数理解析研究所講究録
第587巻 1986年 139-156

Jacobi 和と Hadamard 行列

東京女子大学・文理　山本幸一

1. Hadamard 行列の構成では，合成の方向は別として，低次のものとは独立に作られる系列があり，相対差集合 (relative difference set) か相補差集合 (supplementary difference set) を用いる．２つの型は，大まかに言って次のように対比させられる．

相対差集合	――――	相補差集合
巡回行列	――――	多重巡回行列
巡回群：有限体 F の乗法群 $F^{\times}$	――――	基本アーベル群：F^{+}
一般四元数型	――――	Goethals-Seidel 型
縁取りはない	――――	縁取りがある
相対的 Gauss 和	――――	Jacobi 和

最後の欄は構成に使われる整数論的な工具を表わす．

始めの立場については山本 [4, 5]，山田 [5, 6, 7, 8] を参照．

第２の立場は Whiteman, Szekeres, Wallis らに負う．[1, 2, 3]．

ただし彼等は Jacobi 和の代りに，円分数を用いる．本稿では第２の立場を概説する．

§1. 多重巡回行列

2. ここでは基本アーベル群における多重巡回行列を取り扱う。

$F=GF(q)$, $q=p^r$, $F_0=GF(p)$, p: 素数とする. F/F_0 の基底 ω_1, $\omega_2, \cdots, \omega_r$ について, F の元 α を

$$\alpha = a_1\omega_1 + a_2\omega_2 + \cdots + a_r\omega_r, \qquad a_i \in \mathbf{Z}$$

と書けば a_i は $(\mathrm{mod}\ p)$ で決まる. T_p は

$$T_p = \begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & \\ 1 & & & 0 \end{pmatrix}$$

なる基礎的な p 次巡回行列として,

$$T^\alpha = T_p^{a_1} \otimes T_p^{a_2} \otimes \cdots \otimes T_p^{a_r}$$

と置き, それを α に対応する基本的な多重巡回行列という.

$$T^{\alpha+\beta} = T^\alpha T^\beta$$

で, $\alpha \longrightarrow T^\alpha$ は F^+ から $SL(q, \mathbf{Z})$ の中への同型写像である.

3. F 上に定義された, 複素数値を取る函数 f について, <u>多重巡回行列</u> (multicirculant) $f(T)$ を

$$f(T) = \sum_{\alpha \in F} f(\alpha) T^\alpha$$

で定義する. このとき, 転置行列について

$$f(T)^* = f(T^{-1}) = \sum_{\alpha \in F} f(\alpha) T^{-\alpha} = \sum_{\alpha \in F} f(-\alpha) T^\alpha$$

が成立つ

F^+ 上の２つの函数 f, g についてその対合積(convolution)

$h=f*g$ を

$$h(\alpha)=\sum_{\beta\in F} f(\beta)\,g(\alpha-\beta)$$

で定義すれば，これは

$$h(T)=f(T)\,g(T)$$

と同値である．

基本的な多重巡回行列 T^α の固有値は

$$\lambda(\alpha)=\zeta_p^{u_1a_1+u_2a_2+\cdots+u_ra_r} \qquad (0\leqq u_i\leqq p-1)$$

で与えられる q 個の数である．ただし $\zeta_p=e^{2\pi i/p}$.

$\alpha\longrightarrow\lambda(\alpha)$ は F^+ の指標，あるいは F の加法指標である．

一般に $F^+\longrightarrow F_0^+$ の準同型（１次函数）は，ある β について

$$\alpha\longrightarrow S_F(\beta\alpha) \qquad (S_F：絶対スプール)$$

で与えられる．したがって

$$\lambda(\alpha)=\zeta_p^{S_F(\beta\alpha)}$$

で，凡ての T^α は同時的に対角行列

$$\mathrm{diag}\left\{\zeta_p^{S_F(\beta\alpha)}\right\}_{\beta\in F}=\mathrm{diag}\left\{\lambda(\alpha)\right\}_{\lambda\in\Lambda}$$

に変形される．Λ は加法指標の作る乗法群である．

また $h=f*g$ の対角化は

$$\mathrm{diag}\left\{f\left(\zeta_p^{S_F(\beta\alpha)}\right)g\left(\zeta_p^{S_F(\beta\alpha)}\right)\right\}_{\beta\in F}$$

となる．

§2. F の指標

4. F の乗法群 $F^\times$ の指標を単に F の指標という．それらは $q-1$ 個だけあって，乗法群（指標群）を作り

$$\chi^0(\alpha)=1 \qquad (\alpha\in F^\times)$$

なる単位指標 χ^0 を単位元に持つ．

これらの指標は $\chi(0)=0$ として，F 全体に拡張しておく．さらに函数 ε を

$$\begin{cases}\varepsilon(0)=1 \\ \varepsilon(\alpha)=0 \qquad (\alpha\neq 0)\end{cases}$$

