Hadamard Matrices

Mitsuru Takigahira

アダマール行列と符号

多くの数学的構造は符号を作るために利用できる。ある興味深い種類の符号はアダマール行列と呼ばれる行列から作れる。最初にこれらの行列の初歩的な性質について調べよう (詳細は [Ha67, MS77] を見よ)

定義 アダマール行列

アダマールは与えられた各 n に対し、
$n \times n$ 実行列 H の行列式がどれだけ大きく出来るかに興味を持った。
この問題に意味づけるために H の要素に制限が必要であるが、
全ての i, j に対して、$| h_{ij} | \leq 1$ としても一般性を失わない。
これらの条件の下、アダマールは $| \det H | \leq n^{n/2}$ の等号成立が

(a) 各 $h_{ij} = \pm 1$ かつ

(b) H の相異なる行 $\mathbf{r}_i$ は直交する、つまり $i \neq j$ なる全ての i, j に対し、$\mathbf{r}_i . \mathbf{r}_j = 0$

の必要十分条件であることを証明した。

定義 アダマール行列

(a) 及び (b) を満たす $n \times n$ 行列 H は、n 次アダマール行列と呼ばれる。
(a) は全ての i に対して $\mathbf{r}_i.\mathbf{r}_i = n$ を意味し、HH^T が対角行列

$$HH^T = \begin{pmatrix} n & 0 & \cdots & 0 \\ 0 & n & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & n \end{pmatrix} = nI_n; \tag{6.8}$$

であることがわかる。ここで、
H^T は H の転置行列を意味し、I_n は $n \times n$ の単位行列である。

定義 アダマール行列

$\det H^T = \det H$ より、(6.8) から

$$(\det H)^2 = \det(nI_n) = n^n$$

よって、$|\det H| = n^{n/2}$ である。
このことから、全てのアダマール行列はアダマールの上界に達する。
この逆の証明は難しく、ここでは必要ないので省略する。

例 6.23

見やすさと印刷上の理由により、以下ではアダマール行列の -1 の成分を単に $-$ と記述する。

例 6.23

行列 $H = (1)$ と $\begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}$ はそれぞれ 1 次と 2 次のアダマール行列で、
$|\det H| = 1$ 及び 2 である。

練習 6.12

全ての 1 次及び 2 次のアダマール行列を求めよ。

補題 6.24

次の簡単な結果によって、大きなアダマール行列を小さなアダマール行列から作ることが出来る。

補題 6.24

H を n 次のアダマール行列とおく、そして H' を

$$H' = \begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

と置く。このとき、H' は $2n$ 次のアダマール行列となる。

練習 6.13

補題 6.24 を証明せよ。

系 6.25

系 6.25

各整数 $m \geq 0$ に対して 2^m 次のアダマール行列が存在する。

証明

$H = \begin{pmatrix} 1 \end{pmatrix}$ から始め、補題 6.24 を m 回適用すれば良い。

例 6.26

補題 6.24 の方法で得られる 2^m 次のアダマール行列は
シルベスター行列 (Sylvester matrices) と呼ばれている。
例えば $m = 1$ を取ると、$\begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}$ を与え、そして $m = 2$ に対して以下を得る。

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{pmatrix}$$

しかしながら、アダマール行列は全ての次数で存在するわけではない。例えば $n > 1$ なる奇数次のアダマール行列は存在しない。

補題 6.27

補題 6.27

$n > 1$ なる n 次のアダマール行列 H が存在する場合、n は偶数である。

証明

$i \neq j$ に対して行 $\mathbf{r}_i$ と $\mathbf{r}_j$ の直交性は $h_{i1}h_{j1} + \cdots + h_{in}h_{jn} = 0$ を与える。
それぞれの $h_{ik}h_{jk} = \pm 1$ で、よって n は偶数でなければならない。

補題 6.28

補題 6.28

$n > 2$ なる n 次のアダマール行列 H が存在する場合、n は 4 で割り切れる。

証明

H の任意の異なる行 $\mathbf{r}_i, \mathbf{r}_j$ に対して k 番目の要素に -1 をかけたものをそれぞれ $\mathbf{r}'_i, \mathbf{r}'_j$ としたとき、

$$\mathbf{r}_i . \mathbf{r}_j = r_{i1}r_{j1} + \cdots + r_{ik}r_{jk} + \cdots r_{in}r_{jn} = r_{i1}r_{j1} + \cdots + (-r_{ik})(-r_{jk}) + \cdots + r_{in}r_{jn} = \mathbf{r}'_i . \mathbf{r}'_j$$

