数理解析研究所講究録
第2053巻 2017年 22-29

p-Ranks of conference matrices and association schemes

信州大学・理学部　花木　章秀 (Akihide Hanaki)
Faculty of Science, Shinshu University
信州大学・総合理工学研究科　矢島　秀晃 (Hideaki Yajima)
Graduate School of Science and Technology (Master's Program), Shinshu University
信州大学・総合理工学研究科　吉野　大樹 (Hiroki Yoshino)
Graduate School of Science and Technology (Master's Program), Shinshu University

1　はじめに

この原稿は京大数理研研究集会「有限群・代数的組合せ論・頂点作用素代数の研究」(代表者山内博) (2016年12月5日-8日) での講演 (12月5日、発表者吉野大樹) の記録です。

わたしたちはアソシエーションスキームの標準加群に興味を持って研究してきました。この報告書では、conferece graph [4, §10.2] から得られるアソシエーションスキームとクラス2非対称アソシエーションスキームを同時に扱える、half-caseアソシエーションスキーム $S = \{A_0 = I, A_1, A_2\}$ について書きます。(集会での発表時はhalf-caseアソシエーションスキームという単語は使っていませんが、conference matrixから得られるアソシエーションスキームとは構造的に同じものです。) half-caseアソシエーションスキームはconference matrixと密接な関係があります。half-caseアソシエーションスキーム S に対し、標数 p の体 K 上の隣接代数 KS は半単純でないことは、p が S の位数を割りきらないことと必要十分です。p が S の位数を割りきらないなら、KS は多項式代数 $K[x]$ の商代数 $K[x]/(x^3)$ と同型になります。([7, Theorem 10 and Theorem 12]) したがって、$\overline{x} \in K[x]/(x^3)$ に対応する隣接代数の元 $A_1 - A_2$ に注目していきます。標数 p での $A_1 - A_2$ のrankを $\mathrm{rank}_p(A_1 - A_2)$ と書き、$A_1 - A_2$ の *p-rank* とよびます。$\mathrm{rank}_p(A_1 - A_2)$ を用いて、K 上 S の標準加群の直規約分解を与えます。例として、位数23と29では同じ位数であれば $\mathrm{rank}_p(A_1 - A_2)$ は一定であるが、位数25と27は一定でありません。この報告書ではそれらの違い、

すなわち、素数 p が S の位数をちょうど1回割り切るとき、$\mathrm{rank}_p(A_1 - A_2)$ が一定になるということについても説明します。また、p-rank と標準加群の構造の関係に対して、$A_1 - A_2$ を用いる理由についても解説します。

全体の流れを書きます。§2では、conference matrix を定義し、そのサイズと p-rank の関係を与えます。また、conference matrix と half-case アソシエーションスキームの対応を定義するために、conference matrix を正規化するという操作を導入します。§3では、アソシエーションスキームを定義し、conference matrix からアソシエーションスキームを作る操作を説明します。その後、その操作と p-rank の関係や、half-case アソシエーションスキームの標準加群を考えます。§3では、代数的に同型なアソシエーションスキームを区別するために p-rank に注目します。しかし、p-rank だけでは区別できないアソシエーションスキームも存在しているため、別の観点から調べる必要があります。§4では、half-case アソシエーションスキームから定義される線形符号を考えます。また、その最小距離や weight distribution を考え、また、いくつかの例や実験の結果を説明します。

この報告書で使う記号を定義します。I で単位行列、J で全成分が 1 である行列、O で零行列を表します。また、行列 M に対して、${}^tM$ で M の転置行列を表します。p は素数を表し、標数 p の体を $\mathbb{F}_p$ とかきます。有理整数環 $\mathbb{Z}$ 上の行列 M に対し、M の *p-rank* を M の $\mathbb{F}_p$ 上での rank で定義し、$\mathrm{rank}_p(M)$ とかく。

2 Conference matrices and their p-ranks

この章では、conference matrix を定義し、いくつかの性質を与える。

$m \times m$ 行列 C がサイズ m の *conference matrix* であるとは、C が次の条件を満たすときにいう:

