ガロア体の、確率オートマトンにおける組合せ問題への一応用

貞広泰造* 金岡泰保† 富田真吾†, 栗山 憲§

1 はじめに

数学では表面上は易しく見える問題を、その問題を一般化することにより、いわば難しくすることにより解くことが可能になることはよくあることである。たとえば組合せ問題のように、問題そのものの理解は容易であるが素朴な解法は困難であるような問題では、適切な代数的構造を導入し代数の手法を利用することにより解くことは自然である。

金岡・富田は確率オートマトンの分解の問題に関連して、次の組合せ問題を提起した。[1,2] 任意の $1 \leq k \leq n$ に対して、$(n,k)-$ プロパティをみたす長さ n のビット列の集合 S で要素数が 2^k であるものが存在するか。また存在するならば、実際に S を構成せよ。

本論文では、確率オートマトンに関連して生じるこの組合せ問題を、ガロア体上の線形空間のその性質をもつ部分空間の存在問題に翻訳することにより解決した。

定理　ガロア体を $\mathbf{F}_2 = GF(2)$ すなわち $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ とする。体 $\mathbf{F}_2$ 上の線形空間 $\mathbf{F}_2^n$ の中に、$(n,k)-$ プロパティをみたす k 次元の部分空間が存在する。したがって、$(n,k)-$ プロパティをみたす長さ n のビット列の集合で要素数が 2^k であるものが存在する。

証明は、部分空間の次元を求め、集合の要素の個数を次元を使って計算することが鍵となっている。しかもこの証明はアルゴリズム、すなわち具体的な構成法をも与えている。

2 定理の証明

定義 1 長さ n の 0,1 の列の集合 S に含まれる任意のビット列 $a = a_0a_1\cdots a_{n-1}$、$b = b_0b_1\cdots b_{n-1}$ $(a_i, b_i \in \{0,1\})$ に対して $a \neq b$ なら長さ k のビット列として

$$a_i a_{(i+1)(modn)} \cdots a_{(i+k-1)(modn)} \neq b_i b_{(i+1)(modn)} \cdots b_{(i+k-1)(modn)}$$

が任意の $0 \leq i \leq n-1$ でなりたつとき S は $(n,k)-$ プロパティを持つということにする。

ただし 今後 $[i]_n = i(\mathbf{mod}n) = i$を$n$でわった剰余 と表し、必要ないと思われるところは $[i]_n$ を $[i]$ と書き n を明記しない。

例 1

$$S = \{00000, 10011, 01010, 11001, 00111, 10100, 01101, 11110\}$$

とおくと S は $(5,3)-$ プロパティをもつ。

以下で定理を証明する。

長さ n のビット列は自然にベクトル空間 $\mathbf{F}_2^n$ の元と思える. ここで 2 つの補題を用意する。

*宇部工業高等専門学校・経営情報学科
†山口大学工学部・知能情報システム工学科
‡山口大学工学部・知能情報システム工学科
§山口大学教養部・人間環境論

補題 1 $\{x_1,\cdots x_{k-1}\}$、$\{y_1,\cdots,y_{k-1}\}$ を k 次元ベクトル空間 V (基礎体は任意) の 2 組の部分集合とし $1\leq i\leq k-1$ に対して k 個のベクトルの集合

$$\{x_i,x_{i+1},\cdots,x_{k-1},y_1,\cdots,y_i\}$$

は一次独立であるとする。ここで V の部分空間の族 V_i を次のように定める。

$$\begin{aligned}
V_1 &=< x_1,\cdots,x_{k-1} >\\
V_2 &=< x_2,\cdots,x_{k-1},y_1 >\\
V_3 &=< x_3,\cdots,x_{k-1},y_1,y_2 >\\
&\cdots\\
V_{k-1} &=< x_{k-1},y_1,\cdots,y_{k-2} >\\
V_k &=< y_1,\cdots,y_{k-1} >
\end{aligned}$$

