数理解析研究所講究録
第1872巻 2014年 30-38



# 一般アダマール行列GH($q$, $q$)およびGH($q$, $q^2$)について

福岡大学　城戸　浩章
Hiroaki Kido
Fukuoka University

## 1 Introduction

**Definition 1.1.** $k\,(=u\lambda)$ 次正方行列 $[d_{ij}]$ が位数 $u$ の有限群 $U$ 上の**一般アダマール行列** GH($u$, $\lambda$) であるとは、

$$\sum_{1\leq j\leq k} d_{ij}d_{\ell j}^{-1} = \lambda\sum_{g\in U} g \in \mathbb{Z}[U]$$

$(1\leq i\neq \ell\leq k)$ を満たすことをいう。

**Example 1.1.** $\mathbb{Z}_5 = \langle\omega\,|\,\omega^5=1\rangle$ 上の一般アダマール行列 GH(5, 1)

$$\begin{bmatrix} 1 & \omega & \omega^4 & \omega^4 & \omega \\ \omega & 1 & \omega & \omega^4 & \omega^4 \\ \omega^4 & \omega & 1 & \omega & \omega^4 \\ \omega^4 & \omega^4 & \omega & 1 & \omega \\ \omega & \omega^4 & \omega^4 & \omega & 1 \end{bmatrix}$$

一般アダマール行列については、次の問題等が興味深い研究対象になっている。

- どのような $u$ と $\lambda$ をとれば一般アダマール行列 GH($u$, $\lambda$) を構成することができるのか？
- 知られている一般アダマール行列からさらに大きいサイズの一般アダマール行列を構成することは可能か？

前者の問題に関して、$2\leq u\lambda\leq 99$ に対する一般アダマール行列 GH($u$, $\lambda$) の存在・非存在が確定しているものについては [1] にまとめられている。現在、有限群の位数が素数べきの一般アダマール行列しか知られていないため、「一般アダマール行列が構成できるのは有限群の位数が素数べきの場合に限られるか？」という問題が最大の難問である。( [1] 参照 )

また、後者の問題については、有限群が GF($q$) の加法群のとき、次のことが知られている。

- $q$ が奇素数べきのとき、GH($q$, 1) を拡張して GH($q$, 2) の構成することが可能である。(Jungnickel [4] and Street [5])

- $q$が奇素数べき（ただし、$q \neq 3, 5$）のとき、GH($q$, 1), GH($q$, 2)を拡張してGH($q$, 4)の構成が可能である。(Dawson [2])

- $q$が$19 < q < 200$を満たす奇素数べき（ただし、$q \neq 27$）のとき、GH($q$, 8)が存在する。(de Launey and Dawson [3])

本稿では、GF($q$)の加法群に対するGH($q$, $q$)およびGH($q$, $q^2$)の構成について述べる。§2では、一般アダマール行列に関連した行列の定義を行い、それらについての性質を取り上げる。§3では、§2で扱った行列を利用して、GH($q$, $q$)およびGH($q$, $q^2$)を構成する。

## 2 Other definitions and their properties

$p$を素数とし、$q = p^n$とおく。

**Definition 2.1.** $F = \mathrm{GF}(q) = \{a_0 = 0, a_1, \cdots, a_{q-1}\}$とする。
(i) 写像$f : F \longrightarrow F$に対して、
$M(f) : F \times F \ni (a, b) \longmapsto f(b-a) \in F$と定義する。
このとき、$M(f)$は$F$の元で添え字付けされた$F$上$q$次正方行列と見ることができる。

・$\Omega_q = \{M(f) \mid f : F \longrightarrow F \text{ map}\}$とおく。

(ii) $M(f) \in \Omega_q$とする。
・$M(f)$は**Type I**である$\overset{\text{def}}{\Longleftrightarrow}$ $M(f)$はGH($q$, 1)である
$\Longleftrightarrow \forall a_1 \neq a_2 \in F$に対して、$\{f(b-a_1)-f(b-a_2) \mid b \in F\} = F$

・$M(f)$は**Type II**である$\overset{\text{def}}{\Longleftrightarrow}$ $\forall a \in F, \forall b_1, b_2 \in F$に対して、$f(b_1) - f(b_1 - a) = f(b_2) - f(b_2 - a)$

・$\Omega_{q,I} = \{M(f) \mid f : F \longrightarrow F \text{ map}, M(f) \text{ is type I}\}$

