J. Math. Soc. Japan
Vol. 37, No. 4, 1985

Williamson Hadamard matrices and Gauss sums

By Koichi YAMAMOTO and Mieko YAMADA

(Received Jan. 17, 1984)
(Revised July 25, 1984)

§1. Williamson Hadamard matrices.

1. Let $\mathfrak{A}$ be a rational division algebra with an antiautomorphism $\tau:\xi\rightarrow\bar{\xi}$ of period two, such that the norm $\xi\bar{\xi}$ is a positive definite quadratic form in the coefficients of ξ with respect to a basis of $\mathfrak{A}$ over $\boldsymbol{Q}$. Let $\mathfrak{O}$ be a maximal order in $\mathfrak{A}$ invariant under τ. An element ε of $\mathfrak{O}$ is called a unit if its norm $\varepsilon\bar{\varepsilon}$ equals 1. The set U of all units is finite, and is a subgroup of the multiplicative group $\mathfrak{A}^*$ of $\mathfrak{A}$.

A square matrix H of order n with entries in U is called an *Hadamard matrix* in $\mathfrak{A}$ if

$$HH^*=nI\,,\qquad H^*={}^t\bar{H}\,,$$

for the unit matrix I.

If $\mathfrak{A}=\boldsymbol{Q}$ the rational number field then $U=\{1,\,-1\}$ and H is a usual Hadamard matrix. If $\mathfrak{A}=\boldsymbol{Q}(i)$ the Gaussian imaginary quadratic field, then $U=\{\pm 1,\,\pm i\}$ and H is called a *complex Hadamard matrix.* The character table of an abelian group G of order n provides an Hadamard matrix in the cyclotomic field $\boldsymbol{Q}(\zeta_m)$, $\zeta_m=e^{2\pi i/m}$, for the exponent m of G.

In the present paper we deal with rational quaternion field, although some part of the theory is carried over to a generalized quaternion field where the center is the maximal real subfield of a cyclotomic field of order 2^s. Thus let $\mathfrak{A}=\boldsymbol{Q}+\boldsymbol{Q}i+\boldsymbol{Q}j+\boldsymbol{Q}k$ with the quaternion units 1, i, j, k such that

$$i^2=j^2=k^2=-1\,,$$
$$ij=-ji=k\,,\quad jk=-kj=i\,,\quad ki=-ik=j\,.$$

We take the Hurwitz quaternion ring as $\mathfrak{O}$. The ring $\mathfrak{O}$ consists of quaternions $\xi=a+bi+cj+dk$ with

$$a,\,b,\,c,\,d\in\frac{1}{2}\boldsymbol{Z}\,,\qquad a\equiv b\equiv c\equiv d\pmod 1\,.$$

The antiautomorphism τ assigns the quaternion conjugate $\bar{\xi}=a-bi-cj-dk$ to ξ, and $\xi\bar{\xi}=a^2+b^2+c^2+d^2$. The unit group U consists of 24 elements and contains the quaternion group $U_0=\{\pm 1,\,\pm i,\,\pm j,\,\pm k\}$ as a normal subgroup. It also contains

$$w=(1+i+j+k)/2, \qquad w^2=(-1+i+j+k)/2,$$

and U is a semidirect product of U_0 by $\{w^2\}$, $(w^2)^3=1$. The 16 units in $U-U_0$ are precisely the units $(\pm 1\pm i\pm j\pm k)/2$, and the number of minus signs is even or odd according as ε is in wU_0 or in w^2U_0, or according as $\varepsilon\equiv w \pmod{\mathfrak{L}}$ or $\varepsilon\equiv w^2 \pmod{\mathfrak{L}}$ for the different $\mathfrak{L}=(1-i)$ of the maximal order $\mathfrak{O}$.

2. A square matrix M of order n is called a *circulant* matrix if its rows are obtained from the first row by applying cyclic shifts successively. Namely if $(a_0, a_1, \cdots, a_{n-1})$ is the first row then

$$M=a_0I+a_1T+\cdots+a_{n-1}T^{n-1}=f(T)$$

for the basic circulant matrix

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

and $f(x)\in\mathfrak{O}[x]$. If a usual Hadamard matrix is circulant then its order is necessarily a square, and except for $n=1$ and $n=4$ no such matrix is known. Ryser conjectures that there is no other. If a complex Hadamard matrix is circulant then its order is a sum of two squares, and if a quaternion Hadamard matrix is circulant its order is a sum of four squares. Since any positive integer is a sum of four squares it is plausible that there exists a circulant quaternion Hadamard matrix of any order n.

We treat a special class of circulant quaternion Hadamard matrices H where the entries are in $U-U_0$, i.e. of the form $(\pm 1\pm i\pm j\pm k)/2$. The matrix $2H$ gives rise to a usual Hadamard matrix of order $4n$ by replacing the quaternion units 1, i, j, k by their regular representation matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

The resulting matrix is

$$\begin{pmatrix} X & Y & Z & W \\ -Y & X & -W & Z \\ -Z & W & X & -Y \\ -W & -Z & Y & X \end{pmatrix},$$

for circulant matrices X, Y, Z, W in $\{1, -1\}$ of order n, satisfying

$$XX^*+YY^*+ZZ^*+WW^*=4nI\,.$$

Assume that H is symmetric then so are the matrices X, Y, Z, W. When we write $X=f_1(T)$, $Y=f_2(T)$, $Z=f_3(T)$, $W=f_4(T)$ for polynomials $f_i(x)$ of degree $n-1$, then these polynomials having coefficients ±1, are symmetric in the sense that $f_i(x)=f_i(x^{-1})$, and satisfy the equation

$$(1) \qquad f_1(x)^2+f_2(x)^2+f_3(x)^2+f_4(x)^2=4n\,,$$

for a variable x bound by the condition $x^n=1$. The above equation (1) is called a *Williamson equation* of order n.