によって定め，また F^+ 上の凡ての α について値 1 を取る函数を $\mathbf{1}$ と書く．このとき

$$f*\varepsilon=f,\quad \varepsilon*f=f,$$

$$\mathbf{1}=\chi^0+\varepsilon$$

が成立ち

$$\varepsilon(T)=I_q \qquad (\text{単位行列})。$$

$$\mathbf{1}(T)=J_q \qquad (\text{凡ての成分 1 の行列}).$$

5. F の指標 χ に対する多重巡回行列 $\chi(T)=\sum_{\alpha\in F}\chi(\alpha)T^\alpha$ を対角化して

$$\mathrm{diag}\left\{\sum_{\alpha\in F}\chi(\alpha)\zeta_p^{S_F(\beta\alpha)}\right\}_{\beta\in F}$$

を得るが，各成分は本質的に Gauss の和

$$\tau(\chi)=\sum_{\alpha\in F}\chi(\alpha)\zeta_p^{S_F(\alpha)}$$

で、上記対角行列は

$$\tau(\chi)\,\mathrm{diag}\{\bar{\chi}(\beta)\}_{\beta\in F}$$

と書ける。

6. F の2つの指標 χ_1, χ_2 の convolution については

(1) $$\chi_1 * \chi_2 = \pi(\chi_1, \chi_2)\,\chi_1\chi_2 \qquad (\chi_1\chi_2 \neq \chi^0 \text{ のとき})$$

ここに $\pi(\chi_1, \chi_2)$ は Jacobi の和

$$\pi(\chi_1, \chi_2) = \sum_{\alpha\in F} \chi_1(\alpha)\,\chi_2(1-\alpha)$$

である。

また $\chi_1\chi_2 = \chi^0$, すなわち $\chi_2 = \bar{\chi}_1$ のときは

(2) $$\chi * \bar{\chi} = \chi(-1)(q\varepsilon - \mathbf{1}) \qquad (\chi \neq \chi^0 \text{ のとき}),$$

(3) $$\chi^0 * \chi^0 = (q-2)\mathbf{1} + \varepsilon$$

となる。これらは容易に検証される。

§3. 円分数

7. $e \mid q-1$ のとき, $F^\times$ における e 乗元の全体を

$$C_0 = \{\xi^{e\nu};\ \nu = 0, 1, \cdots, \frac{q-1}{e} - 1\} \qquad (\xi : F^\times \text{ の生成元})$$

とし, その剰余類

$$C_m = \xi^m C_0 \qquad (m = 0, 1, \cdots, e-1)$$

とおく。C_m の特性函数 E_m は, $\alpha \in F$ で定義されて

$$\left.\begin{aligned} E_m(\alpha) &= 1 \qquad (\alpha \in C_m \text{ のとき}) \\ &= 0 \qquad (\alpha \notin C_m \text{ のとき}) \end{aligned}\right\}$$

χ を $\chi(\xi)=\rho_e$ ならしめる『原始 e 乗剰余指標』とする．ここに $\rho_e=e^{2\pi i/e}$ このとき

$$E_m=\sum_{l=0}^{e-1}\rho_e^{ml}\chi^l,$$

$$\chi^l=\frac{1}{e}\sum_{m=0}^{e-1}\rho_e^{-ml}E_m.$$

e 次の円分数 $(l, m)_e$，$0\leqslant l\leqslant e-1$，$0\leqslant m\leqslant e-1$ は

$$\alpha+\beta=1,\quad \alpha\in C_l,\quad \beta\in C_m$$

の解の個数を表わす．伝統的な記法では，上の代りに，$\alpha-\beta=1$，$\alpha\in C_l$, $\beta\in C_m$ の解の個数を $(l, m)_e$ で表わすのだが，本質的には差があるわけではない．

以上は一般論だが，e は偶数とするのが普通である．この仮定のもとでは，$k\equiv\frac{q-1}{2}\pmod{e}$ なる k について

$$-1\in C_k.$$

したがって，右辺の円分数は，$(l, m+k)_e$ となるに過ぎない．

8．特性函数の convolution に円分数が現われる．

$$E_l*E_m=\sum_{k=0}^{e-1}(l-k, m-k)_e E_k+\delta_{l-m,k}\frac{q-1}{e}\varepsilon.$$

円分数はまた Jacobi の和によって表すことができる．

$$(l, m)_e=\frac{1}{e^2}\sum_{i=0}^{e-1}\sum_{j=0}^{e-1}\rho_e^{-li-mj}\pi(\chi^i, \chi^j).$$