・$\Omega_{q,II} = \{M(f) \mid f : F \longrightarrow F \text{ map}, M(f) \text{ is type II}\}$

**Example 2.1.** $F = \mathrm{GF}(3) = \{0, 1, 2\}$とする。
(i) $f(x) = x - x^2$とする。
$M(f)(a, b) = f(b - a)$
$M(f)$の行と列はそれぞれ0, 1, 2の順で添え字付けする。

$$M(f) = \begin{bmatrix} f(0) & f(1) & f(2) \\ f(2) & f(0) & f(1) \\ f(1) & f(2) & f(0) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$ はType Iである。

(ii) $g(x) = 2 + x$とする。
$M(f)(a, b) = f(b - a)$
$M(f)$の行と列はそれぞれ0, 1, 2の順で添え字付けする。

$$M(f)=\begin{bmatrix} f(0) & f(1) & f(2) \\ f(2) & f(0) & f(1) \\ f(1) & f(2) & f(0) \end{bmatrix}=\begin{bmatrix} 2 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{bmatrix}$$ は Type II である。

**Lemma 2.1.** $F=\mathrm{GF}(q)$ とし、$M(f)\in\Omega_q$ とする。このとき、
$M(f)\in\Omega_{q,I} \Longleftrightarrow \forall a\in F^*,\ f:\ F\ni x\longmapsto f(x+a)-f(x)\in F$ は全単射、
すなわち $f$ は planar function である。

**Proof:** $M(f)\in\Omega_{q,I} \Longleftrightarrow M(f)$ は $\mathrm{GH}(q,1)$
$\Longleftrightarrow \forall a_1\neq a_2\in F$ に対して、$\{f(x-a_1)-f(x-a_2)\,|\,x\in F\}=F$
$\Longleftrightarrow \forall a\in F^*$ に対して、$\{f(x+a)-f(x)\,|\,x\in F\}=F$
$\Longleftrightarrow \forall a\in F^*,\ f:\ F\ni x\longmapsto f(x+a)-f(x)\in F$ は全単射 □

**Lemma 2.2.** $F=\mathrm{GF}(q)$, $q=p^n$, ただし、$p$ は奇素数とする。
$f:F\longrightarrow F$ map とする。
このとき、$\exists a_0,\ a_1,\ a_2,\ b_1,\ b_2,\cdots,b_{n-1}\in F\ s.t.\ f(x)=a_0+a_1x+a_2x^2+b_1x^p+b_2x^{p^2}+\cdots+b_{n-1}x^{p^{n-1}}$, $a_2\neq 0 \Longrightarrow f$ は planar function である。□

**Lemma 2.3.** $F=\mathrm{GF}(q)$, $q=p^n$, ただし、$p$ は素数とする。
$f:F\longrightarrow F$ map とする。
このとき、$\exists a,\ b_0,\ b_1,\ b_2,\cdots,b_{n-1}\in F\ s.t.\ f(x)=a+b_0x+b_1x^p+b_2x^{p^2}+\cdots+b_{n-1}x^{p^{n-1}}$
$\Longrightarrow M(f)\in\Omega_{q,II}$ □

# 3 Construction of $\mathrm{GH}(q,\ q)$'s and $\mathrm{GH}(q,\ q^2)$'s

Lemma 2.2 より、$f$ を 2 次式として $M(f)$ を作ると $\Omega_{q,I}$ に属し、$\mathrm{GH}(q,1)$ となる。また、Lemma 2.3 より、$f$ を高々1 次式として $M(f)$ を作ると $\Omega_{q,II}$ に属する。
この節では、これらを用いた一般アダマール行列を考える。

## 3.1 Construcion of $\mathrm{GH}(q,\ q)$'s by using Type I matrices

**Example 3.1.** $F=\mathrm{GF}(3)=\{0,1,2\}$ に対して、

$f_0(x)=x^2$, $f_1(x)=1+x^2$, $f_2(x)=2+x^2$ とおくと、$M(f_0)=\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$, $M(f_1)=\begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix}$, $M(f_2)=\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}$ となる。

