External Difference Families from Gauss Sums*

Yuan Sun † *Yuqin Sun* ‡
Shanghai University of Electric and Power
201300 Shanghai China

Abstract: External Difference families (EDFs) are a new type of combinatorial designs originated from cryptography. In this paper, some constructions of EDFs are presented by using Gauss sums. Several classes of EDFs and related combinatorial designs are obtained.

Key words: *external difference family, disjoint difference family, Gauss sum.*

1 Introduction

Let $(G,+)$ be an Abelian group of order v. A (v,k,λ) difference family over G is a collection of $k-$subsets of G, $D=\{D_1,D_2,\ldots,D_u\}$, such that the multiset union satisfies the following:

$$\bigcup_{i=1}^{u}\{x-y:x,y\in D_i,x\neq y\}=\lambda(G\backslash\{0\}).$$

If furthermore $D_1,D_2,\ldots,D_u$ are mutually disjoint, then $D=\{D_1,D_2,\ldots,D_u\}$ is called a (v,k,λ) disjoint difference family, denoted by $(v,k,\lambda)-$DDF.

Difference families have been well studied and have applications in coding theory and cryptography. Ogata et al.[8] introduced a type of combinatorial designs, external difference families, which are related to difference families and have applications in authentication codes and secret sharing.

Let $(G,+)$ be an Abelian group of order v. A $(v,k,\lambda;u)$ external difference family ($(v,k,\lambda;u)-$EDF in short) D over G is a collection of u

*Project supported by Shanghai Nature Science Foundation(Grant No.10ZR1412500).
†combmathe@shiep.edu.cn
‡2008000011@shiep.edu.cn

k−subsets of G, $D = \{D_1, D_2, \ldots, D_u\}$, such that the multiset union satisfies the following:

$$\bigcup_{1 \le i,j \le u, i \ne j} (D_i - D_j) = \lambda(G \backslash \{0\}),$$

where $D_i - D_j$ is the multiset $\{x - y : x \in D_i, y \in D_j\}$.

It is easily seen that if a $(v, k, \lambda; u)$−EDF over G exists, then

$$\lambda(v-1) = k^2 u(u-1). \tag{1}$$

Note that in an EDF the blocks D_i's are required to be pairwise disjoint, while this is not the case for difference families. EDFS and difference families are different combinatorial designs, but are related.

A difference system of sets (DSS) with parameters $(n, \tau_0, \cdots, \tau_{l-1}, \delta)$ is a collection of l disjoint subsets $Q_i \subseteq \{1, 2, \cdots, n\}$, $|Q_i| = \tau_i$, $0 \le i \le l-1$, such that the multiset

$$\{\, a - b \ (\mod n) \ : \ a \in Q_i, b \in Q_j, \ 0 \le i, j \le l-1, \ i \ne j\} \tag{2}$$

contains every number i, $1 \le i \le n-1$ at least δ times. A DSS is perfect if every number i, $1 \le i \le n-1$, is contained exactly δ times in the multiset (2). A DSS is regular if all Q_i are of the same size. Hence, a perfect and regular DSS is an EDF over Z_n. Therefore, EDFs are an extension of perfect and regular DSSs.

Difference systems of sets were introduced by Levenshtein[4], and were used to construct codes that allow for synchronization in the presence of errors[5]. Tonchev[9], Mutoh and Tonchev[6], and Mutoh[7] presented further constructions of DSSs and studied their applications in code synchronization.

In the case that D is a partition of $G\backslash\{0\}$, $ku = v - 1$ and by (1) we have $\lambda = k(u-1) = v - k - 1$. Whence $u = (v-1)/k$. A connection between some DDFs and some EDFs is given in the following proposition.

Proposition 1 [2] *Let $(G, +)$ be an Abelian group of order v, and let $D = \{D_1, D_2, \ldots, D_u\}$ be a collection of k−subsets of G. If D is a partition of $G\backslash\{0\}$, then D is a $(v, k, v-k-1; (v-1)/k)$−EDF over G if and only if it is a $(v, k, k-1)$−DDF over G.*

Let p be a prime, f a positive integer, and $q = p^f$. Let $\mathbb{F}_q$ be the finite field of order q. Let $\xi_p = e^{\frac{2\pi i}{p}}$. For $r \in \mathbb{F}_q$, let ψ_r be the map defined by

$$\psi_r : \ \mathbb{F}_q \longrightarrow C^*, \quad \psi(x) = \xi_p^{Tr(rx)},$$

where Tr is the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. Then ψ_r, $r \in \mathbb{F}_q$, are all the additive characters of $\mathbb{F}_q$. Let $\chi : \ \mathbb{F}_q^* \longrightarrow C^*$ be a character of $\mathbb{F}_q^*$. We

define Gauss sum

$$g(\chi, \psi_r) = \sum_{a \in \mathbb{F}_q^*} \chi(a)\psi_r(a).$$

When $r \neq 0$,

$$g(\chi, \psi_r) = \sum_{a \in \mathbb{F}_q^*} \chi(a)\psi_r(a) = \chi^{-1}(r) \sum_{a \in \mathbb{F}_q^*} \chi(a)\psi_1(a) = \chi^{-1}(r)g(\chi, \psi_1).$$