このとき $0\leq i_1,< i_2 <\cdots< i_m\leq k-1$ に対して

$$dim(V_{i_1}\cap V_{i_2}\cap\cdots\cap V_{i_m})=k-m$$

が成り立つ。ここで $< x_1,x_2,\cdots x_{k-1} >$ は $\{x_1,x_2,\cdots x_{k-1}\}$ で生成される部分空間とする。

[証明] m に関する帰納法で証明する。$m=1$ のときは $dim(V_i)=k-1$ で成り立つ。$M\geq 2$ として $m=M-1$ のとき成り立つならば $m=M$ のときも成り立つことを示す。

$$\begin{aligned}
& dim(V_{i_1}\cap V_{i_2}\cap\cdots\cap V_{i_M})\\
= \;& dim((V_{i_1}\cap V_{i_2}\cap\cdots\cap V_{i_{M-1}})\cap V_{i_M})\\
= \;& dim(V_{i_1}\cap V_{i_2}\cap\cdots\cap V_{i_{M-1}})+dim(V_{i_M})-dim((V_{i_1}\cap V_{i_2}\cap\cdots\cap V_{i_{M-1}})+V_{i_M})
\end{aligned}$$

上の等式の最後の式の第 1 項は帰納法の仮定により $k-(M-1)$ で第 2 項は $k-1$. 残った第 3 項を計算する. $V_{i_1}\cap V_{i_2}\cap\cdots\cap V_{i_{M-1}}$ は V_{i_M} には含まれない. なぜならば x_{i_M-1} は $V_{i_1}\cap V_{i_2}\cap\cdots\cap V_{i_{M-1}}$ に含まれ、もし $V_{i_1}\cap V_{i_2}\cap\cdots\cap V_{i_M-1}$ が V_{i_M} に含まれたなら $x_i,x_{i+1},\cdots,x_{k-1},y_1,\cdots,y_i$ が一次独立であるという条件に反する. よって第 3 項 $> dimV_{i_m}=k-1$ となりまた k 次元空間の部分空間であることから第 3 項 $\leq k$ となり 第 3 項 $=k$ となる。よって式の値は $k-M$ であることが分かる。

補題 2 任意の $n\geq k$ に対して次のような k 本のベクトル $e_1,e_2,\cdots e_k\in\mathbf{F}_2{}^n$ が存在する。$e_i=(d_{i,0},d_{i,1},\cdots,d_{i,n-1})$ とし、$0\leq j\leq n-1$ に対して

$$e_{i,j}=(d_{i,[j]}d_{i,[j+1]}\cdots d_{i,[j+k-1]})$$

とおく。このとき任意の $0\leq j\leq n-1$ に対して $e_{1,j},e_{2,j},\cdots,e_{k,j}$ は一次独立。

[証明] 帰納法によって証明する。

$n=k$ のときは $e_1=(1,0,\cdots,0)$, $e_2=(0,1,\cdots,0)$, $\cdots$ $e_n=(0,\cdots,0,1)$, とすればよい。

$n=N$ のとき成り立つなら $n=N+1$ のときも成り立つことを示す。$e_1,\cdots,e_k\in\mathbf{F}_2^N$ が上の条件を満たすとする。e_i を行ベクトルとする行列を $E(N,k)$ とし、その列ベクトルを $a_0,\cdots,a_{N-1}$ とする。

$$E(N,k)=\begin{pmatrix} e_1\\ e_2\\ \cdots\\ e_k\end{pmatrix}=(a_0,a_1,\cdots,a_{N-1})$$

このとき ある $a_N\in\mathbf{F}_2^k$ を列ベクトルとして $E(N,k)$ に付け加えた行列 $(a_0,\cdots,a_N)$ の行ベクトルが条件を満たすように出来ることを示す。それは、任意の j について $a_{[j]_{N+1}},a_{[j+1]_{N+1}},\cdots,a_{[j+k-1]_{N+1}}$ が一次