3. In view of a construction problem the case n odd is particularly important. In this paper we treat Hadamard matrices of order $4n$, corresponding to symmetric circulant quaternion Hadamard matrices of odd order n. In this case, as is well known (cf. e.g. [9]), the Williamson equation (1) can be put into a simpler form equivalent to it:

$$(2) \quad (1+2\sum_{m\in A} e_m u_m)^2+(1+2\sum_{m\in B} e_m u_m)^2+(1+2\sum_{m\in C} e_m u_m)^2+(1+2\sum_{m\in D} e_m u_m)^2=4n\,,$$

where the e_m are 1 or -1 and

$$u_m=x^m+x^{-m} \qquad (m=1,\,2,\,\cdots,\,(n-1)/2)\,,$$

and where A, B, C, D is a partition of the half-system

$$\mathscr{H}=\{1,\,2,\,\cdots,\,(n-1)/2\}$$

of $\boldsymbol{Z}(n)-\{0\}$, $\boldsymbol{Z}(n)=\boldsymbol{Z}/n\boldsymbol{Z}$.

This is proved as follows. Assume $H=w^2P+wQ$ where P and Q have entries in $U_0\cup\{0\}$. If we replace nonzero entries by 1, we obtain (0, 1)-matrices P_0, Q_0 such that $P_0+Q_0=J$, where J has all its entries equal to 1. By noticing that $\mathfrak{L}$ is a two-sided ideal of $\mathfrak{O}$ and divides 2, we see that

$$\begin{aligned} &H\equiv w^2P_0+wQ_0\equiv w^2P_0+w(P_0+J)\equiv P_0+wJ \qquad (\mathrm{mod}\,\mathfrak{L})\,,\\ &HH^*\equiv(P_0+wJ)(P_0^*+w^2J)\\ &\quad\equiv P_0P_0^*+J^2+wJP_0^*+w^2P_0J\equiv P_0P_0^*+nJ+aJ \qquad (\mathrm{mod}\,\mathfrak{L})\,, \end{aligned}$$

for the number a of nonzero elements in the first row of P. We can assume a to be odd since otherwise we use $\bar{H}$ in place of H. Thus $I\equiv nI\equiv P_0P_0^*$ (mod 2). If moreover H is symmetric then $P_0^2\equiv I$, and this means that $P_0\equiv I$ (mod 2). In fact, if $P_0=\sum_{m\in S} T^m$ for a subset S of $\boldsymbol{Z}(n)$, then $P_0^2\equiv\sum_{m\in S} T^{2m}\equiv\sum_{m\in 2S} T^m$ (mod 2), so that $2S=\{0\}$, or $S=\{0\}$ since n is odd. Hence $P=\varepsilon I$ for some ε in U_0, and $-w\bar{\varepsilon}wH=wI-\eta Q$, $\eta=w\bar{\varepsilon}w^2=-w\bar{\varepsilon}w^{-1}\in U_0$. We can write $-2w\bar{\varepsilon}wH$ as

$$I+2\sum_{m\in A} e_m(T^m+T^{-m})+(I+2\sum_{m\in B} e_m(T^m+T^{-m}))i$$
$$+(I+2\sum_{m\in C} e_m(T^m+T^{-m}))j+(I+2\sum_{m\in D} e_m(T^m+T^{-m}))k\,,$$

with $e_m=\pm 1$ and A, B, C, D is a partition of H. This leads to (2) immediately.

The equation (2) is called a *reduced Williamson equation* of order n. The reduced Williamson equations were worked out for $n\leqq 27$ by Williamson, Baumert, Sawade and others. See also Agayan-Sarukhanyan [**1**].

A first infinite family of Williamson matrices was found by Turyn [**8**]. He transformed Paley type 2 matrix of order $2(q+1)$, q a prime-power$\equiv 1 \pmod 4$, into the Williamson matrix form. Whiteman [**10**] obtained the Williamson equation of the form (1) directly without resorting to Paley matrices, by using a quadratic extension of a finite field. In this paper we treat the reduced Williamson equations, directly and in detail. It will be shown that an essential point is in the norm relation of Gauss sums in a finite field. It also enables us to write down e_m and the subsets A, B, C, D in an explicit form, relying on a maximal-length linear-feedback shift-register sequence in a finite field. It turns out that two of the subsets are empty. The norm relation of the relative Gauss sums for a more general extensions will lead to a class of Hadamard matrices of *'generalized quaternion type'*, as is discussed in a paper [**11**] by one of the authors, where the center of the quaternion algebra is extended to the maximal real subfield of a cyclotomic field $\boldsymbol{Q}(\zeta_{2^s})$. Also the family of reduced Williamson equations with two empty subsets, in general, will be treated in the sequel.

§ 2. Relative Gauss sums in a finite field.

4. We denote by ζ_m the primitive m^{th} root of unity $e^{2\pi i/m}$ and by $\boldsymbol{Q}_m$ the cyclotomic field $\boldsymbol{Q}(\zeta_m)$. The Galois group of $\boldsymbol{Q}_m/\boldsymbol{Q}$ consists of automorphisms

$$\sigma_c:\zeta_m \longrightarrow \zeta_m^c\,,$$

where c is taken from the multiplicative group $\boldsymbol{Z}(m)^*$ of $\boldsymbol{Z}(m)=\boldsymbol{Z}/m\boldsymbol{Z}$.

Let $F=GF(q)$ be a finite field of q elements where $q=p^t$ is a power of an odd prime p. We denote the absolute trace in F by S_F.