このとき、$\begin{bmatrix} M(f_0) & M(f_0) & M(f_0) \\ M(f_0) & M(f_1) & M(f_2) \\ M(f_0) & M(f_2) & M(f_1) \end{bmatrix}=$

$$\left[\begin{array}{ccc|ccc|ccc} 0&1&1&0&1&1&0&1&1 \\ 1&0&1&1&0&1&1&0&1 \\ 1&1&0&1&1&0&1&1&0 \\ \hline 0&1&1&1&2&2&2&0&0 \\ 1&0&1&2&1&2&0&2&0 \\ 1&1&0&2&2&1&0&0&2 \\ \hline 0&1&1&2&0&0&1&2&2 \\ 1&0&1&0&2&0&2&1&2 \\ 1&1&0&0&0&2&2&2&1 \end{array}\right]$$

はGH(3, 3)となる。

この例をGF($q$)に拡張することを考える。

**Theorem 3.1.** $F = \mathrm{GF}(q) = \{a_0 = 0, a_1, \cdots, a_{q-1}\}$, $q = p^n$, $p$を奇素数とする。
$f_{a_0}(x) = x^2$, $f_{a_1}(x) = a_1 + x^2, \cdots, f_{a_{q-1}}(x) = a_{q-1} + x^2$とおき、$M(f_{a_0}), M(f_{a_1}), \cdots, M(f_{a_{q-1}})$を構成する。

このとき、$q^2$次の正方行列を

$$H = \begin{bmatrix} H_{0,0} & H_{0,1} & \cdots & H_{0,q-1} \\ H_{1,0} & H_{1,1} & \cdots & H_{1,q-1} \\ H_{2,0} & H_{2,1} & \cdots & H_{2,q-1} \\ \vdots & \vdots & & \vdots \\ H_{q-1,0} & H_{q-1,1} & \cdots & H_{q-1,q-1} \end{bmatrix}$$

とブロック分けし、

$$H = \begin{bmatrix} M(f_{a_0}) & M(f_{a_0}) & \cdots & M(f_{a_0}) \\ M(f_{a_0}) & M(f_{a_1 a_1}) & \cdots & M(f_{a_1 a_{q-1}}) \\ M(f_{a_0}) & M(f_{a_2 a_1}) & \cdots & M(f_{a_2 a_{q-1}}) \\ \vdots & \vdots & & \vdots \\ M(f_{a_0}) & M(f_{a_{q-1} a_1}) & \cdots & M(f_{a_{q-1} a_{q-1}}) \end{bmatrix}$$ として、$M(f_{a_i})$を各ブロックに配列させる。

すると、$H$はGH($q$, $q$)となる。

**Proof:** それぞれのブロックはGH($q$, 1)であるので、$H_{i,0}, H_{i,1}, \cdots, H_{i,q-1}$の中の任意の異なる2行の差をとると、$F$の元がそれぞれ$q$回現れる。

したがって、$i \neq j$に対して、$H_{i,0}, H_{i,1}, \cdots, H_{i,q-1}$の$k$行目と$H_{j,0}, H_{j,1}, \cdots, H_{j,q-1}$の$\ell$行目をとったときの差を考えればよい。

・$k = \ell$の場合
$H_{j,m}$と$H_{i,m}$の$k$行目の差について考えると、$a_m a_j - a_m a_i = a_m(a_j - a_i)$が$q$回現れる。
$m \in \{0, 1, \cdots, q-1\}$より、$H$の$k$行目の差として考えると、$F$の元がそれぞれ$q$回現れることになる。

・$k \neq \ell$の場合
$\ell - k = a$とおく。$H_{j,m}$の$k$行目と$H_{i,m}$の$\ell$行目の差については、
$\{f_{a_m a_j}(x + a) - f_{a_m a_i}(x) \mid x \in F\}$を考えると、
$f_{a_m a_j}(x + a) - f_{a_m a_i}(x) = a_m a_j + (x + a)^2 - a_m a_i - x^2 = 2ax + a^2 + a_m(a_j - a_i)$となることから、$\{f_{a_m a_j}(x + a) - f_{a_m a_i}(x) \mid x \in F\} = F$となる。
したがって、$F$の元がそれぞれ1回ずつ現れ、$H$においては、$F$の元がそれぞれ$q$回現れる。

以上より、$H$はGH($q$, $q$)である。□

## 3.2 Construcion of GH($q$, $q$)'s by using Type II matrices

**Example 3.2.** $F = \mathrm{GF}(3) = \{0, 1, 2\}$ に対して、

$f_0(x) = 0$, $f_1(x) = x$, $f_2(x) = 2x$ とおくと、$M(f_0) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $M(f_1) = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$,