その意味で，円分数に関する定理は凡て Jacobi の和に関するものに言い換えられ，逆も成立つ．

その種の定理をここに述べることはしない．Lang の本 [9] を参照されたい．

§4. 円分的相補差集合

9. F^+ の部分集合 $D_1, D_2, \cdots, D_r$ について，$b \in F^\times$ を D_i の2元の差として表わす方法の数 $\lambda_i(b)$ が

$$\lambda_1(b)+\lambda_2(b)+\cdots+\lambda_r(b)=\lambda, \quad \text{一定}$$

となれば，それらは，相補差集合と呼ばれる．

D_i の特性函数を η_i とおけば，その条件は

$$\sum_{i=1}^{r}\eta_i(T)\eta_i(T)^*=nI+\lambda J,$$

$$n=\sum_{i=1}^{r}\#D_i-\lambda$$

である．

さらに各 D_i が e 乗剰余の coset の合併になっている時，それを円分的相補差集合という．ここでは

$$D_i=\bigcup_{\nu\in M_i}C_\nu, \quad f_i(x)=\sum_{\nu\in M_i}x^\nu$$

となる．M_i は $\Omega=\{0,1,\cdots,e-1\}$ の部分集合である．そして

$$\eta_i=\sum_{\nu\in M_i}E_\nu=\frac{1}{e}\sum_{\ell=0}^{e-1}\sum_{\nu\in M_i}\rho_e^{-\ell\nu}\chi^\ell=\frac{1}{e}\sum_{\ell=0}^{e-1}f_i(\rho_e^{-\ell})\chi^\ell$$

だから，上の条件は

$$\frac{1}{e^2}\sum_{k=0}^{e-1}\sum_{\ell=0}^{e-1}\chi(-1)^\ell\sum_{i=1}^{r}f_i(\rho_e^{-k})f_i(\rho_e^{-\ell})\chi^k*\chi^\ell=n\varepsilon+\lambda\mathbf{1}.$$

$\frac{q-1}{e}$ が奇数ならば $\chi(-1)=-1$ で，上式の左辺は k, l について歪対称なので，左辺の和は $k\equiv l \pmod 2$ なるところに制限しておくことができる．

応用上は，$q\equiv 1+e \pmod{2e}$ の外に，非常に特殊な条件

$$\#D_i=\frac{q-1}{2},\quad r=1,2,4,8$$

をみたすものが重要である．すなわち $e-1$ 次以下の多項式 $f_1(x),\cdots,f_r(x)$ は係数が 0 か 1 で，係数 1 の項は $\frac{e}{2}$ 個あるとして，r-$\left(q;\frac{q-1}{2};\frac{r(q-3)}{4}\right)$-相補差集合を考察する．條件は

$$\frac{1}{e^2}\sum_{\substack{k=0\\ k\equiv l \pmod 2}}^{e-1}\sum_{l=0}^{e-1}(-1)^l\sum_{i=1}^{r} f_i(\rho_e^{-k})f_i(\rho_e^{-l})\chi^k*\chi^l=\frac{r(q+1)}{4}\varepsilon+\frac{r(q-3)}{4}\mathbf{1} \tag{4}$$

となる．

ここで $\chi^k*\chi^l$ のところに **6** の (1), (2), (3) を代入すれば，結局 Jacobi 和に関する等式に帰着する．

10. $\underline{\underline{e=2}}$. 平方剰余の場合．$q\equiv 3 \pmod 4$，$r=1$，$f_1(x)=1$．ここでは

$$C_0$$

が 1-$\left(q;\frac{q-1}{2},\frac{q-3}{4}\right)$ 相補差集合になるのは (4) の左辺が

$$=\frac{1}{4}\sum_{\substack{k=0\\ k\equiv l \pmod 2}}^{1}\sum_{l=0}^{1}(-1)^l(\chi^k*\chi^l)=\frac{1}{4}(\chi^0*\chi^0-\psi*\psi)=\frac{1}{4}(q+1)\varepsilon+\frac{1}{4}(q-3)\mathbf{1}$$

となることから分る．($\psi=\chi_1$ は平方剰余指標)．これが Paley 1 型の Hadamard 行列を与える．

11. 同じく $\underline{\underline{e=2}}$. ここでは $\frac{q-1}{2}$ を偶数として，$r=2$，$f_1(x)=1$，

$f_2(x)=x$ とおくと，(4) の左辺で '$k\equiv l \pmod 2$' を除いたものは

$$=\frac{1}{4}\left(\chi^0*\chi^0+2\chi^0*\psi+\psi*\psi\right)+\frac{1}{4}\left(\chi^0*\chi^0-2\chi^0*\psi+\psi*\psi\right)$$
$$=\frac{1}{2}\left(\chi^0*\chi^0+\psi*\psi\right)=\frac{1}{4}(q+1)\varepsilon+\frac{1}{4}(q-3)\mathbf{1}$$

