Skew-symmetric Hadamard matrices and association schemes of prime order

Akihide HANAKI (Shinshu University)

March 3, 2000

アソシエーションスキーム (以下、単にスキームという) は代数的組合せ論の中心的研究対象であり、多くの研究がなされているが、その一般論は難しく、特に有限群と関係しない場合についてはほとんど何も分かっていない。スキームの研究において次の問題は基本的であり、かつ最も重要である。

問題. すべての (原始的な) アソシエーションスキームを分類せよ。

すべてのスキームを分類することはすべての有限群を分類することをある意味では完全に含んでいるため実現はほぼ不可能である。原始的なスキームの分類は有限単純群の分類をほぼ含んでいる。有限単純群の分類は完成しているので、この問題は実現の望みがあるようにも思われるが、実際には多くの問題があり、今のところ手がかりすら得られてはいない。

最も簡単な有限単純群は素数位数巡回群である。スキームにおいても、素数位数のものは常に原始的になる。しかしながら素数位数の場合に限ってもスキームの分類は困難であり、今のところ解決の糸口すら掴めないでいる。今回の話は素数位数のスキームの分類に対する一つのアプローチであり、きちんとした結果が得られたということではないことをはじめに断っておく。目的としたのは、素数位数のスキームで有限群からは得られないものを理解することである。今回は、この問題に対する十分な結果とはいえないが、ある素数位数のスキームの変形で別のスキームが得られることを示した。その際に利用したのが歪対称アダマール行列である。

1 定義と知られている分類

X を有限集合とする ($|X| = n$)。$R_i \subset X \times X$, $i = 0, 1, \cdots, d$ とする。X で添字の付けられた $n \times n$ 行列 A_i を次のように定義する。

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

A_i を隣接行列という。$(X, \{R_i\})$ がアソシエーションスキーム (以下、単にスキームという) であるとは、次の条件が満たされることとする。

(1) $A_0 = I$ (単位行列)

(2) $\sum_{i=0}^{d} A_i = J$ (すべての成分が 1 の行列)

(3) 任意の i に対してある i' があって ${}^tA_i = A_{i'}$

(4) ある整数 p_{ij}^k があって $A_iA_j = \sum_{k=0}^{d} p_{ij}^k A_k$

$|X| = n$ をスキームの位数といい、構造定数 $p_{ii'}^0$ を関係 R_i の valency という。詳しくは [1] を参照。

スキームはもともと可移置換群から得られる Hecke 環の拡張として定義された。すなわち G を X 上の可移置換群とするとき、G は自然に $X \times X$ にも作用する。このとき R_i を $X \times X$ 上の G の軌道とすればスキームが得られる。特に原始的な可移置換群からは原始的なスキームが得られる。ただし二重可移な置換群からは自明なスキームしか得られない。多くの “よい” 性質を持つスキームはこのようにして可移置換群から得られるが、後で問題にするのはそうでない場合である。

スキームを完全に記述するためにはすべての隣接行列を記述すればよいが、紙面の節約のために関係行列

$$R = \sum_{i=0}^{d} iA_i.$$

を用いる。スキームの構造は関係行列で完全に記述される。

二つのスキームが同型であるとは、隣接行列の行と列の入れ換え、および番号の付け替えで移りあうこととする。行と列の入れ換えは集合 X を並べる順番を替えることに過ぎず、また番号の付け替えも R_i の添字を替えることに過ぎないからである。

現在までに計算機を用いたスキームの分類として得られている情報はホームページで公開している [3]。スキームと有限群の同型類の数は以下の様になっている。

order	♯ of a. s.	♯ of f. g.	order	♯ of a. s.	♯ of f. g.
5	3	1	19	7	1
6	8	2	20	95	5
7	4	1	21	32	2
8	21	5	22	16	2
9	12	2	23	22	1
10	13	2	24	750	15
11	4	1	25	45	2
12	59	5	26	34	2
13	6	1	27	502	5
14	16	2	28	185	4
15	25	1			
16	222	14			
17	5	1			
18	95	5			