$M(f_2) = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix}$ となる。

このとき、$\begin{bmatrix} M(f_0) & M(f_1) & M(f_2) \\ M(f_1) & M(f_2) & M(f_0) \\ M(f_2) & M(f_0) & M(f_1) \end{bmatrix} = \left[\begin{array}{ccc|ccc|ccc} 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 & 0 & 1 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 \\ \hline 0 & 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 & 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2 \\ 1 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 1 \\ 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \end{array}\right]$

は GH(3, 3) となる。

**Example 3.3.** $F = \mathrm{GF}(4) = \{0, 1, \alpha, \alpha+1\}$ $(\alpha^2 = \alpha + 1)$ に対して、

$f_0(x) = 0$, $f_1(x) = x$, $f_\alpha(x) = \alpha x$, $f_{\alpha+1}(x) = (\alpha+1)x$ とおくと、$M(f_0) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$,

$M(f_1) = \begin{bmatrix} 0 & 1 & \alpha & \alpha+1 \\ 1 & 0 & \alpha+1 & \alpha \\ \alpha & \alpha+1 & 0 & 1 \\ \alpha+1 & \alpha & 1 & 0 \end{bmatrix}$, $M(f_\alpha) = \begin{bmatrix} 0 & \alpha & \alpha+1 & 1 \\ \alpha & 0 & 1 & \alpha+1 \\ \alpha+1 & 1 & 0 & \alpha \\ 1 & \alpha+1 & \alpha & 0 \end{bmatrix}$, $M(f_{\alpha+1}) =$

$\begin{bmatrix} 0 & \alpha+1 & 1 & \alpha \\ \alpha+1 & 0 & \alpha & 1 \\ 1 & \alpha & 0 & \alpha+1 \\ \alpha & 1 & \alpha+1 & 0 \end{bmatrix}$ となる。

このとき、16 次正方行列 $\begin{bmatrix} M(f_0) & M(f_1) & M(f_\alpha) & M(f_{\alpha+1}) \\ M(f_1) & M(f_0) & M(f_{\alpha+1}) & M(f_\alpha) \\ M(f_\alpha) & M(f_{\alpha+1}) & M(f_0) & M(f_1) \\ M(f_{\alpha+1}) & M(f_\alpha) & M(f_1) & M(f_0) \end{bmatrix}$ は GH(4, 4) となる。

これらの例を GF($q$) に拡張することを考える。

**Theorem 3.2.** $F = \mathrm{GF}(q) = \{a_0 = 0, a_1, \cdots, a_{q-1}\}$, $q = p^n$, $p$ を素数とする。
$f_{a_0}(x) = a_0 x = 0$, $f_{a_1}(x) = a_1 x, \cdots, f_{a_{q-1}}(x) = a_{q-1}x$ とおき、$M(f_{a_0})$, $M(f_{a_1}), \cdots, M(f_{a_{q-1}})$ を構成する。

このとき、$q^2$ 次の正方行列を

$$H_q = \begin{bmatrix} H_{0,0} & H_{0,1} & \cdots & H_{0,q-1} \\ H_{1,0} & H_{1,1} & \cdots & H_{1,q-1} \\ H_{2,0} & H_{2,1} & \cdots & H_{2,q-1} \\ \vdots & \vdots & & \vdots \\ H_{q-1,0} & H_{q-1,1} & \cdots & H_{q-1,q-1} \end{bmatrix}$$

とブロック分けし、

$$H_q = \begin{bmatrix} M(f_{a_0}) & M(f_{a_1}) & \cdots & M(f_{a_{q-1}}) \\ M(f_{a_1}) & M(f_{a_1+a_1}) & \cdots & M(f_{a_1+a_{q-1}}) \\ M(f_{a_2}) & M(f_{a_2+a_1}) & \cdots & M(f_{a_2+a_{q-1}}) \\ \vdots & \vdots & & \vdots \\ M(f_{a_{q-1}}) & M(f_{a_{q-1}+a_1}) & \cdots & M(f_{a_{q-1}+a_{q-1}}) \end{bmatrix}$$ として、$M(f_{a_i})$ を各ブロックに配列させる。