独立であるように a_N をとれることと同値である。$0 \leq j \leq N-k$ のとき一次独立であることは分かっているので、$N-k+1 \leq j \leq N$ で調べればよい。そのためには $\mathbf{F}_2^k$ の部分空間の族

$$V_1 =< a_{N-k+1}, \cdots, a_{N-1} >$$
$$V_2 =< a_{N-k+2}, \cdots, a_{N-1}, a_1 >$$
$$V_3 =< a_{N-k+3}, \cdots, a_{N-1}, a_1, a_2 >$$
$$\cdots$$
$$V_k =< a_0, \cdots, a_{k-2} >$$

のいずれにも属さない $a_N \in \mathbf{F}_2^k$ が在ることを言えば良い。いずれの V_i にも属さない $\mathbf{F}_2^k$ の元の個数 $N(0)$ は

$$N(0) = \sharp(\mathbf{F}_2^k) - \sum_i \sharp(V_i) + \sum_{i<j} \sharp(V_i \cap V_j) - \cdots + (-1)^k \sharp(V_1 \cap \cdots \cap V_k)$$

で与えられる。ここで $x_1 = a_{N-k+1}, x_2 = a_{N-k+2}, \cdots x_{k-1} = a_{N-1}$, $y_1 = a_0, y_2 = a_1, \cdots, y_{k-1} = a_{k-2}$ とおくと補題1の条件が成り立ち $dim(V_{i_1} \cap \cdots \cap V_{i_m}) = k-m$ が成り立つ。つまり $1 \leq m \leq k$ のとき $\sharp(V_{i_1}, \cap \cdots \cap V_{i_m}) = 2^{k-m}$ が成り立つ。よって

$$N(0) = 2^k - \left(\begin{array}{c} k \\ 1 \end{array} \right) 2^{k-1} + \left(\begin{array}{c} k \\ 2 \end{array} \right) 2^{k-2} - \cdots + (-1)^k = (2-1)^k = 1$$

となりたった一つだけ $\mathbf{F}_2^k$ の元でどの V_i にも属さないものがある。

[定理の証明] 補題のベクトル $e_1, e_2, \cdots e_k$ が $\mathbf{F}_2^n$ 中で張る部分空間は (n,k)- プロパティをもつビット列となる。

定理の証明は、与えられた $1 \leq k \leq$ に対して、$\mathbf{F}_2^n$ 中の $(n,k)-$ プロパティを持つ部分空間の構成法を与えている。具体的な例でこのことを詳しく説明する。

例 **2** $(5,3)-$ プロパティをもつ $\mathbf{F}_2^5$ 中の3次元部分空間の構成。

1. $(3,3)-$ プロパティをもつ空間の基底

$$\{(1,0,0),(0,1,0),(0,0,1)\}$$

2. $(4,3)-$ プロパティをもつ $\mathbf{F}_2^4$ 中の部分空間の基底

$$E(3,3) = \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right)$$

$$V_1 = \left\langle \left(\begin{array}{c} 0 \\ 1 \\ 0 \end{array} \right), \left(\begin{array}{c} 0 \\ 0 \\ 1 \end{array} \right) \right\rangle = \left\{ \left(\begin{array}{c} 0 \\ 0 \\ 0 \end{array} \right), \left(\begin{array}{c} 0 \\ 1 \\ 0 \end{array} \right), \left(\begin{array}{c} 0 \\ 0 \\ 1 \end{array} \right), \left(\begin{array}{c} 0 \\ 1 \\ 1 \end{array} \right) \right\}$$

$$V_2 = \left\langle \left(\begin{array}{c} 0 \\ 0 \\ 1 \end{array} \right), \left(\begin{array}{c} 1 \\ 0 \\ 0 \end{array} \right) \right\rangle = \left\{ \left(\begin{array}{c} 0 \\ 0 \\ 0 \end{array} \right), \left(\begin{array}{c} 0 \\ 0 \\ 1 \end{array} \right), \left(\begin{array}{c} 1 \\ 0 \\ 0 \end{array} \right), \left(\begin{array}{c} 1 \\ 0 \\ 1 \end{array} \right) \right\}$$

