名古屋女子大学　紀要　41（家・自）141～146　1995

有限体で定義される Commutative Association scheme のパラメータについて

岩根博之

On Commutative Association Scheme with Class 2

Hirosi IWANE

Abstract. Let F be finite filed. Let p be the number of F. Let p be odd prime. We define the assocation scheme with class 2 on F. We compute the eigenvalue, the multiplicity, and the valency of this asscіation scheme. We study the asoociation scheme with class 2 that has the same valency.

1 Introduction

定義 1.1 (Associstion Scheme): 有限集合 Xと X上の $d+1$ 個の関係 R_i(i=0,1,..., d) (すなわち R_i達は $X \times X$の部分集合) の組 $\Omega = (X, \{R_i\}_{0 \leq i \leq d})$ で次の 4 条件 (i)-(iv) を満たすものを association scheme と呼ぶ。

(i) $R_0 = \{(x,x) \mid x \in X\}$

(ii) $R_0 \cup R_1 \cdots \cup R_d = X \times X$かつ $R_i \cap R_j = \emptyset$ if $i \neq j$

(iii) 各 $i \in \{0,1,\cdots,d\}$ に対して${}^tR_i := \{(x,y) | (y,x) \in R_i\}$ と定義する時 ${}^tR_i = R_{i'}$ for some $i' \in \{0,1,\cdots,d\}$

(iv) $\forall i,j,k \in \{0,1,\cdots,d\}$ に対して $|\{z \in X | (x,z) \in R_i, (z,y) \in R_j\}|$ は $(x,y) \in R_k$のもとで (x,y) のとり方によらず一定 $(= p_{ij}^k)$. この p_{ij}^kを intersection numbers と呼ぶ.

(v) $p_{ii'}^0 = k_i$で k_i を R_i valency とよぶ.

定義 1.2: 次の条件 (v) を満たす時 可換な association scheme とよぶさらに条件 (vi) を満たすものを対称な association scheme とよぶ: (v)$p_{ij}^k = p_{ji}^k$ $for\ \forall i,j,k$, (vi) ${}^tR_i = R_i$ $for\ \forall i$

(対称な assocition scheme は可換な association scheme になる.)

A_iを R_iに対する隣接行列とする. A_iはその行と列が Xの元で parameterrize されている行列で成分は次のように定義される.

$$(A_i)_{x,y} = \begin{cases} 1, & (x,y) \in R_i \\ 0, & (x,y) \notin R_i \end{cases}$$

次の関係式が成り立つ.

$$A_0 = I \qquad (I\text{は単位行列})$$

$$A_0 + A_1 + \cdots + A_d = J \qquad (J\text{はすべて 1 の行列})$$

$${}^tA_i = A_{i'} \qquad (\text{対称な時は } i = i')$$

$$A_iA_j = \sum_{k=0}^{d} p_{ij}^k A_k \qquad (\ p_{ij}^k \text{は intersection numbers})$$

$A_0, A_1, \cdots, A_d$で生成される代数 $\mathcal{A} = \langle A_0, A_1, \cdots, A_d \rangle$ を Bose–Menser algebra と呼ぶ. Ωが可換なことと $\mathcal{A}$ が 可換 な代数 であることは同値になる. $\mathcal{A}$ は次元が $d+1$ の半単純代数で原始巾等元 $\langle E_0, E_1, \cdots, E_d \rangle$ をもつ.

以後 可換な association scheme を association scheme と呼ぶことにする. $\mathcal{A}$ は 2 組の基底 $\langle A_0, A_1, \cdots, A_d \rangle$ と $\langle E_0, E_1, \cdots, E_d \rangle$ を持っていることになる. その間の変換行列を P,Q とおくすなわち

$$(A_0, A_1, \cdots, A_d) = (E_0, E_1, \cdots, E_d)P$$
$$(E_0, E_1, \cdots, E_d) = (A_0, A_1, \cdots, A_d)Q$$

を考える.

有限体の元に差を使って関係をいれて 2-class の Association Scheme が構成できる. この Association scheme は任意の奇素数に対していつでも構成できる. その隣接行列の固有値や巾等元との間の変換行列を intersection number を求めて計算した.

2 有限体の元で作れる 2-class の Association Scheme

有限体を Fとおき, Fの元の数を p とする. ただし p は奇素数とする. F の乗法群を $F^\sharp$とし, $F^\sharp$の中の平方数の集合を $F^{\sharp 2}$とする. $F^{\sharp 2}$は群になりその位数は $(p-1)/2$ になる.