となって，$x(q;\frac{q-1}{2};\frac{q-3}{2})$ 相補差集合：$q\equiv 1 \pmod 4$ のときの

$$C_0\ ,\ C_1$$

を得る．これから Paley 2 型の Hadamard 行列ができる．

12. $\underline{e=4}$. 4 乗剰余の場合．

<u>定理 1.</u> $q\equiv 5 \pmod 8$ のとき，

$$C_0\cup C_2,\quad C_0\cup C_1$$

が 2-$(q;\frac{q-1}{2};\frac{q-3}{2})$ 相補差集合であるための必要十分な條件は

$$q=a^2+4$$

の形であることである．

【証明】 $q\equiv 5 \pmod 8$ のときの Jacobi の和の表は：

	χ^0	χ^1	χ^2	χ^3
χ^0	$q-2$	-1	-1	-1
χ^1	-1	π	$-\pi$	1
χ^2	-1	$-\pi$	-1	$-\bar{\pi}$
χ^3	-1	1	$-\bar{\pi}$	$\bar{\pi}$

$\pi=a+bi$,
$q=a^2+b^2;\ a\equiv -1 \pmod 4$.

$f_1(x)=1+x^2,\ f_2(x)=1+x$ で，(4) の左辺は

$$=\frac{1}{16}\sum_{\substack{k=0\\ k\equiv l\,(\mathrm{mod}\,2)}}^{3}\sum_{l=0}^{3}(-1)^l\left(\left(1+(-1)^k\right)\left(1+(-1)^l\right)+\left(1+i^{-k}\right)\left(1+i^{-l}\right)\right)\chi^k*\chi^l$$

$$=\frac{1}{16}\left(8\chi^0*\chi^0+8\pi(\chi,\chi^2)\psi+4\psi*\psi+2i\pi(\chi,\chi)\psi-2i\pi(\chi^3,\chi^3)\psi-4\chi*\bar{\chi}\right)$$

(1), (2), (3) を 使って

$$=\frac{1}{2}(q+1)\varepsilon+\frac{1}{2}(q-3)\mathbf{1}+\frac{1}{2}\left(1+\frac{k}{2}\right)\psi$$

これは $k=-2$ の時に限って $\frac{1}{2}(q+1)\varepsilon+\frac{1}{2}(q-3)\mathbf{1}$ に等しい.

そのような q の値は

5, 13, 29, 53, 125, 173, 229, 293, 1093, 1229, 1373, 2029, 2217, 3253, 4493, 5333, 7229, 7573, 9029, 9413, ...

で, 始めの 3 つは [**2**, p.305] に出ている. 以上のうち 125 以外は凡て素数である. 素数でなければ 5 の巾であるが, $5^{100} \fallingdotseq 10^{70}$ 以下ではそのようなものはない.

13. <u>e=8</u>. 8乗剰余の場合.

<u>定理 2</u>. $q\equiv 9 \pmod{16}$ で, 8乗剰余について

$$C_0\cup C_1\cup C_2\cup C_3, \quad C_6\cup C_7\cup C_0\cup C_1$$

が $2\text{-}\left(q;\frac{q-1}{2};\frac{q-3}{2}\right)$ 相補差集合をなすための必要十分な条件は $q=q_0^2$, $q_0\equiv 5 \pmod 8$, $q_0>0$ の形であることである.

これは Szekeres-Whiteman の定理([**2**, p.343]) であるが, 同書では十分性だけを証明する.

[証明] $f_1(x)=1+x+x^2+x^3$, $f_2(x)=x^6+x^7+1+x=x^{-2}f_1(x)$

だから

$$\frac{1}{64}\sum_{\substack{k=0\\k\equiv l\ (\mathrm{mod}\,2)}}^{7}\sum_{l=0}^{7}(-1)^l\left(f_1(\rho_8^{-k})f_1(\rho_8^{-l})+f_2(\rho_8^{-k})f_2(\rho_8^{-l})\right)\chi^k*\chi^l$$

を計算すればよい. $\alpha_k = f_1(\rho_8^{-k}) = (1+\rho_8^{-k})(1+i^{-k})$ は $k=2,4,6$ では $=0$.