すると、$H_q$ は GH$(q, q)$ となる。

**Proof:** $H_{i,0}, H_{i,1}, \cdots, H_{i,q-1}$ の任意の異なる2行の差をとると、Lemma 2.3 より、$H_{i,m}$ の中では、$F$ の1つの元が $q$ 回まとまって現れる。また、$H_q$ の行全体では、$f_{a_0}, f_{a_1}, \cdots, f_{a_{q-1}}$ をそれぞれ1回ずつとっているので、$F$ の元がそれぞれ $q$ 回ずつ現れる。

したがって、$i \neq j$ に対して、$H_{i,0}, H_{i,1}, \cdots, H_{i,q-1}$ の $k$ 行目と $H_{j,0}, H_{j,1}, \cdots, H_{j,q-1}$ の $\ell$ 行目をとったときの差を考えればよい。

$\ell - k = a$ とおく。$H_{j,m}$ の $k$ 行目と $H_{i,m}$ の $\ell$ 行目の差の集合 $\{f_{a_m+a_j}(x+a) - f_{a_m+a_i}(x) \mid x \in F\}$ を考えると、
$f_{a_m+a_j}(x+a) - f_{a_m+a_i}(x) = (a_m + a_j)(x+a) - (a_m + a_i)x = (a_j - a_i)x + (a_m + a_j)a$ となることから、$\{f_{a_m+a_j}(x+a) - f_{a_m+a_i}(x) \mid x \in F\} = F$ となる。
したがって、$F$ の元がそれぞれ1回ずつ現れ、$H_q$ においては、$F$ の元がそれぞれ $q$ 回ずつ現れる。

以上より、$H_q$ は GH$(q, q)$ である。□

## 3.3 Construcion of GH$(q, q^2)$'s by using Type II matrices

**Example 3.4.** Example 3.2 における GH(3, 3) を

$$H_3 = \left[\begin{array}{ccc|ccc|ccc} 0&0&0&0&1&2&0&2&1 \\ 0&0&0&2&0&1&1&0&2 \\ 0&0&0&1&2&0&2&1&0 \\ \hline 0&1&2&0&2&1&0&0&0 \\ 2&0&1&1&0&2&0&0&0 \\ 1&2&0&2&1&0&0&0&0 \\ \hline 0&2&1&0&0&0&0&1&2 \\ 1&0&2&0&0&0&2&0&1 \\ 2&1&0&0&0&0&1&2&0 \end{array}\right]$$

とおく。

また、$J=\begin{bmatrix}1 & 1 & \cdots & 1\\ 1 & 1 & \cdots & 1\\ \vdots & \vdots & & \vdots\\ 1 & 1 & \cdots & 1\end{bmatrix}$ （9次正方行列）とおく。

このとき、27次正方行列

$$\begin{bmatrix}H_3 & H_3 & H_3\\ H_3 & J+H_3 & 2J+H_3\\ H_3 & 2J+H_3 & J+H_3\end{bmatrix} =$$