定義 2.1

Fについて Association Scheme $\Omega = (F, \{R_i\}_{0 \le i \le 2})$を次のように定義する.

$$(a,b) \in R_0 \iff a - b = 0$$
$$(a,b) \in R_1 \iff a - b \in F^{\sharp 2}$$
$$(a,b) \in R_2 \iff a - b \notin F^{\sharp 2}$$

$\Omega = (F, \{R_i\}_{0 \le i \le 2})$が Association scheme になることは $F^\sharp$が群になっていることと $a-b=\alpha$, $a-c=\beta$, $c-b=\gamma$ とおくと$\alpha = \beta + \gamma$がなりたつことから容易に示せる.

またよく知られた次のことから

$$-1 \in F^{\sharp 2} \iff p \equiv 1 \pmod 4$$
$$-1 \notin F^{\sharp 2} \iff p \equiv 3 \pmod 4$$

$\Omega = (F, \{R_i\}_{0 \le i \le 2})$ は $p \equiv 1 \pmod 4$ なら 対称な Association scheme になり, $p \equiv 3 \pmod 4$ ならば $\Omega = (F, \{R_i\}_{0 \le i \le 2})$は非対称な Association scheme になる.

Assocition scheme Ωの自明なパラメータについて

Association scheme $\Omega = (F, \{R_i\}_{0 \le i \le 2})$ Fは有限体で 元の数が p 個だからΩのサイズ n は F の元の数 p になる. R_i の valency を k_iとすると $k_i = (p-1)/2$ になる. すなわち $n = p$ で $k_1 = k_2 = (p-1)/2$ の valency が一定の Assocation scheme になっている

3 intersection numbers p_{ij}^kについて

inter sectin number の定義は p_{ij}^k= { $(a,b) \in R_k$ の時 $(a,c) \in R_i$,$(c,b) \in R_j$となる c の個数 } だからΩ の intersectin number p_{11}^1 は $a-b \in R_1$ で $a-c \in R_1, c-b \in R_1$となる c の個数を数えればよいことになる.
上の条件は

$$a-b=\theta_0 \in F^{\sharp 2}$$
$$a-c=\theta_1 \in F^{\sharp 2}$$
$$c-b=\theta_2 \in F^{\sharp 2}.$$

と書きかえられる. さらに

$$b=a-\theta_0$$
$$c=a-\theta_1$$
$$c=b+\theta_2$$
$$\theta_0=\theta_1+\theta_2. \cdots\cdots *$$

と書きなおせる. a と b が固定してあるのでθ_0はきまつているθ_1 を決めれば c が決まり $(*)$ の関係で θ_2もきまりすべての条件を満足する. $\theta_2 \in F^{\sharp 2}$だから両辺を$\theta_2$ にで割ってやる と$\theta_0/\theta_2 = \theta_1/\theta_2+1$ がなりたつ.
$\theta_0/\theta_2 \in F^{\sharp 2}, \theta_1/\theta_2 \in F^{\sharp 2}$だから$p_{11}^1$を求めるには, $F^{\sharp 2} \cap (F^{\sharp 2}+1)$ の個数を数えればよいことになる.

Lemma 1
Fが有限体, $|F|=p$ pは奇素数とおくと

$$|\{(F^{\sharp 2} \cap (F^{\sharp 2}+1)\}| = k \qquad (p=4k+3)$$
$$|\{(F^{\sharp 2} \cap (F^{\sharp 2}+1)\}| = k-1 \qquad (p=4k+1)$$

証明 $x^2=y^2+1$ という方程式を考え この方程式を F上で解いてその解の個数を数えれば良い . x^2-y^2は $(x+y)(x-y)$ と分解できるから $x+y=a$ とおくと $x-y=\frac{1}{a}$となる. $2x=a+\frac{1}{a}, 2y=a-\frac{1}{a}$ となり x,yが求まる. 異なる a に対して x^2と y^2が同じ値をとるのは $(a,-a,\frac{1}{a},\frac{-1}{a})$ の 4 個である. $a=0$ はとれない. $0 \notin F^{\sharp 2}$なので $x=0$ か $y=0$ になる場合は $a=\frac{1}{a}$ が成り立つ時で $a=\pm 1$, または $a=\frac{-1}{a}$ が成り立つ時で $a^2=-1$ と同値 で $p=4k+1$ の時は存在して 2 個ある. $p=4k+1$ の時 5 個を除外する. $p=4k+3$ の時は存在しないので $p=4k+1$ の時は 3 個を除外する. 除外した残りの Fの元は, 4 個で $F^{\sharp 2}$ の元 1 個を決める.