ここで注目したいのが素数位数の場合である。素数点上の原始的置換群は二重可移であるか、または次のような構造を持つ。考える素数を p とする。$X = GF(p)$ として $GF(p)$ の自己同型群 $A \cong GF(p)^\times$ を考える。A の部分群 H に対して半直積 $GF(p) : H$ は X 上原始的な置換群となる。この置換群から先に述べた方法で得られるスキームを cyclotomic なスキームという。明らかに cyclotomic スキームは $p-1$ の約数の個数だけ存在する。

このように考えて上の表の同型類の数を見ると $p \leq 17$ では cyclotomic しかないが、$p = 19$ に一つ、$p = 23$ には 18 の non-cyclotomic スキームがあることが分かる。可移置換群から得られるスキームでなくとも、有限群と強く関係しているスキームでは、その自己同型群を調べればその中に関係する有限群が現れる。しかし、これらの cyclotomic でない場合には、その自己同型群の位数がとても小さく、その情報からスキームを説明することはほぼ不可能である。

2 歪対称アダマール行列

H を $n \times n$ 行列でその成分はすべて 1 または -1 であるとする。H がアダマール行列であるとは

$$^tHH = nI$$

を満たすことと定義する (I は単位行列)。また H が歪対称アダマール行列であるとは、アダマール行列であって、さらにある交代行列 A を使って

$$H = I + A$$

と表されることとする。アダマール行列であることは、各行 (列) ベクトルが互いに直行するということと同値である。したがってアダマール行列の行の置換やある行の成分をすべて -1 倍するという操作で、アダマール行列であるということは変わらない。列についても同様である。

アダマール行列についてよく知られた結果と未解決問題を紹介しておく。

定理. H がアダマール行列ならば $n = 1, 2$ または $n \equiv 0 \pmod 4$ である。

予想. 任意の自然数 m に対して $4m \times 4m$ のアダマール行列が存在する。

定理. $4m-1$ が素数べきならば $4m \times 4m$ の歪対称アダマール行列が存在する。

アダマール行列はデザインと関係が深い。詳しくは [2] を見て頂きたい。

3 アダマール行列とアソシエーションスキーム

ここではアダマール行列を使って、一つのスキームから別のスキームを構成する方法について説明する。一般には必ずしも非同型なものが得られるわけではなく、どのようなときに新しいものが得られるかは分かっていない。この方法が適用できるのは n が $n \equiv 3 \pmod 4$ なる素数べきで、valency が $\{1, (n-1)/2, (n-1)/2\}$ の場合に限られる。しかし位数 19, 23 の cyclotomic でないものはいずれもこの条件を満たしている。ここでは簡単のため $n = 7$ として方法を説明する。

$n=7$ の cyclotomic スキームは以下のような関係行列と隣接行列を持つ。

$$R=\begin{pmatrix}
0&1&1&2&1&2&2\\
2&0&1&1&2&1&2\\
2&2&0&1&1&2&1\\
1&2&2&0&1&1&2\\
2&1&2&2&0&1&1\\
1&2&1&2&2&0&1\\
1&1&2&1&2&2&0
\end{pmatrix}$$

$$A_0=\begin{pmatrix}
1&0&0&0&0&0&0\\
0&1&0&0&0&0&0\\
0&0&1&0&0&0&0\\
0&0&0&1&0&0&0\\
0&0&0&0&1&0&0\\
0&0&0&0&0&1&0\\
0&0&0&0&0&0&1
\end{pmatrix}
\quad
A_1=\begin{pmatrix}
0&1&1&0&1&0&0\\
0&0&1&1&0&1&0\\
0&0&0&1&1&0&1\\
1&0&0&0&1&1&0\\
0&1&0&0&0&1&1\\
1&0&1&0&0&0&1\\
1&1&0&1&0&0&0
\end{pmatrix}
\quad
A_2=\begin{pmatrix}
0&0&0&1&0&1&1\\
1&0&0&0&1&0&1\\
1&1&0&0&0&1&0\\
0&1&1&0&0&0&1\\
1&0&1&1&0&0&0\\
0&1&0&1&1&0&0\\
0&0&1&0&1&1&0
\end{pmatrix}$$