$$\left[\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc|ccc|ccc}
0&0&0&0&1&2&0&2&1&0&0&0&0&1&2&0&2&1&0&0&0&0&1&2&0&2&1\\
0&0&0&2&0&1&1&0&2&0&0&0&2&0&1&1&0&2&0&0&0&2&0&1&1&0&2\\
0&0&0&1&2&0&2&1&0&0&0&0&1&2&0&2&1&0&0&0&0&1&2&0&2&1&0\\
\hline
0&1&2&0&2&1&0&0&0&0&1&2&0&2&1&0&0&0&0&1&2&0&2&1&0&0&0\\
2&0&1&1&0&2&0&0&0&2&0&1&1&0&2&0&0&0&2&0&1&1&0&2&0&0&0\\
1&2&0&2&1&0&0&0&0&1&2&0&2&1&0&0&0&0&1&2&0&2&1&0&0&0&0\\
\hline
0&2&1&0&0&0&0&1&2&0&2&1&0&0&0&0&1&2&0&2&1&0&0&0&0&1&2\\
1&0&2&0&0&0&2&0&1&1&0&2&0&0&0&2&0&1&1&0&2&0&0&0&2&0&1\\
2&1&0&0&0&0&1&2&0&2&1&0&0&0&0&1&2&0&2&1&0&0&0&0&1&2&0\\
\hline
0&0&0&0&1&2&0&2&1&1&1&1&1&2&0&1&0&2&2&2&2&2&0&1&2&1&0\\
0&0&0&2&0&1&1&0&2&1&1&1&0&1&2&2&1&0&2&2&2&1&2&0&0&2&1\\
0&0&0&1&2&0&2&1&0&1&1&1&2&0&1&0&2&1&2&2&2&0&1&2&1&0&2\\
\hline
0&1&2&0&2&1&0&0&0&1&2&0&1&0&2&1&1&1&2&0&1&2&1&0&2&2&2\\
2&0&1&1&0&2&0&0&0&0&1&2&2&1&0&1&1&1&1&2&0&0&2&1&2&2&2\\
1&2&0&2&1&0&0&0&0&2&0&1&0&2&1&1&1&1&0&1&2&1&0&2&2&2&2\\
\hline
0&2&1&0&0&0&0&1&2&1&0&2&1&1&1&1&2&0&2&1&0&2&2&2&2&0&1\\
1&0&2&0&0&0&2&0&1&2&1&0&1&1&1&0&1&2&0&2&1&2&2&2&1&2&0\\
2&1&0&0&0&0&1&2&0&0&2&1&1&1&1&2&0&1&1&0&2&2&2&2&0&1&2\\
\hline
0&0&0&0&1&2&0&2&1&2&2&2&2&0&1&2&1&0&1&1&1&1&2&0&1&0&2\\
0&0&0&2&0&1&1&0&2&2&2&2&1&2&0&0&2&1&1&1&1&0&1&2&2&1&0\\
0&0&0&1&2&0&2&1&0&2&2&2&0&1&2&1&0&2&1&1&1&2&0&1&0&2&1\\
\hline
0&1&2&0&2&1&0&0&0&2&0&1&2&1&0&2&2&2&1&2&0&1&0&2&1&1&1\\
2&0&1&1&0&2&0&0&0&1&2&0&0&2&1&2&2&2&0&1&2&2&1&0&1&1&1\\
1&2&0&2&1&0&0&0&0&0&1&2&1&0&2&2&2&2&2&0&1&0&2&1&1&1&1\\
\hline
0&2&1&0&0&0&0&1&2&2&1&0&2&2&2&2&0&1&1&0&2&1&1&1&1&2&0\\
1&0&2&0&0&0&2&0&1&0&2&1&2&2&2&1&2&0&2&1&0&1&1&1&0&1&2\\
2&1&0&0&0&0&1&2&0&1&0&2&2&2&2&0&1&2&0&2&1&1&1&1&2&0&1
\end{array}\right]$$

は GH(3, 9) となる。

この例を GF($q$) に拡張することを考える。

**Theorem 3.3.** $F=\mathrm{GF}(q)=\{a_0=0, a_1, \cdots, a_{q-1}\}$, $q=p^n$, $p$ を素数とする。
$f_{a_0}(x)=a_0x=0, f_{a_1}(x)=a_1x, \cdots, f_{a_{q-1}}(x)=a_{q-1}x$ とおき、$M(f_{a_0})$, $M(f_{a_1}), \cdots, M(f_{a_{q-1}})$ を求め、Theorem 3.2 の方法で GH($q$, $q$) となる $H_q$ を構成する。

また、$J=\begin{bmatrix}1 & 1 & \cdots & 1\\ 1 & 1 & \cdots & 1\\ \vdots & \vdots & & \vdots\\ 1 & 1 & \cdots & 1\end{bmatrix}$（$q^2$ 次正方行列）とおく。

このとき、$q^3$ 次の正方行列を

$$H=\begin{bmatrix}H_q & H_q & \cdots & H_q\\ H_q & a_1a_1J+H_q & \cdots & a_1a_{q-1}J+H_q\\ H_q & a_2a_1J+H_q & \cdots & a_2a_{q-1}J+H_q\\ \vdots & \vdots & & \vdots\\ H_q & a_{q-1}a_1J+H_q & \cdots & a_{q-1}a_{q-1}J+H_q\end{bmatrix}$$

として $q^2$ 次の正方行列を用いてブロック分けする。

すると、$H$ は GH$(q, q^2)$ となる。

**Proof:** $H_q$ は GH$(q, q)$ であるから、$H_q, a_ia_1J+H_q, \cdots, a_ia_{q-1}J+H_q$ の中の任意の異なる2行の差をとると、$F$ の元がそれぞれ $q^2$ 回現れる。