For a (multiplicative) character χ of F we extend this to F by letting $\chi(0)=0$. We define the *Gauss sum* $\tau(\chi)=\tau_F(\chi)$ by

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

For two characters χ, χ' of F we define the *Jacobi sum* $\pi(\chi,\chi')=\pi_F(\chi,\chi')$ by

$$\pi(\chi,\chi')=-\sum_{\alpha\in F}\chi(\alpha)\chi'(1-\alpha)\,.$$

The Gauss sums and the Jacobi sums satisfy a number of basic relations, for instance (cf. [5])

$$\sum_{\alpha\in F}\chi(\alpha)\zeta_p{}^{S_F(\beta\alpha)}=\bar{\chi}(\beta)\tau(\chi)\qquad \text{for}\quad \beta\in F^*,$$

$$\tau(\chi^p)=\tau(\chi)\,,$$

$$\tau(\chi)\overline{\tau(\chi)}=q\qquad \text{for a nonprincipal character } \chi, \tag{3}$$

$$\frac{\tau(\chi)\tau(\chi')}{\tau(\chi\chi')}=\pi(\chi,\chi')\qquad \text{if } \chi\chi' \text{ is nonprincipal.} \tag{4}$$

The finite field F can be identified with the residue class field $\mathfrak{o}/\mathfrak{p}$ for the integer ring $\mathfrak{o}$ of $\boldsymbol{Q}_{q-1}$ and a prime ideal divisor $\mathfrak{p}$ of p in $\mathfrak{o}$. A nonzero class $\alpha+\mathfrak{p}$ in $\mathfrak{o}/\mathfrak{p}$ contains just one power ζ_{q-1}^x of ζ_{q-1}, and the operation ω to single it out,

$$\omega(\alpha+\mathfrak{p})=\zeta_{q-1}^x\,,$$

is a character of $F=\mathfrak{o}/\mathfrak{p}$, which is called the *Teichmüller character* of F. This is a generator of the group of characters of F.

Let m be a divisor of $q-1$. We say that a character χ has the order m if $\chi^m=1$, the principal character. Such a character is a power of the primitive m^{th} power residue character χ_m defined by

$$\chi_m=\omega^{(q-1)/m}.$$

If χ has the order m, then the m^{th} power $\tau(\chi)^m$ of Gauss sum $\tau(\chi)$ belongs to $\boldsymbol{Q}_m$ and its prime ideal decomposition is given by Stickelberger's theorem. Namely let $\boldsymbol{p}$ be the prime ideal in $\boldsymbol{Q}_m$ divisible by $\mathfrak{p}$, and $\chi=\chi_m^{-k}$, then

$$\tau(\chi)^m\sim\boldsymbol{p}^{(mt/f)\theta},\qquad \text{or symbolically } \tau(\chi)\sim\boldsymbol{p}^{(t/f)\theta},$$

$$\theta=\sum_{c\in\boldsymbol{Z}(m)^*}\left\langle\frac{kc}{m}\right\rangle\sigma_c^{-1},$$

where $\sim$ means that two ideals on both sides are the same, and where $\langle x\rangle$ denotes the fractional part of x, and f is the smallest positive integer satisfying $p^f\equiv 1 \pmod{m}$, i.e. $\boldsymbol{p}^{t/f}$ is the relative norm of $\mathfrak{p}$ in $\boldsymbol{Q}_{q-1}/\boldsymbol{Q}_m$.

5. Next let K be an extension of degree r of F so that $K=GF(q^r)$ and denote relative trace and norm in K/F by $S_{K/F}$ and $N_{K/F}$ respectively. The character of F induced by a character χ of K is denoted by χ_F. Notice that ω_F is the Teichmüller character of F if ω is the Teichmüller character of K. In this connection there is an important result due to Davenport and Hasse [2]: If χ_F is nonprincipal then

$$\tau_K(\chi_F\circ N_{K/F})=(\tau_F(\chi_F))^r.$$

Now we need the notion of a *relative Gauss sum*. For a character χ of K

we define the relative Gauss sum $\vartheta_{K/F}(\chi)$ as the ratio of Gauss sums

$$\vartheta_{K/F}(\chi)=\tau_K(\chi)/\tau_F(\chi_F)\,.$$

This belongs to $\boldsymbol{Q}_m$ if χ has the order m. Notice that this has the norm q^{r-1} if χ_F is nonprincipal.

THEOREM 1. *If χ is a character of K inducing in F a nonprincipal character, then*

$$\vartheta_{K/F}(\chi)=\sum_{\alpha \bmod F^*}\bar{\chi}_F(S_{K/F}\alpha)\chi(\alpha)\,,$$

where the sum is extended over a system of representatives of the quotient group K^*/F^*. Also we have

$$\vartheta_{K/F}(\chi)=\sum_{S_{K/F}\beta=1}\chi(\beta)\,.$$

PROOF. An element of K^* is uniquely written as $a\alpha$ where $a\in F^*$ and α runs over a system of representatives of K^*/F^* so that

$$\begin{aligned}\tau_K(\chi)&=-\sum_{\alpha \bmod F^*}\Big(\sum_{a\in F^*}\chi(a\alpha)\zeta_p{}^{S_F(aS_{K/F}\alpha)}\Big)\\&=-\sum_{\alpha \bmod F^*}\chi(\alpha)\sum_{a\in F^*}\chi(a)\zeta_p{}^{S_F(aS_{K/F}\alpha)}\\&=\tau_F(\chi_F)\sum_{\alpha \bmod F^*}\chi(\alpha)\bar{\chi}_F(S_{K/F}\alpha)\,.\end{aligned}$$

Similarly, an element α of K^* is written uniquely as $\alpha=a\beta$ where $a\in F^*$ and $S_{K/F}\beta=1$ as long as $S_{K/F}\alpha\neq 0$. In fact $a=S_{K/F}\alpha$, $\beta=\alpha a^{-1}$ will suffice. Thus

$$\begin{aligned}\tau_K(\chi)&=-\sum_{a\in F^*}\sum_{S_{K/F}\beta=1}\chi(a)\chi(\beta)\zeta_p{}^{S_F a}\\&=\tau_F(\chi_F)\sum_{S_{K/F}\beta=1}\chi(\beta)\,,\end{aligned}$$

by noticing that the partial sum $S=\sum'\chi(\alpha)$ extended over α with $S_{K/F}\alpha=0$ is equal to 0. In fact $S=\sum'\chi(c\alpha)=\chi(c)S$ for $c\in F^*$ and we can take a c such that $\chi(c)\neq 1$ by assumption.