また $\alpha_0 = 4$. ゆえに上式では $k=l=0$ から生ずる主要項

$$\frac{1}{64}\,2\cdot 4\cdot 4\,\chi^0 * \chi^0 = \frac{1}{2}\left(\varepsilon + (q-2)\mathbf{1}\right)$$

以外は $k \equiv l \equiv 1 \pmod 2$ なる所を考えればよい. その部分和は

$$-\frac{1}{64}\sum_{\substack{k=0\\k\equiv 1}}^{7}\sum_{\substack{l=0\\l\equiv 1}}^{7}\left(1+(-1)^{\frac{k+l}{2}}\right)\alpha_k\alpha_l\left(\chi^k * \chi^l\right)$$

$$= -\frac{1}{64}\sum_{s\equiv 0 \,(\mathrm{mod}\,2)}\left(1+(-1)^{\frac{s}{2}}\right)\sum_{k\equiv 1}\alpha_k\alpha_{s-k}\left(\chi^k * \chi^{s-k}\right)$$

で, $s=2$, $s=6$ のところは消えて, $s=0$ と $s=4$ が残る.

$s=0$ のところは, (2) によって

$$-\frac{1}{32}\sum_{k\equiv 1}\alpha_k\alpha_{-k}\,\chi^k * \chi^{-k} = -\frac{1}{32}\chi_1(-1)\Big(\sum_{k\equiv 1}\alpha_k\alpha_{-k}\Big)(q\varepsilon - \mathbf{1}) = \frac{1}{2}(q\varepsilon - \mathbf{1}).$$

ここで $\sum_{k\equiv 1}\alpha_k\alpha_{-k} = 16$ を使っている (**14.** に述べる).

$s=4$ のところは, Jacobi の和の具体形を必要とする. $q \equiv 9\ (16)$ の時,

	χ^0	χ^1	χ^2	χ^3	χ^4	χ^5	χ^6	χ^7
χ^0	$q-2$	-1	-1	-1	-1	-1	-1	-1
χ^1	-1	$\varkappa$	$-\pi$	$-\varkappa$	$\varkappa$	π	$-\varkappa$	1
χ^2	-1	$-\pi$	π	$-\varkappa$	π	$-\pi$	-1	$-\bar{\varkappa}$
χ^3	-1	$-\varkappa$	$-\varkappa$	$\varkappa$	$\varkappa$	1	$-\bar{\pi}$	$\bar{\pi}$
χ^4	-1	$\varkappa$	π	$\varkappa$	-1	$\bar{\varkappa}$	$\bar{\pi}$	$\bar{\varkappa}$
χ^5	-1	π	$-\pi$	1	$\bar{\varkappa}$	$\bar{\varkappa}$	$-\bar{\varkappa}$	$-\bar{\varkappa}$
χ^6	-1	$-\varkappa$	-1	$-\bar{\pi}$	$\bar{\pi}$	$-\bar{\varkappa}$	$\bar{\pi}$	$-\bar{\pi}$
χ^7	-1	1	$-\bar{\varkappa}$	$\bar{\pi}$	$\bar{\varkappa}$	$-\bar{\varkappa}$	$-\bar{\pi}$	$\bar{\varkappa}$

$\pi = a + bi$, $a \equiv -1\ (4)$
$q = a^2 + b^2$,

$\varkappa = c + 2\sqrt{-2}\,d$, $c \equiv -1\ (4)$
$q = c^2 + 8d^2$.

$$-\frac{1}{32}\sum_{k=1} \alpha_k \alpha_{4-k}\pi(\chi^k, \chi^{4-k})\psi = -\frac{1}{32}\left(2\alpha\alpha_3\pi(\chi,\chi^3)+2\alpha_5\alpha_7\pi(\chi^5,\chi^7)\right)\psi$$

$$= -\frac{1}{32}\left(-4\sqrt{2}i(-x)+4\sqrt{2}i(-\bar{x})\right)\psi = -\frac{\sqrt{2}}{8}i(x-\bar{x})\psi = d\psi.$$

ゆえに $2\text{-}\left(q; \frac{q-1}{2}; \frac{q-3}{2}\right)$ 相補差集合であるための条件は $d=0$。

$q=c^2=q_0^2$。q_0 は p の巾であるが，$p\equiv 3 \pmod 8$ ならば，p がすでに $p=u^2+2v^2$ の形だから，Jacobi 和の Stickelberger 分解から x が平方数になることはない。故に $p\equiv 5 \pmod 8$, $q_0\equiv 5 \pmod 8$ となる。