したがって、$i\neq j$ に対して、$H_q, a_ia_1J+H_q, \cdots, a_ia_{q-1}J+H_q$ の $k$ 行目と $H_q, a_ja_1J+H_q, \cdots, a_ja_{q-1}J+H_q$ の $\ell$ 行目をとったときの差を考えればよい。

・$k$ と $\ell$ が $H_q$ の同一ブロック内の2行で、しかも $k=\ell$ であったとき
$a_ia_mJ+H_q$ と $a_ja_mJ+H_q$ の $k$ 行目同士の差は、$a_ja_m-a_ia_m=a_m(a_j-a_i)$ が $q^2$ 回現れる。$m\in\{0, 1, \cdots, q-1\}$ であるから、$H$ においては、$F$ の元がそれぞれ $q^2$ 回現れることになる。

・$k$ と $\ell$ が $H_q$ の同一ブロック内の2行で、$k\neq\ell$ であったとき
$a_ia_mJ+H_q$ の $k$ 行目と $a_ja_mJ+H_q$ の $\ell$ 行目の差の集合を考える。$H_q$ の1つのブロックにおいては、$F$ の1つの元が $q$ 回まとまって現れる。また、$f_{a_0}, f_{a_1}, \cdots, f_{a_{q-1}}$ を $H_q$ のブロックの中で1回ずつとっているので、上述の集合は、$F$ の元がそれぞれ $q$ 回含まれたものになる。
$H$ の行には $q$ 個の $H_q$ のブロックがあるので、$H$ の $k$ 行目と $\ell$ 行目の差の集合は、$F$ の元がそれぞれ $q^2$ 回含まれたものになる。

・$k$ と $\ell$ が $H_q$ の別のブロックの2行であったとき
$a_ia_mJ+H_q$ の $k$ 行目と $a_ja_mJ+H_q$ の $\ell$ 行目の差の集合を考える。
$\ell-k=a$ とおき、$\{a_ja_m+f_{a_{m'}+a_j}(x+a)-a_ia_m-f_{a_{m'}+a_i}(x)\,|\,x\in F\}$ を考えると、
$a_ja_m+f_{a_{m'}+a_j}(x+a)-a_ia_m-f_{a_{m'}+a_i}(x)=a_ja_m+(a_{m'}+a_j)(x+a)-a_ia_m-(a_{m'}+a_i)x$
$=(a_j-a_i)x+(a_{m'}+a_j)a+a_m(a_j-a_i)$ であるから、$\{a_ja_m+f_{a_{m'}+a_j}(x+a)-a_ia_m-f_{a_{m'}+a_i}(x)\,|\,x\in F\}=F$ となり、$F$ の元がそれぞれ1回ずつ現れる。$H_q$ の行には $q$ 個のブロックがあるので（つまり、$m'\in\{0, 1, \cdots, q-1\}$ であるので）、$a_ia_mJ+H_q$ の $k$ 行目と $a_ja_mJ+H_q$ の $\ell$ 行目の差の集合は、$F$ の元がそれぞれ $q$ 回含まれたものになる。
$H$ の行には $q$ 個の $H_q$ のブロックがあるので（つまり、$m\in\{0, 1, \cdots, q-1\}$ であるので）、$H$ の $k$ 行目と $\ell$ 行目の差の集合は、$F$ の元がそれぞれ $q^2$ 回含まれたものになる。

以上より、$H$ は GH$(q, q^2)$ である。□

# References

[1] C. J. Colbourn and J. F. Dinitz, Handbook of Combinatorial Designs, Second Edition, Çhapman & Hall/CRC, 2007.

[2] J. Dawson, A construchion for the generalized Hadamard matrices GH($4q$, EA($q$)), *Journal of Statistical Planning and Inference*, **11** (1985), 103-110.

[3] W. de Launey and J. Dawson, A Note on the Construction of GH($4tq$, EA($q$)) for $t = 1, 2$, *Australasian Journal of Combinatorics*, **6** (1992), 177-186.

[4] D. Jungnickel, On difference matrices, resovable TDs and generalized Hadamard matrices, *Math. Z.*, **167** (1979), 49-60.

[5] D. J. Street, Generalized Hadamard matrices, orthogonal arrays and F-squares, *Ars Combinatoria*, **3** (1979), 131-141.