Usually we simply write $g(\chi)$ for $g(\chi, \psi_1)$. Note that if χ_0 is the trivial multiplicative character of $\mathbb{F}_q$, then $g(\chi_0, \psi_r) = -1$. We are usually concerned with nontrivial Gauss sums $g(\chi, \psi_r)$, i.e., those with $\chi \neq \chi_0$. Gauss sums can be viewed as the Fourier coefficients in the Fourier expansion of $\psi|_{\mathbb{F}_q^*}$ in terms of the multiplicative characters of $\mathbb{F}_q$. That is, for every $c \in \mathbb{F}_q^*$,

$$\psi_r(c) = \frac{1}{q-1} \sum_{\chi \in \hat{\mathbb{F}}_q^*} g(\bar{\chi}, \psi_r)\chi(c),$$

where $\bar{\chi} = \chi^{-1}$ and $\hat{\mathbb{F}}_q^*$ denotes the character group of $\mathbb{F}_q^*$.

We first recall some properties of Gauss sums. For proofs of these properties, see [1].

(1) $g(\chi, \psi_r)\overline{g(\chi, \psi_r)} = q$, if $\chi \neq \chi_0$ and $r \neq 0$,

(2) $g(\chi^{-1}, \psi_r) = \chi(-1)g(\chi, \psi_r)$,

(3) $g(\chi^{-2}) = \overline{g(\chi^2)}$.

Lemma 1 *Let G be an abelian group of order v, D be a collection of u $k-$subsets of G, $D = \{D_1, D_2, \ldots, D_u\}$, where $D_1, D_2, \ldots, D_u$ are mutually disjoint, and let λ be a positive integer. Then D is a $(v, k, \lambda)-DDF$ in G if and only if*

$$\sum_{i=1}^{u} \psi(D_i)\overline{\psi(D_i)} = uk - \lambda$$

for every nontrivial complex character ψ of G.

Lemma 2 *Let G be an abelian group of order v, D be a collection of u $k-$subsets of G, $D = \{D_1, D_2, \ldots, D_u\}$, where $D_1, D_2, \ldots, D_u$ are mutually disjoint, and let λ be a positive integer. Then D is a $(v, k, \lambda; u)-EDF$ in G if and only if*

$$\sum_{1 \leq i,j \leq u, i \neq j} \psi(D_i)\overline{\psi(D_j)} = -\lambda$$

for every nontrivial complex character ψ of G.

In both lemmas, $\psi(D_i)$ stands for $\sum_{d \in D_i} \psi(d)$.

A number of results on the existence of EDFs and DDFs were presented in [2],[3]. The authors of these paper used cyclotomic class of order 2,4 or

6 to construct external difference families. In this paper, we extend cyclotomic constructions of combinatorial designs by Gauss sums and present further results on the existence of EDFs and DDFs, and also give answers to the problems in [2].

2 Some Results based on Gauss Sums

In this section, let $N \equiv 2 \pmod 4$, $N \geq 6$. Let q be a prime power, $\mathbb{F}_q$ be the finite field of order q, and γ be a primitive element of $\mathbb{F}_q$. Assume that $(q-1)/N$ and $q \equiv 3 \pmod 4$. Let $C_0 = \{\gamma^{Nt} \mid t = 0, 1, 2, \cdots, \frac{q-1}{N}-1\}$, and $C_i = \gamma^i C_0$ for $1 \leq i \leq N-1$. These C_i are called the cyclotomic classes of order N of $\mathbb{F}_q$. Also $(i,j) = |(C_i+1) \cap C_j|$, $1 \leq i, j \leq N$, are called the cyclotomic numbers of order N.

We need some lemmas before we give the main result.

Let $C_0^{\perp}$ be the unique subgroup of order N of $\hat{\mathbb{F}}_q^*$ and χ be a fixed generator of $C_0^{\perp}$. Then $C_0^{\perp} = \{\chi^l \mid l = 0, 1, 2, \ldots, N-1\}$.

For $r \in \mathbb{F}_q^*$, $i = 0, 1, \ldots, N-1$, let $\eta_{r,i} = \psi_r(C_i)$. We have

$$\begin{aligned}
\eta_{r,i} &= \frac{1}{N} \sum_{x \in \mathbb{F}_q^*} \psi_r(\gamma^i x^N) \\
&= \frac{1}{N} \sum_{l=0}^{N-1} g(\chi^{-l}, \psi_r) \chi^l(\gamma^i) \\
&= -\frac{1}{N} + \frac{1}{N} \sum_{l=1}^{N-1} g(\chi^{-l}, \psi_r) \chi^l(\gamma^i).
\end{aligned}$$

Lemma 3. $\sum_{i=0}^{N-1} \eta_{r,i} \overline{\eta_{r,i}} = q - \frac{q-1}{N}$.