14. $e=2^s$, $s>2$ の場合の Whiteman-Wallis の相補差集合の拡張。

$q\equiv 1+2^s \pmod{2^{s+1}}$ とし，$N=2^s$ について F の N 乗剰余を扱う。

定理 3. 上の仮定の F で，$i_1, i_2, \cdots, i_{\frac{N}{2}}$ は $\mathrm{mod}\ \frac{N}{2}$ で凡て非合同とすれば，

$$D_0 = C_{i_1}\cup C_{i_2}\cup\cdots\cup C_{i_{\frac{N}{2}}},\quad D_1 = C_{i_1-1}\cup C_{i_2-1}\cup\cdots\cup C_{i_{\frac{N}{2}}-1},\quad \cdots,$$

$$D_{\frac{N}{2}-1} = C_{i_1-(\frac{N}{2}-1)}\cup C_{i_2-(\frac{N}{2}-1)}\cup\cdots\cup C_{i_{\frac{N}{2}}-(\frac{N}{2}-1)}$$

は，$\frac{N}{2}\text{-}\left(q; \frac{q-1}{2}; \frac{N}{8}(q-3)\right)$ 相補差集合である。

[証明] ここでは Jacobi 和の具体形を必要としない。

$$f_0(x)=\sum_{\nu=1}^{N/2} x^{i_\nu},\quad f_1(x)=x^{-1}f_0(x),\ \cdots,\ f_{\frac{N}{2}-1}(x)=x^{-(\frac{N}{2}-1)}f_0(x)$$

だから

$$\frac{1}{N^2}\sum_{\substack{k=0\\ k\equiv l \pmod 2}}^{N-1}\sum_{l=0}^{N-1}(-1)^l\sum_{\nu=0}^{\frac{N}{2}-1}\rho_N^{(k+l)\nu} f_0(\rho_N^{-k})f_0(\rho_N^{-l})\chi^k*\chi^l$$

の計算になる。

$k\equiv l \pmod 2$ より $k+l$ は偶数で
$$\left.\begin{aligned}\sum_{\nu=0}^{\frac{N}{2}-1}\rho_N^{(k+l)\nu} &= \frac{N}{2} && (k+l\equiv 0 \pmod N)\\ &= 0 && (k+l\not\equiv 0 \pmod N)\end{aligned}\right\}$$

だから上式は

$$=\frac{1}{2N}\sum_{k=0}^{N-1}(-1)^k f_0(\rho_N^k)f_0(\rho_N^{-k})(\chi^k * \chi^{-k}).$$

その主要項 ($k=0$) は

$$\frac{1}{2N}\left(\frac{N}{2}\right)^2 \chi^0 * \chi^0 = \frac{N}{8}(\varepsilon + (q-1)\mathbf{1}).$$

その他の項 ($k\neq 0$) では $\chi^k * \chi^k = \chi^k(-1)(q\varepsilon - \mathbf{1}) = (-1)^k(q\varepsilon-\mathbf{1})$ から，

その部分の部分和は

$$\frac{1}{2N}\sum_{k=1}^{N-1} f_0(\rho_N^k)f_0(\rho_N^{-k})\cdot(q\varepsilon - \mathbf{1}).$$

しかし

(5) $$\sum_{k=1}^{N-1} f_0(\rho_N^k)f_0(\rho_N^{-k}) = \frac{N^2}{4}$$

だから，証明すべき等式が出る．(5)については

$$\sum_{k=0}^{N-1} f_0(\rho_N^k)f_0(\rho_N^{-k}) = \left(\frac{N}{2}\right)^2 + \sum_{k=1}^{N-1} f_0(\rho_N^k)f_0(\rho_N^{-k}),$$

$$\sum_{k=0}^{N-1} f_0(\rho_N^k)f_0(\rho_N^{-k}) = \sum_{k=0}^{N-1}\sum_{\mu=0}^{N/2-1}\sum_{\nu=0}^{N/2-1}\rho_N^{k\mu-k\nu} = \sum_{\mu=0}^{N/2-1}\sum_{\nu=0}^{N/2-1}\sum_{k=0}^{N-1}\rho_N^{k(\mu-\nu)}$$

$$= N\sum_{\mu=0}^{\frac{N}{2}-1}\sum_{\nu=0}^{N/2-1}\delta_{\mu,\nu} = \frac{N^2}{2}$$

のように検証される．

定理2中の証明未済の部分は，$N=8$ とおいて得られる．

Wallis-Whiteman では $i_1=0, i_2=1, \dots, i_{\frac{N}{2}}=\frac{N}{2}-1$ を取扱かうが，その証明は明徹とは言えない．

15. 最後に $\underline{e=6}$，6乗剰余の Jacobi 和を取上げる．

$q\equiv 7 \pmod{12}$ と仮定し，$\omega=\frac{-1+\sqrt{-3}}{2}$，$\rho_6=-\omega^2$ とおく．Jacobi の和の表は次のようになる．

