数理解析研究所講究録
第178巻 1973年 59-64

等差集合とHadamard 行列

東女大　　山本幸一

1. Hadamard 行列，又はもっと一般な組合せ論的構図を論ずる際に，積極的に実例を示す方向と，反対にその不可能性を示す消極的な方向とがある．多くの実例は整数論的な構成に基づくので，その理由は複雑な構造を特殊な場合に制限してより簡単な数の問題に還元されるところにある．このことはたとえば電子計算機による探索にあたっても，次元の短縮が極めて効果的であることからも分る．

本稿では整数論的組合せ論とでも言うべき分野の一つの重要な対象，等差集合を主にしてそれに関連する話題を思い付くままに説明することにしたい．

2. v 個の元から成る集合 Ω の k 部分集合とは，Ω の元の k 個から成り立つ部分集合のことである．Ω の k 部分集合 v 個から成る集合 $\mathcal{F}$ が組合せ論的構図であるというのは，Ω の任意の元 x を含む $\mathcal{F}$ の元の個数が r に等しく，Ω の任意の2元 x, y を同時に含む $\mathcal{F}$ の元の個数が一定数 λ に等しいことである．パラメーター v, k, λ の間には

$$k(k-1)=(v-1)\lambda$$

なる関係がある．$\mathcal{F}$の各元をそのΩにおける余集合でおきかえて生ずる集合$\mathcal{F}'$も同じく組合せ論的構図で，そのパラメーターはv, k', λ'である．ここに

$$k'=v-k,\quad \lambda'=v-2k+\lambda.$$

(v,k,λ)-構図$\mathcal{F}$において

$$n=k-\lambda$$

なる量が重要な役割を持つ．たとえば$n=k'-\lambda'$である．

v行v列の$(0,1)$-行列Mが(v,k,λ)-構図を記述する行列であると，前述の条件は

$$JM=MJ=kJ,\quad M^tM=nI+\lambda J$$

と書き替えられる．ここでIは単位行列で，Jは凡ての成分が1なる正方行列である．$\mathcal{F}'$は行列$J-M$で記述される．

3．(v,k,λ)構図でパラメーターnを中心的に考えることにする．事実nの大小が$\mathcal{F}$の複雑さをかなり忠実に反映することが知られている．たとえば$n=0$，$n=1$はいわゆる自明な構図しか与えることができない．

nに次いで重要な量はvであるが，与えられたnの値に対してvの取り得る範囲は

$$4n-1\leqslant v\leqslant n^2+n+1$$

を満たし，しかも

$s=v^2-4nv+4n$ が完全平方

でなければならない．このことは

$$\lambda+\lambda'=v-2n,\quad \lambda\lambda'=n(n-1)$$

からの帰結である．

上記の範囲で v の最小値 $v=4n-1$ は Hadamard 型の構図に対応し，同じく v の最大値 $v=n^2+n+1$ は射影平面に対応する．これら両極端の場合が最も頻繁に研究がなされているものである．

ここで v が最小値 $4n-1$ を1つだけ超過する場合を取り上げれば $s=4n$ の完全平方なることから n が完全平方である必要がある．この形の構造はそれ程研究が行われていないようである．

4. 以上は一般論だが，集合 Ω が群であり，その正則表現を通して Ω に作用しているものと考えて，それを 2^Ω に拡張した時，$\mathbf{F}$ がその作用の下で閉じていてしかも単一の軌道から成るものと仮定しよう．すなわち $\mathbf{F}$ はその中の一つの元 D から Ω を作用させることによって生ずるものと仮定するのである．この際集合 D を Ω の等差集合といい，v, k, λ をパラメーターとして継承する．

特に v 位の巡回群 Ω を基礎におく時には D を巡回等差集合という．前記の例では，$v=p=4n-1$ が素数で D が法 p の

平方剰余の全体である場合とか，$v=n^2+n+1$ で n は素数巾，そして $\mathbf{F}$ が有限体 $GF(n)$ 上の解析的射影平面を表わしている場合は周知であるが，これらは又，巡回等差集合の例でもある．