となるので、任意の列に -1 をかけた行列はアダマール行列の性質を失わず、そのため最初の行 $\mathbf{r}_1$ は全ての要素が 1 と仮定して良い。
各行 $\mathbf{r}_i$ $(i \neq 1)$ は $\mathbf{r}_1$ と直交し、$n/2$ 個の要素は 1 で、残りの $n/2$ 個は -1 である。
列を交換すると (これも同様の議論からアダマール行列の性質を失わない)、以下のように仮定できる

$$\mathbf{r}_2 = \begin{pmatrix} 1 & 1 & \ldots & 1 & -1 & -1 & \ldots & -1 \end{pmatrix}$$

証明: 補題 6.28

証明

次に $\mathbf{r}_1, \mathbf{r}_2$ のそれぞれと異なる 3 つ目の行 $\mathbf{r}_3$ について考える
$\mathbf{r}_3$ の最初と最後の $n/2$ 個の要素がそれぞれ 1 を u 個と v 個含むとする (そして残りの要素が -1 となる)。 このとき

$$0 = \mathbf{r}_1 . \mathbf{r}_3 = u - \left(\frac{n}{2} - u\right) + v - \left(\frac{n}{2} - v\right) = 2u + 2v - n$$

さらに、

$$0 = \mathbf{r}_2 . \mathbf{r}_3 = u - \left(\frac{n}{2} - u\right) - v + \left(\frac{n}{2} - v\right) = 2u - 2v$$

よって、$u = v$ で、それゆえに $n = 2u + 2v = 4u$ は 4 で割り切れる。

この逆、つまり 4 で割り切れる n に対して、n 次のアダマール行列が存在することが推測できる。これは未だに未解決問題である。

定理 6.29

符号理論とアダマール行列の関係性は次の結果に基づいている。

定理 6.29

それぞれ n 次のアダマール行列 H から符号長 n で符号語数 $M = 2n$、最小距離 $n/2$ の二元符号を構成できる。

証明: 定理 6.29

アダマール行列からの符号の構成

1. $2n$ 個のベクトル $\pm\mathbf{r}_1, \ldots, \pm\mathbf{r}_n \in \mathbf{R}^n$ を H の各行 $\mathbf{r}_i$ から構成する
   - 行の直交性からこれらのベクトルは全て互いに素である。
2. -1 の要素を 0 に置き換えることにより、$0, 1$ の要素からなる $2n$ 個のベクトルを得る。
   - これらのベクトルは $\mathcal{V} = \mathbf{F}_2^n$ の元とみなすことが出来るので、これらは 2 元符号 C となる。

以上の構成法によって構成された任意の符号 C は符号長 n のアダマール符号と呼ばれ、このような符号で符号長 32 のものは 1969 年火星探査機マリナーからの写真伝送に使われた。

アダマール符号の性質

アダマール符号は以下のような性質を持つ。

アダマール符号の性質

- 符号語は $\bar{\mathbf{u}}_i = \mathbf{1} - \mathbf{u}_i$ のもと $\mathbf{u}_1, \bar{\mathbf{u}}_1, \ldots, \mathbf{u}_n, \bar{\mathbf{u}}_n$ の形になる。
- C は最小距離 $d = n/2$ を持つ。
    - 任意の i に対して、$d(\mathbf{u}_i, \bar{\mathbf{u}}_i) = n$
        - $\mathbf{u}_i$ と $\bar{\mathbf{u}}_i$ は全ての要素が異なっているため
    - $i \neq j \Rightarrow d(\mathbf{u}_i, \mathbf{u}_j) = d(\bar{\mathbf{u}}_i, \mathbf{u}_j) = d(\mathbf{u}_i, \bar{\mathbf{u}}_j) = d(\bar{\mathbf{u}}_i, \bar{\mathbf{u}}_j) = n/2$
        - アダマール行列の性質 (b) より各行の要素の $n/2$ が 1、残りの $n/2$ が 0 となるため

練習問題

練習 6.14

例 6.26 のアダマール行列 H から上記の方法によって得られる全ての符号語を求めよ。これらは線形符号か？

練習 6.15

8 次のアダマール行列を構成し、符号長 8 のアダマール符号を構成せよ。
この符号の伝送速度はどうなるか？この符号はどれだけの誤りを訂正できるか？そしてどれだけの誤りを検出するか？

アダマール符号の性質

n が 2 の累乗数でない場合、$2n$ もまた 2 の累乗数ではない。
よってそのような n に対して符号長 n のアダマール符号は線形にはなりえない。
任意の符号長 n のアダマール符号の伝送速度は

$$R = \frac{\log_2(2n)}{n} = \frac{1 + \log_2 n}{n} \to 0 \text{ as } n \to \infty$$

訂正可能な誤りの数は ($n > 2$ の場合) 定理 6.10 と 定理 6.29 と 系 6.28 から

$$t = \lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{n-2}{4} \rfloor = \frac{n}{4} - 1$$

なので、よって訂正される誤りの割合は

$$\frac{t}{n} = \frac{1}{4} - \frac{1}{n} \to \frac{1}{4} \text{ as } n \to \infty$$

となる。