(1) C の対角成分が0、その他の成分は1または -1

(2) ${}^tCC = (m-1)I$

conference matrix C は $C{}^tC = (m-1)I$ も満たしていて、これらの性質はいくつかの行や列を -1 倍しても保たれる。そのため、conference matrix C と C' に対し、$C' = DCD'$ を満たす対角行列で、対角成分が $\{1, -1\}$ である行列 D と D' が存在するとき、C と C' は**同値**であるという。C と C' が同値であるとき、任意の素数 p に対して $\mathrm{rank}_p(C)$ と $\mathrm{rank}_p(C')$ は等しくなる。conference matrix の性質は [12, §18] と [2, §52] に書かれている。

サイズ m の conference matrix が存在するなら、m は1または偶数である。([2, §52]) 以下では、自明な例外を除くために、C と書いたらサイズが $m \geq 4$ の conference matrix を表すことにする。そのため、m は常に偶数で考える。conference matrix C が ${}^tC = C$ (または ${}^tC = -C$) を満たすとき、**対称** (または **歪対称**) という。conference

matrix Cは、$m \equiv 2 \pmod 4$であるとき対称 conference matrix と同値になり、$m \equiv 0 \pmod 4$であるとき歪対称 conference matrix と同値になることは簡単に分かる。さて、conference matrix のいくつかの性質について考える。

命題 2.1. $p \nmid m-1$ ならば、$\mathrm{rank}_p(C) = m$。$p \mid m-1$ ならば、$\mathrm{rank}_p(C) \leqq m/2$。特に、$p \mid m-1$ *and* $p^2 \nmid m-1$ ならば、$\mathrm{rank}_p(C) = m/2$。

combinatorial design に対しても、[8] において似た結果が得られている。

conference matrix の p-rank は素数 p が $p \mid m-1$ と $p^2 \nmid m-1$ を満たすとき、サイズ m のみによって決まる。しかし、$p^2 \mid m-1$ のとき、一般には m に対して p-rank は一定ではない。そのような例を Remark 3.6 で示す。

$1 \leqq k \leqq m$ に対し、conference matrix $C = (c_{ij})$ が任意の $\ell \neq k$ で $c_{k\ell} = 1$ と $c_{\ell k} = (-1)^{m/2+1}$ を満たしているとき、k で**正規化されている**という。conference matrix C と $1 \leqq k \leqq m$ に対し、対称か歪対称な conference matrixC' であって、k で正規化されているものがただ 1 つ存在する。この C' を k での C の**正規化**という。

3 Half-case association schemes and p-ranks

この章では、アソシエーションスキームを定義する。次に、conference matrix とアソシエーションスキームの関係を考える。その後、conference matrix から得られるアソシエーションスキームの隣接代数の元の p-rank を調べる。また、p-rank と標準表現の関係についても述べる。

定義 3.1. n 次の非零行列であって、成分が 0,1 の行列の集合 $\{A_0, \ldots, A_\ell\}$ が以下を満たすとき、**アソシエーションスキーム** (association scheme) であるという。

(1) $\sum_{i=0}^{\ell} A_i = J$、ただし J は全成分が 1 の行列

(2) $A_0 = I$、ただし I は単位行列

(3) 任意の i に対して、${}^tA_i$ は集合に属している

(4) 任意の i, j, k に対して、$A_iA_j = \sum_{k=0}^{\ell} p_{ij}^k A_k$ を満たす非負整数 p_{ij}^k が存在する

アソシエーションスキーム $\{A_0, \ldots, A_\ell\}$ が任意の i に対して ${}^tA_i = A_i$ を満たすとき、**対称**であるという。また、定義の中に表れる非負整数 p_{ij}^k を**交叉数**という。

K を体、$S = \{A_0, \ldots, A_\ell\}$ をアソシエーションスキームとする。また、S によって張られる K 上の空間を KS とおく。このとき KS は全行列代数 $M_n(K)$ の部分代数になっていて、これを S の K 上の**隣接代数**という。

また、K^n を n 次元の K 上の線形空間とする。このとき、K^n に KS の右からの作用を行列の積で定義すると、K^n は右 KS 加群になる。これを S の K 上の**標準加群**という。

K^n を n 次元 K ベクトル空間とする。このとき、K^n は右からの積によって、右 KS 加群となる。この作用をもつ加群 KS を K 上 S の**標準加群**という。標準加群から得られる KS の表現を K 上 S の**標準表現**という。