上の lemma から Ω の intersection number は $p=4k+3$ の時 $p_{11}^1=k$で $p=4k+1$ の時 $p_{11}^1=k-1$ になる. 他の intersection number も $F^{\sharp 2}$ の補集合考えればよい.
p_{11}^2は

$$a-b=\theta_0 \notin F^{\sharp 2}$$
$$a-c=\theta_1 \in F^{\sharp 2}$$
$$c-b=\theta_2 \in F^{\sharp 2}$$
$$\theta_0=\theta_1+\theta_2.$$

で $\theta_0/\theta_2 = \theta_1/\theta_2 + 1$ がなりたつ.
$\theta_0/\theta_1 \notin F^{\sharp 2}$ で$\theta_1/\theta_2 \in F^{\sharp 2}$ で $F^{\sharp 2}$ の補集合を $(F)^c$とおくと 同様の考え方で $((F)^c) \cap (F^{\sharp 2}+1))$ を数えればよい.
または

$$k_\gamma p^\gamma_{\alpha\beta} = k_\beta p^\beta_{\alpha'\gamma} = k_\alpha p^\alpha_{\gamma\beta'}$$

$$\sum_{j=0}^{2} p^k_{ij} = k_i$$

の 関係式を使って求められる.

4 $p = 4k+1$ の場合

F が有限体で $|F| = p$ で p は奇素数 Ω の頂点の数を n, 各 R_iの valancy を k_iとおく.
$n = p, k_1 = k_2 = (p-1)/2$ になる.
$p \equiv 1 \pmod 4$ だからΩ は対称な Association scheme になる. valancy が等しいことから $p^2_{11} = p^1_{21}$が成り立つから intersectoin matrix B_1 を次のように定義する.

$$B_1 = \begin{pmatrix} p^0_{10} & p^1_{10} & p^2_{10} \\ p^0_{11} & p^1_{11} & p^2_{11} \\ p^0_{12} & p^1_{12} & p^2_{12} \end{pmatrix}$$

$k_1 = p^0_{11} = (p-1)/2 - 1$ で $p^1_{12} = p^2_{11}$ がなりたつ.

$$B_1 = \begin{pmatrix} 0 & 1 & 0 \\ (p-1)/2 & (p-1)/4 - 1 & (p-1)/4 \\ 0 & (p-1)/4 & (p-1)/4 \end{pmatrix}$$

B_1 の固有値が A_1の固有値になる. A_1の固有値はつぎのようになる. A_1 は対称行列なので固有値は実数になり.

$$\frac{p-1}{2}, \qquad \frac{-1+\sqrt{p}}{2}, \qquad \frac{-1-\sqrt{p}}{2}$$

$\sqrt{p}$は p が素数なので無理数になるので重複度も同じになる. 解に対応してならべるとつぎのようになる.

$$1, \qquad \frac{p-1}{2}, \qquad \frac{p-1}{2}$$

P行列

$$P = \begin{pmatrix} 1 & (p-1)/2 & (p-1)/2 \\ 1 & (-1+\sqrt{p})/2 & (-1-\sqrt{p})/2 \\ 1 & (-1-\sqrt{p})/2 & (-1+\sqrt{p})/2 \end{pmatrix}$$

Q 行列

$$Q = \begin{pmatrix} 1 & (p-1)/2 & (p-1)/2 \\ 1 & (-1+\sqrt{p})/2 & (-1-\sqrt{p})/2 \\ 1 & (-1-\sqrt{p})/2 & (-1+\sqrt{p})/2 \end{pmatrix}$$

5 $p = 4k + 3$ の場合

対称でないので A_1の固有値は実数とはかぎらない.

$$B_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & (p-3)/4 & (p+1)/4 \\ (p-1)/2 & (p-3)/4 & (p-3)/4 \end{pmatrix}$$

固有値は次のようになる.

$$(p-1)/2, \quad (-1+\sqrt{p}i)/2, \quad (-1-\sqrt{p}i)/2$$

重複度は

$$1, \quad (p-1)/2, \quad (p-1)/2$$

P 行列

$$P = \begin{pmatrix} 1 & (p-1)/2 & (p-1)/2 \\ 1 & (-1+\sqrt{p}i)/2 & (-1-\sqrt{p}i)/2 \\ 1 & (-1-\sqrt{p}i)/2 & (-1+\sqrt{p}i)/2 \end{pmatrix}$$

Q 行列

$$Q = \begin{pmatrix} 1 & (p-1)/2 & (p-1)/2 \\ 1 & (-1+\sqrt{p}i)/2 & (-1-\sqrt{p}i)/2 \\ 1 & (-1-\sqrt{p}i)/2 & (-1+\sqrt{p}i)/2 \end{pmatrix}$$

6 valency が一定の Assocation scheme with class 2

命題

2-class の Association scheme で valency がすべて等しく頂点の数が素数の Association scheme は重複度も同じになり，元の数が素数個の有限体から構成できる Association scheme と同じ固有値をもつ.

