcal{A}[i]| \end{aligned}$$

この計算を、(k, n) しきい値 [Sha79] を持つアクセス構造に適用してみる。(k, n) しきい値法によると、n 個中の任意の k個以上から成る部分集合が秘密を復元できるから、計算量は

$$ {}_nC_k \cdot \sum_{i=k+1}^{n} |\mathcal{A}[i]| $$

となる。

一般に極小集合が m 個の集合から成る場合には、計算量は最大でも

$$ m \cdot |\mathcal{A}| $$

を越えることはない。すなわち、これが計算量の上限を与えている。更に計算量を減らすためには、何らかの手段を用いて途中に行なう計算を省く工夫が必要となる。

6 おわりに

秘密情報分散方式に応用できる、モノトーン性を持つ集合族の極小集合決定アルゴリズムを提案した。このアルゴリズムは、与えられた集合族のモノトーン性の判定も同時に行なっている。しかし、計算量の下限を示したとは言い難い。アルゴリズム改良の余地について、研究の必要がある。

7 謝辞

本研究に対して、熱心に討論して下さった北陸先端科学技術大学院大学の岡本研究室、植松研究室の方々に感謝致します。

参考文献

[ISN87] Ito,M., Saito,A., and Nishizeki,T. : 'Secret sharing scheme realizing general access structure' , Proc. Glob. Com.87, pp.99-102, 1987

[Sha79] A.Shamir : 'How to share a secret', Commun.ACM, vol.22, no.11,pp.612-613, 1979

[OD93] Okamoto,E.,and Doi,H.: '秘密分散管理方式の構造と複雑さについて', The 1993 Symposium on Cryptography and Information Security, SCIS93-11A, 1993