$S = \{A_i \mid i = 0, \ldots, \ell\}$、$S' = \{A'_i \mid i = 0, \ldots, \ell'\}$ をアソシエーションスキームとする。また、S と S' の交叉数をそれぞれ p_{ij}^k、$p_{ij}'^k$ とする。このとき、S と S' が $\ell = \ell'$ を満たし、さらに置換行列 P と $\{0, 1, \ldots, \ell\}$ 上の置換 σ が存在し、任意の i に対して $P^{-1}A_iP = A'_{\sigma(i)}$ が成り立つとき、S と S' は**同型**であるという。また、S と S' が $\ell = \ell'$ を満たし、さらに $\{0, 1, \ldots, \ell\}$ 上の置換 σ が存在し、任意の i, j, k に対して $p_{ij}^k = p'^{\sigma(k)}_{\sigma(i)\sigma(j)}$ が成り立つとき、S と S' は**代数的に同型**であるという。

アソシエーションスキーム S が conference graph [4, §10.2] に対応しているか、あるいは、$|S| = 3$ である非対称アソシエーションスキームのとき、*half-case* であるという。S が half-case であることは、次の命題 3.2 の証明中にある交叉数をもつことと同値であることに注意する。half-case アソシエーションスキームは conference matrix と次のような関係がある。

命題 3.2. $1 \leqq k \leqq m$ を満たす k を固定する。C' は k での C の正規化とする。$A = (a_{ij})$ を C' の k 行目と k 列目を取り除いて得られる行列とする。このとき、$\{A_0 = (\delta_{i,j})_{ij},\ A_1 = (\delta_{1,a_{ij}})_{ij},\ A_2 = (\delta_{-1,a_{ij}})_{ij}\}$ は位数 $n = m - 1$ の *half-case* アソシエーションスキームになる。

このようにして作られたアソシエーションスキームは次の交叉数を持っている。

- $n \equiv 0 \pmod 4$ のとき、

$$\begin{aligned} A_1^2 &= \frac{n-3}{4}A_1 + \frac{n+1}{4}A_2, \\ A_1A_2 = A_2A_1 &= \frac{n-1}{2}A_0 + \frac{n-3}{4}A_1 + \frac{n-3}{4}A_2, \\ A_2^2 &= \frac{n+1}{4}A_1 + \frac{n-3}{4}A_2. \end{aligned}$$

- $n \equiv 2 \pmod 4$ のとき、

$$\begin{aligned} A_1^2 &= \frac{n-1}{2}A_0 + \frac{n-5}{4}A_1 + \frac{n-1}{4}A_2, \\ A_1A_2 = A_2A_1 &= \frac{n-1}{4}A_1 + \frac{n-1}{4}A_2, \\ A_2^2 &= \frac{n-1}{2}A_0 + \frac{n-1}{4}A_1 + \frac{n-5}{4}A_2. \end{aligned}$$

上ようにして得られる half-case アソシエーションスキームを C と k から得られる**アソシエーションスキーム**といい、$\mathrm{AS}(C, k)$ とかく。アソシエーションスキーム $\mathrm{AS}(C, k)$ と $\mathrm{AS}(C, k')$ は必ずしも同型ではないが、代数的には同型になる。

逆の手順で、half-case アソシエーションスキームから conference matrix が構成できることは容易に分かる。

注意 3.3. $\mathrm{AS}(C,k)=\{A_0,A_1,A_2\}$とおく。$p\nmid n$とする。このとき、$\mathrm{rank}_p(A_1-A_2)=n-1$となり、一定である。そのため、$\mathrm{rank}_p(A_1-A_2)$はアソシエーションスキームの分類には使えない。

さて、conference matrix Cのp-rankとアソシエーションスキーム$AS(C,k)$について考える。

補題 3.4. Bを$C=(c_{ij})$のi行目とj列目を取り除いて得られる行列とする。$p\mid m$とする。このとき、$\mathrm{rank}_p(B)=\mathrm{rank}_p(C)$となる。とくに、$\mathrm{AS}(C,k)=\{A_0,A_1,A_2\}$とすると、$\mathrm{rank}_p(A_1-A_2)=\mathrm{rank}_p(C)$が成り立つ。

補題 3.4より、以下の定理を得る。

定理 3.5. $\mathrm{AS}(C,i)=\{A_0,A_1,A_2\}$、$\mathrm{AS}(C,j)=\{A_0',A_1',A_2'\}$とおく。このとき、$\mathrm{rank}_p(A_1-A_2)=\mathrm{rank}_p(A_1'-A_2')$が成り立つ。