$$V_1 = \left\langle \left(\begin{array}{c} 1 \\ 0 \\ 0 \end{array} \right), \left(\begin{array}{c} 0 \\ 1 \\ 0 \end{array} \right) \right\rangle = \left\{ \left(\begin{array}{c} 0 \\ 0 \\ 0 \end{array} \right), \left(\begin{array}{c} 1 \\ 0 \\ 0 \end{array} \right), \left(\begin{array}{c} 0 \\ 1 \\ 0 \end{array} \right), \left(\begin{array}{c} 1 \\ 1 \\ 0 \end{array} \right) \right\}$$

$$\mathbf{F}_2^3 - (V_1 \cup V_2 \cup V_3) = \left\{ \left(\begin{array}{c} 1 \\ 1 \\ 1 \end{array} \right) \right\}$$

3. $(5,3)-$ プロパティをもつ $\mathbf{F}_2^5$ 中の部分空間の基底

$$E(4,3)=\begin{pmatrix}1&0&0&1\\0&1&0&1\\0&0&1&1\end{pmatrix}$$

$$V_1=\left\langle\begin{pmatrix}0\\0\\1\end{pmatrix},\begin{pmatrix}1\\1\\1\end{pmatrix}\right\rangle=\left\{\begin{pmatrix}0\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\end{pmatrix},\begin{pmatrix}1\\1\\1\end{pmatrix},\begin{pmatrix}1\\1\\0\end{pmatrix}\right\}$$

$$V_2=\left\langle\begin{pmatrix}1\\1\\1\end{pmatrix},\begin{pmatrix}1\\0\\0\end{pmatrix}\right\rangle=\left\{\begin{pmatrix}0\\0\\0\end{pmatrix},\begin{pmatrix}1\\1\\1\end{pmatrix},\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\1\end{pmatrix}\right\}$$

$$V_1=\left\langle\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\end{pmatrix}\right\rangle=\left\{\begin{pmatrix}0\\0\\0\end{pmatrix},\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\end{pmatrix}\right\}$$

$$\mathbf{F}_2^3-(V_1\cup V_2\cup V_3)=\left\{\begin{pmatrix}1\\0\\1\end{pmatrix}\right\}$$

よって $(5,3)-$ プロパティをもつ $\mathbf{F}_2^5$ の部分空間は $\{(1,0,0,1,1),(0,1,0,1,0),(0,0,1,1,1)\}$ によって張られる。これが例1と同じビット列となる。

$\{0,1\}$ の列に対してのみでなく $\{0,1,\cdots q\}$,(qは素数の冪乗) の列に対しても同じような議論出来る。このことについては 別の機会に報告する。

参考文献

[1] 金岡 泰保、富田真吾 ：確率システムの一様構造相互接続分解、電子通信学会論文誌 (D)、 Vol1.J.66-D, No.3,264-280 (1983)

[2] Taiho Kanaoka and Singo Tomita : Homogeneous Decomposition of Stochatic Systems, Theoretical Computer Science, Vol.40,245-255 (1985)

[3] 栗山 憲、 金岡 泰保、富田 真吾：有限体上の線形代数の組合せへの応用、日本数学会秋季総会 (1983)

[4] Takefumi Shudo, Ken kuriyama and Taiho Kanaoka : Number Theoretical Remarks on the paper "Some Structual Properties of Product Automata" by Kanaoka and Tomita, Technology Reports of the Yamaguchi University, Vol.3, No.1, 69-77 (1982)

[5] 佐竹 一郎 ： 線形代数学、 裳華房 (1973)

ガロア体の、確率オートマトンにおける組合せ問題への一応用

貞広泰造　　金岡泰保　　富田真吾　　栗山　憲

山口大学教養部紀要　第29巻　自然科学篇　（1995年）別刷