6. The special case where $r=2$, $q\equiv 1 \pmod 4$ and χ has the order $2(q+1)$ will be used for a construction of Williamson matrices.

THEOREM 2. *Assume $q\equiv 1 \pmod 4$ and let $q+1=2n$. Let K be a quadratic extension of $F=GF(q)$ and suppose that a character χ of K has the order $4n$ and induces in F a nonprincipal character. Then $\vartheta_{K/F}(\chi)$ is a square root of the Jacobi sum $\pi_K(\chi, \chi^q)$.*

If moreover $\chi=\chi_{4n}^{-k}$ for the primitive $4n^{th}$ power residue character of K, then $\vartheta_{K/F}(\chi)$ has the prime ideal decomposition

$$\vartheta_{K/F}(\chi) \sim \prod_{\substack{-n<c<n,\ (c,4n)=1 \\ \langle kc/4n\rangle>1/2}} \mathfrak{p}^{\sigma_c^{-1}},$$

where $\mathfrak{p}$ *is the prime ideal of* $\boldsymbol{Q}_{4n}$ *divisible by the prime ideal* $\mathfrak{P}$ *of* $\boldsymbol{Q}_{q^2-1}$, *for which the residue class field is identified with* K.

PROOF. First we see from the Davenport-Hasse relation that

$$\begin{aligned}\pi_K(\chi, \chi^q) &= \tau_K(\chi)\tau_K(\chi^q)/\tau_K(\chi^{q+1}) \\ &= \tau_K(\chi)^2/\tau_K(\chi_F \circ N_{K/F}) \\ &= \tau_K(\chi)^2/\tau_F(\chi_F)^2 \\ &= \vartheta_{K/F}(\chi)^2.\end{aligned}$$

Next we see that k is odd so that χ induces in F the quadratic residue character ψ by assumption, so by Stickelberger's theorem

$$\vartheta_{K/F}(\chi) \sim \mathfrak{p}^{\theta}, \qquad 2\theta = \sum_{c\in \boldsymbol{Z}(4n)^*} \left(\left\langle \frac{kc}{4n}\right\rangle + \left\langle \frac{kcq}{4n}\right\rangle - \frac{1}{2}\right)\sigma_c^{-1}.$$

Here

$$\left\langle \frac{kc}{4n}\right\rangle + \left\langle \frac{kcq}{4n}\right\rangle - \frac{1}{2} = \left\langle \frac{kc}{4n}\right\rangle + \left\langle \frac{1}{2} - \frac{kc}{4n}\right\rangle - \frac{1}{2},$$

and $\langle x\rangle + \langle 1/2 - x\rangle - 1/2 = 0$ or 1 according as $\langle x\rangle \leqq 1/2$ or $>1/2$. If we write M for the subset of $\boldsymbol{Z}(4n)^*$ consisting of c represented by $-n<c<n$, then $\boldsymbol{Z}(4n)^* = M \cup qM$, and the inequalities $\langle kc/4n\rangle > 1/2$ and $\langle kcq/4n\rangle > 1/2$ are equivalent, so that

$$\theta = \sum_{c\in M,\ \langle kc/4n\rangle>1/2} \sigma_c^{-1}.$$

REMARK. Theorem 2 shows that if $\chi = \chi_4^{-1}$, $k=n$, then since $\langle c/4\rangle > 1/2$ if and only if $c\equiv 3 \pmod 4$,

$$\begin{aligned}\vartheta_{K/F}(\chi) &\sim \Big(\prod_{c\equiv 3 \ (\mathrm{mod}\ 4)} \mathfrak{p}^{\sigma_c}\Big)^{1/2} \\ &\sim (\bar{\pi})^t \qquad \text{if} \quad p\equiv 1 \pmod 4, \\ &\sim (p^{t/2}) \qquad \text{if} \quad p\equiv 3 \pmod 4,\end{aligned}$$

where in the former case $\pi = a+bi$ is the prime in $\boldsymbol{Q}(i)$ divisible by $\mathfrak{P}$, or $p = a^2+b^2$, $a\equiv 1 \pmod 4$.

7. We can transform the relative Gauss sum in Theorem 2 by means of Theorem 1. Now let $\chi = \chi_{4n}^k$, k odd. Then since

$$\frac{1}{4n} = \frac{\varepsilon}{4} + \frac{1}{n}\,\frac{1-\varepsilon n}{4} \qquad \text{for} \quad \varepsilon = (-1)^{(n-1)/2} \equiv n \pmod 4$$

we have $\chi_{4n} = \chi_4^{\varepsilon}\chi_n^{(1-\varepsilon n)/4}$. Let α be the element of K which is identified with the element $\zeta_{q^2-1}+\mathfrak{P}$ of the residue class field in $\boldsymbol{Q}_{q^2-1}$. Then α^{2n} is the lowest power of α belonging to F, and $\omega(\alpha)=\zeta_{q^2-1}$, $\chi_d(\alpha)=\zeta_d$ for any divisor d of q^2-1. Thus it follows from Theorem 1 that

$$\begin{aligned}\vartheta_{K/F}(\chi)&=\sum_{l=0}^{2n-1}\psi(S_{K/F}\alpha^l)\chi(\alpha^l)\\&=\sum_{l=0}^{2n-1}\psi(S_{K/F}\alpha^l)\chi_4^{k\varepsilon}(\alpha^l)\chi_n^{k(1-\varepsilon n)/4}(\alpha^l).\end{aligned}$$