	χ^0	χ^1	χ^2	χ^3	χ^4	χ^5
χ^0	$q-2$	-1	-1	-1	-1	-1
χ^1	-1	$-\eta\pi$	$\bar{\eta}\pi$	$-\bar{\eta}\pi$	$\eta\pi$	1
χ^2	-1	$\bar{\eta}\pi$	π	$\bar{\eta}\pi$	-1	$\bar{\eta}\bar{\pi}$
χ^3	-1	$-\bar{\eta}\pi$	$\bar{\eta}\pi$	1	$\eta\bar{\pi}$	$-\eta\bar{\pi}$
χ^4	-1	$\eta\pi$	-1	$\eta\bar{\pi}$	$\bar{\pi}$	$\eta\bar{\pi}$
χ^5	-1	1	$\bar{\eta}\bar{\pi}$	$-\eta\bar{\pi}$	$\eta\bar{\pi}$	$-\bar{\eta}\bar{\pi}$

$\pi=\dfrac{a+3b\sqrt{-3}}{2}$,

$a\equiv 1 \pmod 3$.

$4q=a^2+27b^2$

$\eta=\chi^2(2)=\chi_3(2)$ は 2 の立方剰余指標.

$\eta=1 \Longleftrightarrow$ 2 が立方剰余

$\Longleftrightarrow a\equiv b\equiv 0 \pmod 2$

ここでは $r=1$, すなわち

$$C_{i_1}\cup C_{i_2}\cup C_{i_3} \qquad 0\leqq i_1<i_2<i_3\leqq 5$$

が普通の差集合になる条件をしらべる.

$$f(x)=x^{i_1}+x^{i_2}+x^{i_3}$$

として (4) は

$$\frac{1}{36}\sum_{\substack{k=0\\ k\equiv l\ (\mathrm{mod}\,2)}}^{5}\sum_{l=0}^{5}(-1)^l f(\rho_6^{-k})f(\rho_6^{-l})\,\chi^k*\chi^l=\frac{1}{4}\left((q+1)\varepsilon+(q-3)\mathbb{1}\right)$$

となる. 左辺で $k=l=0$ なる主要項は (3) から

$$f(1)^2\left(\varepsilon+(q-2)\mathbb{1}\right)=9\left(\varepsilon+(q-2)\mathbb{1}\right).$$

他の $k+l\equiv 0 \pmod 6$ なる部分は (2) から

$$\sum_{k=1}^{5}f(\rho_6^{k})f(\rho_6^{-k})\left(q\varepsilon-\mathbb{1}\right)=9\left(q\varepsilon-\mathbb{1}\right).$$

ここで $\sum_{k=1}^{5}f(\rho_6^{k})f(\rho_6^{-k})=9$ であることは, (5) と同様にして検証されるからである.

ゆえに, 条件は

$$\sum_{\substack{s=2\\ s\equiv 0\ (\mathrm{mod}\ 2)}}^{4} \sum_{k=0}^{5} (-1)^k f(\rho_6^{-k})\, f(\rho_6^{-s+k})\, \pi(\chi_1^k, \chi_1^{s-k})\, \chi^s = 0,$$

すなわち

$$\sum_{k=0}^{5}(-1)^k f(\rho_6^{-k})\, f(\rho_6^{-2+k})\, \pi(\chi_1^k,\chi_1^{2-k})=0$$

となる. 前の表からそれは具体的に:

(6) $$-2f(1)f(\rho_6^{-2})+\eta\pi f(\rho_6^{-1})^2+2\eta\bar{\pi} f(\rho_6^{-3})f(\rho_6^{-5})+\bar{\pi} f(\rho_6^{-4})^2=0.$$

一方, 差集合を与える i_1, i_2, i_3 は, 同型なもの除いて, 次の3つに帰着する.

$\boxed{\#1}$: 0, 1, 2. $f(x)=1+x+x^2$.

$\boxed{\#2}$: 0, 1, 3. $f(x)=1+x+x^3$.

$\boxed{\#3}$: 0, 2, 4. $f(x)=1+x^2+x^4$.

まず $\boxed{\#1}$ では (6) は

$$4\omega^2\eta\pi-4\omega^2\eta\bar{\pi}=0,\quad \pi=\bar{\pi},\quad q=a^2$$

となるが, $q\equiv 7 \pmod{12}$ からそれは不可能.

次に $\boxed{\#2}$ では (6) は

$$6\sqrt{-3}\,\omega^2+\eta\pi\omega^2+2\eta\bar{\pi}\omega^2-3\bar{\pi}\omega^2=0,$$

$$(3-2\eta)\bar{\pi}-\eta\pi=6\sqrt{-3}.$$

$\eta=1$, すなわち2が立方剰余ならば

$$\pi-\bar{\pi}=-6\sqrt{-3},\quad \therefore\ b=-2,\quad q=a^2+27.$$

$\eta\neq 1$ ならば, $\eta=\omega$ とおいて

$$9(a-b)+(3a-21b)\sqrt{-3}=24\sqrt{-3},\quad a=b=-1$$

$a \equiv 1 \pmod 3$ に矛盾する.