証明の概略

Association scheme の頂点の数 を n, 一定の valency を kとおく. $n = 2k + 1$ で n は奇数となる.
非対称な場合 ($k_1 = k_2$は不要になる)
$p^1_{11} = \lambda$ とおく. $k_1 p^1_{12} = k_1 p^1_{11}$, $p^1_{12} = p^2_{21}$と $k_1 = k_2$ から で $p^1_{11} = p^1_{21} = p^2_{21} = \lambda$ になり,$k = 2\lambda + 1$ になる. $n = 4\lambda + 3$ となり intersection matrix を考えると

$$B_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & \lambda & \lambda+1 \\ k & \lambda & \lambda \end{pmatrix}$$

固有値は k, $(-1+\sqrt{n}i)/2$, $(-1-\sqrt{n}i)/2$ になる重複度も 1, k, kになる. $n = 4\lambda + 3$ の形の素数ならば，同じ固有値，同じ重複度をもつ非対称な 2-class の Association scheme は存在する .

対称な場合

$p^1_{11} = \lambda$とおく.$k_1 p^1_{12} = k_2 p^2_{11}$がなりたち $p^1_{12} = p^2_{11}$になる. 対称なときはこれと $k = \sum_{j=0}^{2} p^1_{1j}$で intersection matrix を考える.

$$B_1 = \begin{pmatrix} 0 & 1 & 0 \\ k & \lambda & k-\lambda-1 \\ 0 & k-\lambda-1 & \lambda+1 \end{pmatrix}$$

固有値は $D=(2\lambda+1-k)^2+4(\lambda+1)$ とおくと

$$\{k, \quad (2\lambda+1-k\pm\sqrt{D})/2\}$$

になる.

重複度を $\{1, \quad m_1, \quad m_2\}$ とおく. A_1 の trace をとると

$$k+m_1(2\lambda+1-k+\sqrt{D})/2+m_2(2\lambda+1-k-\sqrt{D})/2=0$$

で

$$k(2\lambda+2-k)+\sqrt{D}(m_1-m_2)/2$$

になる.
もし $m_1=m_2$ならば $k=2\lambda+2$ で $n=2k+1=4(\lambda+1)+1$ となり n は $4k+1$ と現せる素数になり. 固有値は $\{k,(-1\pm\sqrt{4(\lambda+1)+1})/2\}$ となる. $k,(-1\pm\sqrt{n})/2$ と書き直せる. 有限体 $(p=4k+1)$ から作れる Asoocation scheme の固有値と重複度に一致する.
$m_1\neq m_2$ のとき, $\sqrt{D}$は有理数になり固有値 $(2\lambda+1-k\pm\sqrt{D})/2$ は代数的整数だから $(2\lambda+1-k\pm\sqrt{D})/2$ も$\sqrt{D}$ も整数になる. A_1でのグラフを考える事で辺の数が $nk/2$ となり k は偶数になるから$\sqrt{D}$ は奇数になり. $D=(2s+1)^2$ とおける. $D=(2\lambda+2-k)^2+2k+1$ とおきなおし $2k+1$ は n で素数であることから $(2s+1-2\lambda-2+k)(2s+1+2\lambda+2-k)=n$ として

$$\begin{cases} 2s+1-2\lambda-2+k &= \alpha \\ 2s+1+2\lambda+2-k &= \beta \end{cases}$$

$(\alpha,\beta)=(n,1) \quad (1,n) \quad (-n,-1) \quad (-1,-n)$ で連立方程式をとくと λ が正の整数になることと重複度が整数になることからどの場合もおこりえない. $m_1\neq m_2$はおこらなく $m_1=m_2$ の場合だけである.

参考文献

1.Bannai and Ito : "Algebraic Combinatorics I" Benjamin(1984)
2.N.Biggs : "Algebraic Graph Theory " Cambridge UNIV press(1979)
3.Bela Bollobas : "Graph Theory " Springer-Verlag (1979)