補題2.1より、$m-1$でわり切れるかどうかに応じて、conference matrixのp-rankが決まるかどうかがわかった。一方、$m-1$をp^2が割り切る場合、同じサイズのconference matrixであっても、異なるp-rankをもつことがある。しかし、同じconference matrixから得られるアソシエーションスキームに対しては、p-ranksは一定である。

注意 3.6. [6]にある位数25のアソシエーションスキームの4番目から9番目について、A_1-A_2の5-rankは全て異なっている。したがって、それらに対応するconference matrixは全て異なることが分かる。同様に、位数27のアソシエーションスキームの5番目と6番目については、対応するconference matriceは異なっている。

[1, §4.1]と[5, Corollary 4.4]において、cyclotomicアソシエーションスキームとPaleyグラフに対するp-rankが調べられている。

これから、p-rankと標準表現の関係を説明する。$\mathrm{rank}_p(A_1-A_2)$を考えることで、標準表現を理解できる。

$S=\{A_0,A_1,A_2\}$を位数nのhalf-caseアソシエーションスキームとする。Kを標数pの体とする。$p\mid n$と仮定する。このとき、はじめに、[7, Theorem 10 and Theorem 12]より、$KS\cong K[x]/(x^3)$が分かる。K上でA_1-A_2は$\overline{x}\in K[x]/(x^3)$に対応する元である。よって、3つだけ直規約表現がある。

$$M_1:\overline{x}\mapsto\begin{pmatrix}0\end{pmatrix},\quad M_2:\overline{x}\mapsto\begin{pmatrix}0&1\\0&0\end{pmatrix},\quad M_3:\overline{x}\mapsto\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}.$$

ある非負整数m_i $(i=1,2,3)$によって、A_1-A_2が$m_1M_1\oplus m_2M_2\oplus m_3M_3$に対応することは分かる。また、$\mathrm{rank}_p((A_1-A_2)^2)=1$であるので、$m_3=1$がわかる。さらに、

$$\mathrm{rank}_p(A_1-A_2)=m_2+2$$

であるので、$m_1+2m_2+3m_3=n$ より、$m_1=n-2m_2-3=n-2\,\mathrm{rank}_p(A_1-A_2)+1$ が得られる。したがって、A_1-A_2 の p-rank によって、標準表現の同値類は完全に決定し、その逆も成り立つ。

元 $\alpha=aA_0+b(A_1-A_2)+c(A_1-A_2)^2\in KS$ は

$$m_1\begin{pmatrix}a\end{pmatrix}\oplus m_2\begin{pmatrix}a & b\\ 0 & a\end{pmatrix}\oplus\begin{pmatrix}a & b & c\\ 0 & a & b\\ 0 & 0 & a\end{pmatrix}$$

に対応し、$\mathrm{rank}(\alpha)$ は $\mathrm{rank}_p(A_1-A_2)$ のみで決まる。そのため、我々の議論では $\mathrm{rank}_p(A_1-A_2)$ を考えるだけで十分であると言える。[11] では、Peeters が他の元で p-rank を決めていたが、我々の議論では $\mathrm{rank}_p(A_1-A_2)$ でよい。

4 Linear codes of half-case association schemes

skew-Hadamard design の関係行列のスミス標準形は行列のサイズで決まる [9]。したがって、その p-rank は行列のサイズのみによって決まる。そのため、それを生成行列にもつコードが研究されている。例えば、[10] がある。

さて、前の章では half-case アソシエーションスキームの標準加群は p-rank 以上の情報を持っていないことが分かった。そのため、この章では、p-rank よりも多くの情報を得るために線形符号を考える。特に、符号の最小距離と weight distribution を調べることで、いくつかの場合において、p-rank では区別できないアソシエーションスキームを区別できることを示す。