$\boxed{\#3}$ では (6) は自明な式 $0=0$ となる. これはしかし平方剰余の全体で, Paley 1 型の差集合である.

定理 4. $q \equiv 7 \pmod{12}$ で, 6 乗剰余の coset 3 個の合併から成る差集合は, Paley 1 型のものか, 又は $q=a^2+27$ の形の場合の $E_0 \cup E_1 \cup E_3$ と同値である.

これは M. Hall の定理で, 第 2 の差集合は Hall の差集合と呼ばれる. q の値は

31, 43, 127, 223, 283, 811, 1051, 1471, 1627, 2143, 2731, 3163,

3391, 4651, 5503, 6427, 8863, 9631, …

で, 素数巾 (≠素数) が現われるかどうかは, 筆者には知られていない.

§ 5. 縁取り

16. **9.** で述べた r-$\left(q; \frac{q-1}{2}; \frac{r(q-3)}{4}\right)$-円分的相補差集合 $D_1, \cdots, D_r$ の特性函数 $\eta_1, \cdots, \eta_r$ について

$$\sum_{i=1}^{r} \eta_i(T)\eta_i(T)^* = r\left(\frac{q+1}{4} I + \frac{q-3}{4} J\right)$$

だから $\eta_i(T)$ で成分 0 を -1 で置き換えた行列 A_i は

$$\sum_{i=1}^{r} A_i A_i^* = r\left((q+1)I - J\right)$$

をみたす.

$r=1$ ならば

$$H=\begin{pmatrix} -1 & \mathbf{e}^* \\ \mathbf{e} & A_1 \end{pmatrix}, \quad \mathbf{e}=\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

$r=2$ ならば

$$H=\begin{pmatrix} 1 & 1 & \mathbf{e}^* & -\mathbf{e}^* \\ 1 & -1 & \mathbf{e}^* & \mathbf{e}^* \\ \mathbf{e} & -\mathbf{e} & A_1 & A_2 \\ \mathbf{e} & \mathbf{e} & -A_2^* & A_1^* \end{pmatrix}.$$

$r=4$ ならば

$$H=\begin{pmatrix} L^*\otimes 1 & -L\otimes \mathbf{e}^* \\ L^*\otimes \mathbf{e} & M \end{pmatrix}, \quad M=\begin{pmatrix} A_1 & A_2R & A_3R & A_4R \\ -A_2R & A_1 & -A_4^*R & A_3^*R \\ -A_3R & A_4^*R & A_1 & -A_2^*R \\ -A_4R & -A_3^*R & A_2^*R & A_1 \end{pmatrix}$$

がそれぞれ $r(q+1)$ 次の Hadamard 行列になる. R はいわゆる backcirculant 行列: $x_\alpha \longrightarrow x_{-\alpha}$ $(\alpha\in F^+)$ である.

$r=8$ の場合にも 8 次 Hadamard array [2, p.364] を用いて同様のことができるが, ここでは他の付帯条件が必要になる.

17. 付言. 定理4に対応する $e=14$ の場合はまだ決定されていない. その理由は14次のJacobi和の『標準型』というべき有力な形が, 決め難いところにある.

文献

[1] E. Spence ; Hadamard matrices from relative difference sets, J. Comb. Theory, A, vol. 19 (1975), 287-300.

[2] W. D. Wallis, A. P. Street, J. S. Wallis ; Combinatorics : Room Squares, Sum-Free Sets, Hadamard Matrices, Lecture Notes in Math., vol. 292 (1970), Springer-Verlag.

[3] A. L. Whiteman ; Hadamard matrices of order 4(2p+1), J. Number Theory, vol. 8 (1976), 1-11.

[4] K. Yamamoto ; On a generalized Williamson equation, Colloquia Mathematica Societatis János Bolyai, vol. 37 (1985), 839-850.

[5] K. Yamamoto, M. Yamada ; Williamson Hadamard matrices and Gauss sums, J. Math. Soc. Japan, vol. 37 (1985), 703-717.

[6] M. Yamada ; Hadamard matrices of generalized quaternion type, to appear in Discrete Math.

[7] M. Yamada ; On a relation of a cyclic relative difference set associated with the quadratic extension of a finite field and the Szekeres difference set, to appear in Combinatorica.

[8] M. Yamada ; Hadamard matrices generated by an adaptation of generalized quaternion type array, to appear in Graphs and Combinatorics.

[9] S. Lang ; Cyclotomic Fields, 1978, Springer-Verlag.