Partial difference sets and Jacobi sums

Partial difference sets and Jacobi sums

Rep. Fac. Sci., Kagoshima Univ.,
No. 36, pp. 11~15 (2003)

Partial difference sets and Jacobi sums

Tsuyoshi Atsumi

Department of Mathematics and Computer Science, Faculty of Science, Kagoshima University, Japan

Abstract

Let D be a union of eth cyclotomic classes . We shall give necessary and sufficient conditions that the subset D becomes a (q, k, λ, μ)-partial difference set.

Key words: partial difference set, Jacobi sum, group algebra, cyclotomic class, residue character

1 Introduction

We recall the definition of partial difference sets

Definition. Let G be an additive abelian group of order v and D be a subset of G with k elements. Then D is called a (v, k, λ, μ)-partial difference set(PDS) if the expressions gh^{-1}, for g and h in D with $g \neq h$, represent each nonidentity element in D exactly λ times and represent each nonidentity element not in D exactly μ times.

Proposition 1 (Ma) *If D is a (v, k, λ, μ)-PDS with $\lambda \neq \mu$, then $D^{-1} = D$, where $D^{-1} = \{d^{-1} \in G | d \in D\}$.*

2 Group algebra

Denote the integer ring of cyclotomic field of the eth root of unity by O_e. Let F be a finite field and F^+ be its additive group . For our discussion, it will be advisable to use group rings and thus to think of F^+ as a multiplicatively written group. We consider the group ring $\Re = O_e F$. An element of $\Re$ takes the form $\sum_{\alpha \in F} c_\alpha \alpha$. We regard the element $\sum_{\alpha \in F} c_\alpha \alpha$ in $\Re$ as a function $f : f(\alpha) = c_\alpha$ defined on F with values in O_e. For a subset S of F we use the same symbol S to denote the characteristic function of S, i.e., $S = \sum_{\alpha \in S} \alpha$ and denote by $\mathbf{0} = \{0\}$ the characteristic function of 0. The conjugate $\hat{f}$ of f is denoted by $\hat{f}(\alpha) = f(-\alpha)$. Before concluding this section, we note that for $f,\ g \in \Re$,

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

where $*$ denote product in the group ring $\Re$.

3 Cyclotomic classes

Let $q = p^\gamma = ef + 1$ where p is a prime and let ω be a primitive element in $F = GF(q)$. Then the eth cyclotomic classes $C_0, C_1, \ldots, C_{e-1}$ are defined by

$$C_i = \{\omega^{es+i} | s = 0, \ldots, f-1\}.$$

Note that the elements of C_0 are called the eth power residues, and $\{C_0, C_1, \ldots, C_{e-1}\}$ is a partition of $F - \{0\}$.

4 Jacobi sums over a finite field

Let χ be an eth power residue character, i.e., $\chi(\omega) = \zeta_e^m$ where ζ_e is a primitive eth root of unity and m is a nonnegative integer. We let $\chi(0) = 0$. For the eth power residue characters χ_1 and χ_2 we define the Jacobi sum as follows:

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

The Jacobi sum $\pi(\chi_1, \chi_2)$ for the eth power residue characters χ_1, χ_2 is an integer of the cyclotomic field of the eth root of unity.

The following are well known.

Theorem 1 *For the eth power residue characters, the following relations on Jacobi sums are satisfied:*

(i) $\pi(\chi_1, \chi_2) = \pi(\chi_2, \chi_1)$.

(ii) $\pi(\chi_1, \chi_2) = \chi(-1)\pi(\chi_1, \overline{\chi_1\chi_2})$.

(iii) $\pi(\chi_0, \chi_0) = q - 2$.

(iv) $\pi(\chi, \chi_0) = -1$ *for* $\chi \neq \chi_0$.

(v) $\pi(\chi, \bar{\chi}) = -\chi(-1)$ *for* $\chi \neq \chi_0$.

(vi) *If* χ_1, χ_2 *and* $\chi_1\chi_2$ *are nonprincipal characters, then*

$$\pi(\chi_1, \chi_2)\overline{\pi(\chi_1, \chi_2)} = q.$$

5 Lemmas

The following are useful.

Lemma 1 *Let χ be a primitive eth residue character. Then we have*

$$C_l = \frac{1}{e}\sum_{m=0}^{e-1} \zeta_e^{-lm}\chi^m.$$

Proof. See [4]. □

Lemma 2

$$\chi^l * \hat{\chi}^m = \pi(\chi^m, \chi^{-l-m})\chi^{l+m} + (q-1)\delta_{l+m,\,0}\mathbf{0},$$

where

$$\delta_{l+m,\,o} = \begin{cases} 1 & \text{when } l+m \equiv 0 (mod\ e), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. See [4]. □

Lemma 3 χ^t $(0 \leq t \leq e-1)$ *and* $\mathbf{0}$ *are linearly independent elements of* $\Re$.

Proof. See [4]. □

6 Main theorem

Let $A \subset \{0, 1, \ldots, e-1\}$ and $D = \cup_{i \in A} C_i$. When we put $\sharp A = s$, then $\sharp D = k = fs$. We now give necessary and sufficient conditions that the subset D becomes a (q, k, λ, μ)-PDS.