F を標数 p の体とする。F^n の部分空間 V を長さ n の *(linear) code* という。普通、V の次元を k とする。ベクトル $\boldsymbol{v}=(v_1,\dots,v_n)\in F^n$ に対して、$\mathrm{wt}(\boldsymbol{v})=|\{i\mid v_i\neq 0\}|$ は $\boldsymbol{v}$ の**ハミングウェイト**という。また、$d=\min\{\mathrm{wt}(\boldsymbol{v})\mid \mathbf{0}\neq\boldsymbol{v}\in V\}$ は V の**最小距離**という。$a_i=|\{\boldsymbol{v}\in V\mid \mathrm{wt}(\boldsymbol{v})=i\}|$ を各成分にもつベクトル $(a_0,a_1,\dots,a_d)$ は V の *weight distribution* という。また、(n,k,d) は符号 V の**パラメータ**という。

行列 M に対し、M の各行で張られる符号を M **の符号**という。half-case アソシエーションスキームに対し、A_1-A_2 の符号の最小距離の上限はすぐに分かる。

命題 4.1. F を標数 p の有限体とする。$\{A_0,A_1,A_2\}$ を位数 n の *half-case* アソシエーションスキームとし、V を F 上の A_1-A_2 の符号とする。$p\mid n$ とする。このとき、V の最小距離は $(n+1)/2$ 以下となる。

half-case アソシエーションスキームの符号に対して、あまり良い結果は得られていないが、いくつかの例を挙げる。[6] にあるアソシエーションスキームの分類と、計算のために GAP[3] の GUAVA パッケージを用いた。

例 4.2 (位数 25, $p=5$). 位数 25 に対し、[6] にある 4 番目から 11 番目までのアソシエーションスキームは half-case である。A_1-A_2 の F_5 上の符号のパラメータは次の

通りである：

$$(n,k,d) = (25,12,7),\ (25,11,7),\ (25,9,13).$$

パラメータ k はちょうど $A_1 - A_2$ の p-rank に等しいことと、$(n,k,d) = (25,9,13)$ が命題 4.1 における上限を満たしていることに注意せよ。データは書かないが、weight distributions は全て異なっていた。

例 4.3 (位数 27, $p = 3$). 位数 27 に対し、[6] にある 5 番目から 378 番目までのアソシエーションスキームは half-case である。$A_1 - A_2$ の F_3 上の符号のパラメータは次の通りである：

$$\begin{aligned}(n,k,d) \ = \ & (27,8,14),\ (27,10,5),\ (27,10,6),\ (27,12,5),\ (27,12,6),\\ & (27,12,8),\ (27,14,5),\ (27,14,6),\ (27,14,8).\end{aligned}$$

それらのいくつかは同じ weight distribution を持っている。例えば、11 番目と 13 番目が同じである。

参考文献

[1] A. E. Brouwer and C. A. van Eijl, *On the p-rank of the adjacency matrices of strongly regular graphs*, J. Algebraic Combin. **1** (1992), no. 4, 329–346.

[2] C. J. Colbourn and J. H. Dinitz (eds.), *The CRC handbook of combinatorial designs*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1996.

[3] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8*, 2016, (`http://www.gap-system.org`).

[4] C. D. Godsil, *Algebraic combinatorics*, Chapman and Hall Mathematics Series, Chapman & Hall, New York, 1993.

[5] A. Hanaki, *Modular adjacency algebras, standard representations, and p-ranks of cyclotomic association schemes*, J. Algebraic Combin. **44** (2016), no. 3, 587–602.

[6] A. Hanaki and I. Miyamoto, *Classification of association schemes with small vertices*, published on web http://math.shinshu-u.ac.jp/~hanaki/as/.

[7] A. Hanaki and M. Yoshikawa, *On modular standard modules of association schemes*, J. Algebraic Combin. **21** (2005), no. 3, 269–279.

[8] M. Klemm, *Über den p-Rang von Inzidenzmatrizen*, J. Combin. Theory Ser. A **43** (1986), no. 1, 138–139.

[9] T. S. Michael and W. D. Wallis, *Skew-Hadamard matrices and the Smith normal form*, Des. Codes Cryptogr. **13** (1998), no. 2, 173–176.

[10] A. Munemasa and H. Tamura, *The codes and the lattices of Hadamard matrices*, European J. Combin. **33** (2012), no. 4, 519–533.

[11] R. Peeters, *On the p-ranks of the adjacency matrices of distance-regular graphs*, J. Algebraic Combin. **15** (2002), no. 2, 127–149.

[12] J. H. van Lint and R. M. Wilson, *A course in combinatorics*, second ed., Cambridge University Press, Cambridge, 2001.