If we put $m=(1-\varepsilon n)l/4$ then m is determined (mod n) and $l\equiv 4m$ or $\equiv 4m-n$ (mod $2n$), according as l is even or odd. Hence the above sum equals

$$\begin{aligned}&\sum_{m=0}^{n-1}(\psi(S_{K/F}\alpha^{4m})\zeta_n^{km}+\psi(S_{K/F}\alpha^{4m-n})i^{-k}\zeta_n^{km})\\&=\psi(2)+\sum_{m=1}^{n-1}(\psi(S_{K/F}\alpha^{4m})-i^k\psi(S_{K/F}\alpha^{4m-n}))\zeta_n^{km}.\end{aligned}$$

It is easy to check that

$$\psi(S_{K/F}\alpha^{m+2n})=-\psi(S_{K/F}\alpha^m),\qquad \psi(S_{K/F}\alpha^{-m})=(-1)^m\psi(S_{K/F}\alpha^m).$$

Let us write

$$(5)\qquad e_m=\psi(2S_{K/F}\alpha^{4m}),\qquad d_m=\psi(2S_{K/F}\alpha^{4m-n}),$$

and define the polynomial

$$(6)\qquad f(x)=1+\sum_{m=1}^{n-1}(e_m-id_m)x^m.$$

Then $f(x)\equiv f(x^{n-1})$ (mod x^n-1), and it was shown above that

$$\vartheta_{K/F}(\chi)=\psi(2)f(\zeta_n^k),$$

if $k\equiv 1$ (mod 4). Hence the norm relation of relative Gauss sums

$$\vartheta_{K/F}(\chi)\overline{\vartheta_{K/F}(\chi)}=q$$

implies that $f(x)\bar{f}(x^{-1})-q$ vanishes at an arbitrary n^{th} root of unity ζ_n^k, so that

$$f(x)\bar{f}(x)\equiv q\qquad(\text{mod }x^n-1).$$

§ 3. Williamson equation arising from relative Gauss sums.

8. We can now state our main theorem.

THEOREM 3. *Let n be odd and assume $q=2n-1$ is a power of prime. Let K be a quadratic extension of the finite field $F=GF(q)$, ψ the quadratic residue character of F, and α an element of K such that αF^* generates the quotient group K^*/F^*. Define z_m $(m=1, 2, \cdots, n-1)$ by*

$$z_m=(\phi(2S_{K/F}\alpha^{4m})-i\phi(2S_{K/F}\alpha^{4m-n}))/(1-i)\,.$$

Then $H=wI+\sum_{m=1}^{n-1}z_mT^m$ *is a symmetric circulant quaternion Hadamard matrix of order* n.

PROOF. If α is a primitive element, then we apply argument of the preceding section to define a polynomial $f(x)$ by (5), (6) to obtain $f(x)\bar{f}(x)\equiv q$ $(\mathrm{mod}\, x^n-1)$, or $f(T)\bar{f}(T)=qI$. Hence

$$\begin{aligned}H&=\frac{1+i}{2}(jI+f(T))\,,\\ HH^*&=(jI+f(T))(-jI+\bar{f}(T))/2\\ &=(I+f(T)\bar{f}(T)+j\bar{f}(T)-f(T)j)/2\\ &=(I+qI)/2=nI\,,\end{aligned}$$

by noticing that j acts dihedrally on $\boldsymbol{Q}(i)$, i.e., $jz=\bar{z}j$ for $z\in\boldsymbol{Q}(i)$. It was shown in the above that H is symmetric, and it is evident that H has entries in U and is circulant. In general if αF^* generates K^*/F^*, then $\alpha=c\alpha_0$ for $c\in F^*$ and a primitive element α_0 of K, so that in this case we have only to replace $f(x)$ by $\bar{f}(x)$ if necessary.

THEOREM 4. *The reduced Williamson equation corresponding to H in Theorem 3 has the form*

$$(1+2\sum_{m\in A}e_mu_m)^2+(1+2\sum_{m\in B}e_mu_m)^2+1^2+1^2=4n\,,$$

where

$$e_m=\phi(2S_{K/F}\alpha^{4m})\,,\qquad d_m=\phi(2S_{K/F}\alpha^{4m-n})\,,$$

and A, B *are subsets of* $\mathcal{H}=\{1, 2, \cdots, (n-1)/2\}$ *consisting of* m *such that* $d_me_m=1$ *or* -1 *respectively.*

This theorem enables us to write down the Williamson equation in an explicit form.

9. For a practical computation we rely on linear-feedback shift-register sequences in a finite field. Let g be an element of F such that both g and $1+4g$ are quadratic nonresidues of F. We construct the shift-register sequence $\{x_m\}_{m=0,1,2,\dots}$ based on the polynomial x^2-x-g, i.e. satisfying the recurrence formula

$$x_{m+2}=x_{m+1}+gx_m \qquad (m=0,\ 1,\ 2,\ \cdots)$$

with the initial condition

$$x_0=0\,,\qquad x_1=1\,.$$

Here let us assume

(7) $x_1,\ x_2,\ \cdots,\ x_n$ are all different from 0.

The shift-register sequence $\{x_m\}$ is determined by knowing only its first $2n$ terms, through the periodicity relation

$$x_{m+2n}=gx_m .$$

Now put

$$d_m=\psi(x_{4m}), \qquad e_m=\psi(x_{4m+n}), \qquad v=\psi(x_n),$$

and define the four subsets A_+, A_-, B_+, B_- of H by the rule:

(i) If $v=1$, then let $m\in A_+$ or A_- according as $(e_m, d_m)=(1, 1)$ or $(-1, -1)$, and $m\in B_+$ or B_- according as $(e_m, d_m)=(1, -1)$ or $(-1, 1)$.