この隣接行列から次のようにして $(n+1)\times(n+1)$ 行列を作る。

$$\left(\begin{array}{c|ccc}
1&1&\cdots\cdots&1\\
\hline
-1&&&\\
\vdots&&A_0+A_1-A_2&\\
-1&&&
\end{array}\right)=\left(\begin{array}{c|ccccccc}
1&1&1&1&1&1&1&1\\
\hline
-1&1&1&1&-1&1&-1&-1\\
-1&-1&1&1&1&-1&1&-1\\
-1&-1&-1&1&1&1&-1&1\\
-1&1&-1&-1&1&1&1&-1\\
-1&-1&1&-1&-1&1&1&1\\
-1&1&-1&1&-1&-1&1&1\\
-1&1&1&-1&1&-1&-1&1
\end{array}\right)$$

この行列が歪対称アダマール行列であることは直ちに分かる。この行列の一行、一列はきれいな形をしている。これを行と列を -1 倍することで i 行、i 列に移す。これを i で正規化するということにする。例えば上の行列を 3 で正規化すると

$$\left(\begin{array}{cc|c|cccc}
1&1&-1&-1&-1&1&-1&1\\
-1&1&-1&-1&1&1&1&-1\\
\hline
1&1&1&1&1&1&1&1\\
\hline
1&1&-1&1&1&-1&-1&-1\\
1&-1&-1&-1&1&-1&1&1\\
-1&-1&-1&1&1&1&-1&1\\
1&-1&-1&1&-1&1&1&-1\\
-1&1&-1&1&-1&-1&1&1
\end{array}\right)$$

となる。この 3 行と 3 列を取り除いて、更に今までの逆を辿れば新たな隣接行列

A'_0, A'_1, A'_2 を得る。

$$\left(\begin{array}{cc|ccccc} 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 & -1 & 1 & 1 \end{array}\right) = A'_0 + A'_1 - A'_2$$

これより新しいスキーム

$$\begin{pmatrix} 0 & 1 & 2 & 2 & 1 & 2 & 1 \\ 2 & 0 & 2 & 1 & 1 & 1 & 2 \\ 1 & 1 & 0 & 1 & 2 & 2 & 2 \\ 1 & 2 & 2 & 0 & 2 & 1 & 1 \\ 2 & 2 & 1 & 1 & 0 & 2 & 1 \\ 1 & 2 & 1 & 2 & 1 & 0 & 2 \\ 2 & 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

が得られる。

上の $n = 7$ の例では結果として得られたものは元のスキームと同型なものである。しかし一般には非同型なものが得られる場合がある。位数 23 で valency が $\{1, 11, 11\}$ のものは cyclotomic を含めて 19 個ある。[3] の番号でいうと No. 2 から 20 である。これらについて上の方法を試すと

$$\{2, 11\}, \{3, 5, 7, 16\}, \{4, 6\}, \{8, 15, 17\}, \{9, 10, 13\}, \{12, 14\}, \{18\}, \{19\}, \{20\}$$

と分類される。つまり No. 2 から No. 11 が構成されるといった具合である。cyclotomic は No. 20 で、残念ながらこれから別のスキームを構成することは出来なかった。また、素数位数ではないが $n = 27$ のときもこの方法が適用できるものはたくさんある。

以上、現在のところ単なる試行でしかないが、それまで関係の分からなかった non-cyclotomic スキームが、ある関係で結ばれることが分かったのは意味のある結果であると思われる。また、講演の原稿を準備しているときには素数位数の non-cyclotomic スキームは $n \equiv 3 \pmod 4$ のものしかなかったが、その後 $n = 29$ でも例が構成された。上の方法はこれには適用できないので新たな方法を考える必要がある。

References

[1] E. Bannai and T. Ito, Algebraic Combinatorics I : Association Schemes, Benjamin / Cummings, Menlo Park CA, 1984.

[2] T. Beth, D. Jungnickel, and H. Lenz, Design Theory, Cambridge, 1985.

[3] A. Hanaki and I. Miyamoto, Data of association schemes, http://kissme.shinshu-u.ac.jp/as.