巡回等差集合については，$\mathbf{F}$ を記述する行列 M の満たすべき条件は数量的な等式となって現われる．それは群行列が本質的に固有値で決定されることからの結果である．詳しく言えば，Ω は有理整数を法 v で還元した加法群として，Ω の等差集合 D からその生成函数

$$f(x)=\sum_{a\in D} x^a$$

を定義する．これは $(\mathrm{mod}\ x^v-1)$ で確定する．そして D の満足すべき条件は

$$f(1)=k,\qquad |f(\zeta)|=\sqrt{n}$$

となる．ここで ζ は1の v 乗根 $\neq 1$ であり，当然のことながら複素数として考えるのである．この条件は v が与えられた時画一的な近似計算ができる点では行列等式の検算にくらべてはるかに便利であり，その方法の応用は広い．というのは完全な等差集合でない場合でもある程度その手法が準用できるからである．

5. Ω は v 位巡回群，Γ は有限群で有理整係数で群環 R を作り，それと円周等分体 $Q(\zeta_v)$，$\zeta_v=e^{2\pi i/v}$ の整数環

$\mathbf{Z}[\zeta_v]$ の直積 K の中の元 $\xi=\sum_{\gamma\in\Gamma} a_\gamma \gamma$, $a_\gamma\in\mathbf{Z}[\zeta_v]$ の共役 ξ を $\xi=\sum_{\gamma\in\Gamma}\bar{a}_\gamma\gamma^{-1}$ で定義する. 多くの整数論的組合せ論の問題が

$$\xi\bar{\xi}=c,\quad c\in\mathbf{Z}$$

の形に書き表わされることが認められる. c は予め指定された値である. 前記巡回等差集合においては $\Gamma=\{I\}$, $c=n$ であり, 又これに関係する e 乗剰余指標に対する Gauss の和では, Γ が 1 の e 乗根の乗法群である. さらに Williamson 型の Hadamard 行列については, Γ が非可換な群, 四元数群となる. K からのノルム形式が取り扱い易い形であれば, いくつかの候補に対して簡単な近似計算を電子計算機に行なわせることも比較的容易にできることになる.

他の例で言えば, ある代数体の単数 $\varepsilon_1,\varepsilon_2,\varepsilon_3$ の和が 0 になることが自明の場合 $\varepsilon_1+\varepsilon_2=0$ 等以外にあるかという chowla の問題等が考えられる.

6. 循環 Hadamard 行列は, その第 1 行を順次 1 コマづつずらして得られる Hadamard 行列 H のことで, 適当な整数 t に関して

$$HJ=JH=tJ,\quad HH^*=vI$$

を成立させる. そのさい

$$M=\frac{1}{2}(H+J)$$

は v 行 v 列の $(0,1)$-行列で

$$MJ=JM=\frac{1}{2}(t+v)J,\quad M^{*}M=\frac{1}{4}\left(vI+(2t+v)J\right)$$

が成立する．従って v は4の倍数で，M は $n=\frac{v}{4}$ なる値をもつ構図を記述する行列となる．§3 から n が完全平方であることが必要となる．

$n=N^2$ とおいて，パラメーター

$$v=4N^2,\quad n=N^2>1$$

を有する巡回等差集合は存在しない という Ryser の推測があり，Turyn のすぐれた研究があるが，問題は現在未解決のようである．

Baumert の本に載せられている式の，代数体の理論の応用によって $N\leqslant 100$ ぐらいまでは非存在が確認される．それは $v\leqslant 40000$ というのに等しいから，問題がすでに実用の範囲を遠く離れていることは事実である．

文献

R. Turyn: Sequences with Small Correlation, *Error Correcting Codes*, Wiley, 1968, pp. 195-228.

L. D. Baumert: Cyclic Difference Sets, Lecture Notes in Mathematics, vol. 182 (1971).

山本幸一：等差集合の電子計算機による探査，数理解析研究所講究録，155 (1972), pp. 43-55.