(ii) If $v=-1$, then let $m\in A_+$ or A_- according as $(e_m, d_m)=(-1, -1)$ or $(1, 1)$, and $m\in B_+$ or B_- according as $(e_m, d_m)=(-1, 1)$ or $(1, -1)$.

Then we have the Williamson equation

$$(1+2\sum_{m\in A_+}u_m-2\sum_{m\in A_-}u_m)^2+(1+2\sum_{m\in B_+}u_m-2\sum_{m\in B_-}u_m)^2+1^2+1^2=4n .$$

In fact, the condition (7) assures that a root α of $x^2-x-g=0$ generates K^*/F^*, and it is easy to see that there is an element $c\in F^*$ such that

$$x_m=cS_{K/F}\alpha^{-n+m} \qquad (m=0, 1, \cdots).$$

Thus $v=\psi(2c)$, $e_m=\psi(2c)\psi(2S_{K/F}\alpha^{4m})$, $d_m=\psi(2c)\psi(S_{K/F}\alpha^{4m-n})$, so that ve_m and vd_m are the quantities appearing in Theorem 4.

10. Theorem 4 shows that $2q=4n-2$ is a sum of two integers $1+4\sum_{m\in A}e_m\cos(2\pi m/n')$ and $1+4\sum_{m\in B}e_m\cos(2\pi m/n')$ of the maximal real subfield $\boldsymbol{Q}(\cos 2\pi/n')$ of $\boldsymbol{Q}_{n'}$ for any divisor n' of n. In particular for $n'=1$, $2q$ is a sum of two odd integers:

$$2q=(1+4(\#A_+-\#A_-))^2+(1+4(\#B_+-\#B_-))^2.$$

The following theorem gives an interpretation of the numbers $\#A_+$, $\#A_-$, $\#B_+$, $\#B_-$ in terms of the cyclotomy. We need *cyclotomic numbers* of order 4. Denote by E_4 the subgroup of F^* consisting of fourth powers, and by g a generator of F^*/E_4. For $0\leqq k$, $l\leqq 3$ we denote the number of solutions in F^* of

$$x-y=1, \qquad x\in g^kE_4, \quad y\in g^lE_4$$

by $(k, l)_4$, called cyclotomic numbers of order 4.

THEOREM 5. *The numbers $\#A_+$, $\#A_-$, $\#B_+$, $\#B_-$ are the cyclotomic numbers $(0, 1)_4$, $(2, 3)_4$, $(0, 3)_4$, $(2, 1)_4$ respectively for a suitable choice of g.*

PROOF. Let α be a primitive element of K. Then for b and c in F not both zero there corresponds an integer m (mod q^2-1) by means of $b+c\alpha^n=\alpha^m$. If in particular b, c satisfy the condition

$$(8) \qquad b^2-gc^2 \in E_4\,,$$

for $g=\alpha^{2n}=N_{K/F}\alpha$, a primitive element of F, then we have

$$(9) \qquad b+c\alpha^n=\alpha^{4m}$$

for some $m\in \boldsymbol{Z}(n^2-n)$. We write this as a function $m=\mu(b, c)$ of the pair (b, c). Now we classify the $(n-1)^2$ pairs (b, c) satisfying (8) into $n-1$ equivalence classes D, each containing $n-1$ pairs, based on an equivalence relation

$$(b, c) \sim (bg^{2\nu}, cg^{2\nu}) \qquad (\nu=0, 1, \cdots, n-1)\,.$$

Here the mapping $(b, c)\rightarrow(\phi(b), \phi(c))$ can be regarded as a mapping Ψ of the set of the equivalence classes D. So, let e and d vary independently over the set $\{1, -1\}$, and consider the complete inverse image $\Psi^{-1}(e, d)$ of (e, d). We calculate $\#\Psi^{-1}(e, d)$ in two different ways.

First, each class D contains a unique pair (b, c) such that $m=\mu(b, c)$ lies in the range $0\leqq m\leqq n-1$, since $\mu(bg^{2\nu}, cg^{2\nu})\equiv m+n\nu \pmod{n^2-n}$. Then the relation (9) implies that $2b=S_{K/F}\alpha^{4m}$, $2c=S_{K/F}\alpha^{4m-n}$, so that if $D\in\Psi^{-1}(e, d)$ we have

$$\phi(2S_{K/F}\alpha^{4m})=e\,, \qquad \phi(2S_{K/F}\alpha^{4m-n})=d\,.$$

Therefore by Theorem 4,

$$\#\Psi^{-1}(1, 1)=2\#A_+\,, \qquad \#\Psi^{-1}(-1, -1)=2\#A_-\,,$$
$$\#\Psi^{-1}(1, -1)=2\#B_+\,, \qquad \#\Psi^{-1}(-1, 1)=2\#B_-\,.$$

Secondly each class D contains a unique pair (b, c) with $b^2-gc^2=1$ since $(bg^{2\nu})^2-g(cg^{2\nu})^2=(b^2-gc^2)g^{4\nu}$. Hence the number of solutions of

$$b^2-gc^2=1\,, \qquad \phi(b)=e\,,\ \ \phi(c)=d$$

is equal to 4 times the number of solutions of

$$x-y=1\,, \qquad x\in g^{1-e}E_4\,,\ \ y\in g^{2-d}E_4\,.$$

Out of the four solutions we see that $(b, c)\sim(-b, -c)\not\sim(b, -c)\sim(-b, c)$, thus $\#\Psi^{-1}(e, d)=2(1-e, 2-d)_4$ for the cyclotomic numbers of order 4. The theorem is proved by comparing two results on $\#\Psi^{-1}(e, d)$.