Theorem 2 *The subset* D *of* F *becomes a* (q, k, λ, μ)-PDS *if and only if the following equations are satisfied:*

(i) $k = s(q-1)/e$.

(ii) $\mu + s(\lambda - \mu)/e = (-es + (q-1)s^2)/e^2$.

(iii) $(\lambda - \mu)w_t = (1/e)\sum_{m=0}^{e-1} w_m w_{t-m}\pi(\chi^m, \chi^{-t})$ *for all* t, $1 \leq t \leq e-1$, *where* $w_m = \sum_{l \in A} \zeta_e^{-lm}$.

Proof.

The necessary and sufficient condition that the subset D of F becomes a (q, k, λ, μ)-PDS is that the equation

$$D * \hat{D} = \mu\chi_0 + (\lambda - \mu)D + k\mathbf{0} \tag{1}$$

is satisfied.

Suppose that equation (1) holds.

From Lemmas 1 and 2,

$$\begin{aligned} D &= \frac{1}{e}\sum_{m=0}^{e-1}\left(\sum_{l \in A}\zeta_e^{-lm}\right)\chi^m \\ &= \frac{1}{e}\sum_{m=0}^{e-1} w_m \chi^m. \end{aligned} \tag{2}$$

$$
\begin{aligned}
D * \hat{D} &= \frac{1}{e^2}\sum_{l=0}^{e-1}\sum_{m=0}^{e-1} w_l w_m \chi^l * \hat{\chi}^m \\
&= \frac{1}{e^2}\sum_{l=0}^{e-1}\sum_{m=0}^{e-1} w_l w_m (\pi(\chi^m, \chi^{-l-m})\chi^{l+m} + (q-1)\delta_{l+m,0}\mathbf{0}) \\
&= \frac{1}{e^2}\sum_{l=0}^{e-1}\sum_{m=0}^{e-1} w_l w_m \pi(\chi^m, \chi^{-l-m})\chi^{l+m} \\
&+ \frac{1}{e^2}(q-1)\sum_{m=0}^{e-1} w_m w_{-m}\mathbf{0} \\
&= \frac{1}{e^2}\sum_{t=0}^{e-1}\sum_{m=0}^{e-1} w_m w_{t-m} \pi(\chi^m, \chi^{-t})\chi^t \\
&+ \frac{1}{e^2}(q-1)\sum_{m=0}^{e-1} w_m w_{-m}\mathbf{0}. \qquad (3)
\end{aligned}
$$

On the other hand, we have

$$
\begin{aligned}
\sum_{m=0}^{e-1} w_m w_{-m} &= \sum_{m=0}^{e-1}\left(\sum_{l\in A}\zeta_e^{-lm}\right)\left(\sum_{h\in A}\zeta_e^{-hm}\right) \\
&= \sum_{l\in A}\sum_{h\in A}\sum_{m=0}^{e-1}\zeta_e^{-lm+hm} \\
&= \sum_{l\in A} e = es. \qquad (4)
\end{aligned}
$$

By (2), (3) and (4)

$$
\frac{1}{e^2}\sum_{t=0}^{e-1}\sum_{m=0}^{e-1} w_m w_{t-m}\pi(\chi^m, \chi^{-t})\chi^t + \frac{1}{e^2}(q-1)es\mathbf{0} = \mu\chi_0 + (\lambda-\mu)\frac{1}{e}\sum_{m=0}^{e-1} w_m\chi^m + k\mathbf{0} \qquad (5)
$$

By considering the coefficient of $\chi^t (t \neq 0)$ in (5), we get $(\lambda - \mu)w_t = (1/e)\sum_{m=0}^{e-1} w_m w_{t-m}\pi(\chi^m, \chi^{-t})$ for all t, $1 \leq t \leq e-1$. This proves (iii). Similarly by considering the coefficient of $\mathbf{0}$ and that of χ^0 in (5), we obtain (i) and (ii), respectively.

Suppose that equations (i), (ii) and (iii) are satisfied. From Lemma 3 it follow that equation (1) holds. This completes the proof of Theorem 2. □

We note the following;

$$
\begin{aligned}
\pi(\chi^{t-m}, \chi^{-t}) &= \bar{\chi}^t(-1)\pi(\chi^m, \chi^{-t}) \\
&= \begin{cases} \pi(\chi^m, \chi^{-t}) & \text{when } -1 \in C_0 \\ (-1)^t\pi(\chi^m, \chi^{-t}) & \text{when } -1 \notin C_0. \end{cases}
\end{aligned}
$$

If t is odd, then the above fact implies that $\sum_{m=0}^{e-1} w_m w_{t-m} \pi(\chi^m, \chi^{-t}) = 0$. So we have

Lemma 4 *If t is odd, then $w_t = 0$*

Proof. Because $\lambda \neq \mu$. □

References

[1] S. L. Ma: *Partial difference stes*, Discrete Math. **52**(1984), 75–89.

[2] S. L. Ma: *A survey of partial difference sets*, Designs, Codes and Cryptography, **4**(1994), 221–261.

[3] K. Yamamoto: *On Jacobi sums and difference sets* , J. of Combin. Th. (A) **3**(1967), 146–181.

[4] M. Yamada: *Supplementary difference sets and Jacobi sums*, Discrete Math. **103**(1992), 75–90.