An explicit form of these cyclotomic numbers is known (cf. [7]). In case $p\equiv1 \pmod 4$ and $p=a^2+b^2$, $a\equiv1 \pmod 4$, define r and s by $r+si=(a+bi)^t$, and in case $p\equiv3 \pmod 4$ define $r=(-p)^{t/2}$, $s=0$.

If $q\equiv1 \pmod 8$, i.e. $\phi(2)=1$, then

$$16(0, 1)_4=q-3+2r+4s\,,$$
$$16(0, 3)_4=q-3+2r-4s\,,$$

$$16(2,\ 1)_4=16(2,\ 3)_4=q+1-2r\,.$$

If $q\equiv 5 \pmod 8$, i. e. $\phi(2)=-1$, then

$$16(2,\ 1)_4=q+1+2r+4s\,,$$

$$16(2,\ 3)_4=q+1+2r-4s\,,$$

$$16(0,\ 1)_4=16(0,\ 3)_4=q-3-2r\,.$$

§ 4. Two-square Williamson equations.

11. In case n odd and $2n-1$ is a power of prime Theorem 4 shows that there is a Williamson equation

$$(1+2\sum_{m\in A} e_m x^m)^2+(1+2\sum_{m\in B} e_m x^m)^2=4n-2\,,$$

for a variable x bound by $x^n=1$, where $e_{-m}=e_m$ and A, B is a partition of $\boldsymbol{Z}(n)-\{0\}$. We call an equation of this form a *two-square Williamson equation* of order n.

The existence of a two-square Williamson equation of order n is equivalent to the existence of a pair of symmetric circulant matrices P, Q of order n with entries ± 1 except on the main diagonal of Q where we have 0, which satisfies

$$P^2+Q^2=(2n-1)I\,.$$

In fact $R=P-Qi$ is a symmetric circulant complex matrix satisfying $RR^*=(2n-1)I$, so that if we assume that the main diagonal of P consists of 1's, the matrix

$$\begin{aligned} H&=\frac{1+i}{2}(jI+R)\\ &=(j+k)I/2+(P+Q)/2+i(P-Q)/2\\ &=wI+M, \end{aligned}$$

where M has entries from $\{\pm 1,\ \pm i\}$ except on the main diagonal where we have 0. This gives rise to a two-square Williamson equation by a procedure used in the proof of Theorem 3.

12. It is sometimes convenient to treat the two-square Williamson equation in the form

$$(\varepsilon+2\sum_{m\in A} e_m x^m)^2+(\varepsilon+2\sum_{m\in B} e_m x^m)^2=4n-2\,,\qquad e_{-m}=e_m\,, \tag{10}$$

where A, B is a partition of $\boldsymbol{Z}(n)-\{0\}$ and

$$\varepsilon=(-1)^{(n-1)/2}.$$

THEOREM 6. *Suppose that a modified two-square Williamson equation* (10) *is valid for a partition A, B, and denote by A_+, A_- the subsets of A consisting of m with $e_m=1$ or -1 respectively, and by B_+, B_- the similar subsets of B. Then*

$$A_+=A\cap 2A\,,\qquad A_-=A\cap 2B\,,\qquad B_+=B\cap 2B\,,\qquad B_-=B\cap 2A\,.$$

Moreover if $s=\#A-\#B$ then $2n-1=r^2+s^2$ for an integer $r\equiv 1$ (mod 4), *and*

$$4\#A_+=n-1-\varepsilon+r+2s\,,$$
$$4\#B_+=n-1-\varepsilon+r-2s\,,$$
$$4\#A_-=4\#B_-=n-1+\varepsilon-r\,.$$

PROOF. Writing $P=\sum_{m\in A}e_mT^m$, $Q=\sum_{m\in B}e_mT^m$ and $P_0=\sum_{m\in A}T^m$, $Q_0=\sum_{m\in B}T^m$, we see that the equation (10) written in a matric form

$$(\varepsilon I+2P)^2+(\varepsilon I+2Q)^2=(4n-2)I \tag{11}$$

is equivalent to one of a slightly simpler form

$$\varepsilon P+\varepsilon Q+P^2+Q^2=(n-1)I\,.$$

Let us consider this (mod 4). Since $P_0+Q_0+I=J$ has all its entries equal to 1, and since $\varepsilon\equiv -n+2$ (mod 4), we have

$$\begin{aligned}(n-1)I&\equiv\varepsilon P+\varepsilon Q+P_0^2+Q_0^2\\ &\equiv\varepsilon P+\varepsilon Q+P_0^2+(J-I-P_0)^2\\ &\equiv\varepsilon P+\varepsilon Q+2P_0+2P_0^2+I+(n-2)J\\ &\equiv\varepsilon(P-P_0)+\varepsilon(Q-Q_0)+2P_0+2P_0^2+(n-1)I \qquad (\mathrm{mod}\ 4)\,,\end{aligned}$$

so that

$$(P_0-P)/2+(Q_0-Q)/2+P_0+P_0^2\equiv 0 \qquad (\mathrm{mod}\ 2).$$

Now

$$(P_0-P)/2=\sum_{m\in A_-}T^m,\qquad (Q_0-Q)/2=\sum_{m\in B_-}T^m,$$

and

$$P^2\equiv\sum_{m\in A}T^{2m}\equiv\sum_{m\in 2A}T^m \qquad (\mathrm{mod}\ 2)\,.$$

Therefore comparing coefficients of T^m, we see that if $m\in A$ then $m\in A_+$ if and only if $m\in 2A$, namely that $A_+=A\cap 2A$, $A_-=A\cap 2B$. Similarly $B_+=B\cap 2B$, $B_-=B\cap 2A$.

Next denote the numbers $\#A_+$, $\#A_-$, $\#B_+$, $\#B_-$ by a_+, a_-, b_+, b_- respectively, and let

$$r=\varepsilon+a_+-a_-+b_+-b_-\,,\qquad s=a_+-a_--(b_+-b_-)\,. \tag{12}$$

Then the equation (11) with T replaced by its eigenvalue 1 shows that

$$(\varepsilon+2(a_+-a_-))^2+(\varepsilon+2(b_+-b_-))^2=4n-2\,,$$
$$(\varepsilon+a_+-a_-+b_+-b_-)^2-(a_+-a_--(b_+-b_-))^2$$
$$=r^2+s^2=2n-1\,.$$

The relation (12) together with

$$a_++a_-+b_++b_-=n-1\,, \qquad a_-=b_-$$

determines the values a_+, a_-, b_+, b_- completely as stated in the theorem. The equality $a_-=b_-$ is a consequence of $\#A=\#(2A)$, i.e. $a_++a_-=a_++b_-$, and $r\equiv 1 \pmod 4$ is checked as follows:

$$r=\varepsilon+a_++b_+-2a_-\equiv\varepsilon+a_++b_++2a_-$$
$$\equiv\varepsilon+n-1\equiv 2n-1\equiv 1 \qquad (\mathrm{mod}\ 4)\,.$$

Theorem 6 shows that the existence of a two-square Williamson equation implies that $2n-1$ is a sum of two squares: $2n-1=r^2+s^2$, $r\equiv 1 \pmod 4$. There may be more than one decomposition of this kind, but still the partition A, B of $\boldsymbol{Z}(n)-\{0\}$ involved should be such that $2\#A-(n-1)=s$ for one of the solutions. Moreover, once the set A is specified, then the distribution of $e_m=\pm 1$ within A, and within B is completely determined.

If we write the Williamson equation described in Theorem 4 in the form (10), then the values r and s are determined by Remark to Theorem 2. Namely, by using the polynomial $f(x)$ of 7 and the subsets A, B of $\boldsymbol{Z}(n)-\{0\}$ corresponding to those of 8, we have

$$r+si=\varepsilon+(a_+-a_-+b_+-b_-)+(a_+-a_--(b_+-b_-))i$$
$$=\varepsilon+\sum_{m\in A}e_m+\sum_{m\in B}e_m+(\sum_{m\in A}e_m-\sum_{m\in B}e_m)i$$
$$=\varepsilon+\sum_{m\in A}e_m+\sum_{m\in B}e_m+(\sum_{m\in A}d_m+\sum_{m\in B}d_m)i$$
$$=\varepsilon+\sum_{m=1}^{n-1}(e_m+id_m)$$
$$=\varepsilon\bar{f}(1)$$
$$=\varepsilon\vartheta_{K/F}(\chi_4)\,.$$

Here the role of A_+, A_- and of B_+, B_- should be interchanged if $\varepsilon=-1$. Now Remark to Theorem 2 shows that the ideal $(r+si)=(\vartheta_{K/F}(\chi_4))$, in $\boldsymbol{Q}(i)$, is equal to $(\pi)^t$ or to $(-p)^{t/2}$ according as $p\equiv 1 \pmod 4$ or $p\equiv 3 \pmod 4$. Thus we have

$$r+si=(a+bi)^t \qquad \text{for} \quad p\equiv 1 \pmod 4\,,$$
$$r=(-p)^{t/2},\quad s=0 \qquad \text{for} \quad p\equiv 3 \pmod 4\,.$$

This can be regarded as another derivation of an explicit formula for the cyclotomic numbers of order 4. No two-square Williamson equation is known at present except for those obtained by means of Theorem 4, and Turyn conjectured that there is none other. And this has been checked for $n \leqq 37$ and $n=61$ by Sawade.

References

[1] S. S. Agayan and A. G. Sarukhanyan, Recurrence formulas for the construction of Williamson-type matrices, Math. Notes, **30** (1982), 796-804.

[2] H. Davenport and H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. Reine Angew. Math., **172** (1935), 151-182.

[3] A. V. Geramita and J. Seberry, Orthogonal Designs: Quadratic Forms and Hadamard Matrices, Lecture Notes in Pure and Applied Math., **45**, Marcel Dekker, New York and Basel, 1979.

[4] Z. Kiyasu, Hadamard matrix and its applications, Denshi-Tsushin Gakkai, Tokyo, 1980, (in Japanese).

[5] S. Lang, Cyclotomic Fields, Springer-Verlag, New York - Heidelberg - Berlin, 1978.

[6] K. Sawade, Hadamard matrices of order 100 and 108, Bull. Nagoya Inst. Technology, **29** (1977), 147-153.

[7] T. Storer, Cyclotomy and Difference Sets, Markham Publishing Company, Chicago, 1967.

[8] R. J. Turyn, An infinite class of Williamson matrices, J. Combinatorial Theory Ser. A, **12** (1972), 319-321.

[9] W. D. Wallis, A. P. Street and J. S. Wallis, Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices, Lecture Notes in Math., **292**, Springer-Verlag, 1972.

[10] A. L. Whiteman, An infinite family of Hadamard matrices of Williamson type, J. Combinatorial Theory Ser. A, **14** (1973), 334-340.

[11] M. Yamada, On Gauss sums in a finite field and their applications to Hadamard matrices, Reports of symposium on algebraic number theory held at University of Tokyo, Oct. 17-19, 1983, 9-30, (in Japanese).

[12] K. Yamamoto, A generalized Williamson equation, Colloq. Math. Soc. János Bolyai, **37** (1983), 839-850.

Koichi YAMAMOTO
Department of Mathematics
Tokyo Woman's Christian University
Zenpukuji 2-6-1
Suginamiku, Tokyo 167
Japan

Mieko YAMADA
Department of Mathematics
Tokyo Woman's Christian University
Zenpukuji 2-6-1
Suginamiku, Tokyo 167
Japan