Proof:

$$\begin{aligned}
\sum_{i=0}^{N-1} \eta_{r,i} \overline{\eta_{r,i}} &= \frac{1}{N^2} \sum_{i=0}^{N-1} (-1 + \sum_{l=1}^{N-1} g(\chi^{-l}, \psi_r) \chi^l(\gamma^i))(-1 + \\
&\quad \sum_{k=1}^{N-1} \overline{g(\chi^{-k}, \psi_r)} \chi^{-k}(\gamma^i)) \\
&= \frac{1}{N} - \frac{1}{N^2} (\sum_{l=1}^{N-1} g(\chi^{-l}, \psi_r) \sum_{i=0}^{N-1} \chi^l(\gamma^i) + \\
&\quad \sum_{k=1}^{N-1} \overline{g(\chi^{-k}, \psi_r)} \sum_{i=0}^{N-1} \chi^{-k}(\gamma^i)) + \\
&\quad \frac{1}{N^2} \sum_{l=1}^{N-1} \sum_{k=1}^{N-1} g(\chi^{-l}, \psi_r) \overline{g(\chi^{-k}, \psi_r)} \chi^l(\gamma^i) \chi^{-k}(\gamma^i) \\
&= \frac{1}{N} + \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{l=1}^{N-1} q +
\end{aligned}$$

$$= \sum_{1\le k\neq l\le N-1} g(\chi^{-l},\psi_r)\overline{g(\chi^{-k},\psi_r)}\sum_{i=0}^{N-1}\chi^{l-k}(\gamma^i)$$
$$= q-\frac{q-1}{N}.$$

Lemma 4. $\sum_{i=0}^{\frac{N}{2}-1}(\eta_{r,2i}\overline{\eta_{r,2i+1}}+\eta_{r,2i+1}\overline{\eta_{r,2i}}) = -\frac{q-1}{N}$.

Proof:

$$\sum_{i=0}^{\frac{N}{2}-1}(\eta_{r,2i}\overline{\eta_{r,2i+1}}+\eta_{r,2i+1}\overline{\eta_{r,2i}})$$
$$= \frac{1}{N^2}\sum_{i=0}^{\frac{N}{2}-1}(-1+\sum_{l=1}^{N-1}g(\chi^{-l},\psi_r)\chi^l(\gamma^{2i}))(-1+$$
$$\sum_{k=1}^{N-1}\overline{g(\chi^{-k},\psi_r)}\chi^{-k}(\gamma^{2i+1}))+\frac{1}{N^2}\sum_{i=0}^{\frac{N}{2}-1}(-1+$$
$$\sum_{l=1}^{N-1}g(\chi^{-l},\psi_r)\chi^l(\gamma^{2i+1}))(-1+\sum_{k=1}^{N-1}\overline{g(\chi^{-k},\psi_r)}\chi^{-k}(\gamma^{2i}))$$
$$= \frac{1}{N^2}\cdot N-\frac{1}{N^2}\sum_{l=1}^{N-1}g(\chi^{-l},\psi_r)\sum_{i=0}^{N-1}\chi^l(\gamma^i)-$$
$$\frac{1}{N^2}\sum_{k=1}^{N-1}\overline{g(\chi^{-k},\psi_r)}\sum_{i=0}^{N-1}\chi^{-k}(\gamma^i)+$$
$$\sum_{i=0}^{\frac{N}{2}-1}\sum_{l=1}^{N-1}\sum_{k=1}^{N-1}g(\chi^{-l},\psi_r)\overline{g(\chi^{-k},\psi_r)}\chi^l(\gamma^{2i})\chi^{-k}(\gamma^{2i+1})+$$
$$\sum_{i=0}^{\frac{N}{2}-1}\sum_{l=1}^{N-1}\sum_{k=1}^{N-1}g(\chi^{-k},\psi_r)\overline{g(\chi^{-l},\psi_r)}\chi^k(\gamma^{2i})\chi^{-l}(\gamma^{2i+1})$$
$$= \frac{1}{N}-\frac{1}{N^2}\sum_{l=1}^{N-1}g(\chi^{-l},\psi_r)\sum_{i=0}^{N-1}\chi^l(\gamma^i)-$$
$$\frac{1}{N^2}\sum_{l=1}^{N-1}\overline{g(\chi^{-l},\psi_r)}\sum_{i=0}^{N-1}\chi^{-l}(\gamma^i)+$$
$$\frac{1}{N^2}\sum_{l=1}^{N-1}\sum_{k=1,k\neq l}^{N-1}g(\chi^{-l},\psi_r)\overline{g(\chi^{-k},\psi_r)}\chi^{-k}(\gamma)\sum_{i=0}^{\frac{N}{2}-1}\chi^{l-k}(\gamma^{2i})+$$
$$\frac{1}{N^2}\sum_{l=1}^{N-1}\sum_{k=1,k\neq l}^{N-1}g(\chi^{-k},\psi_r)\overline{g(\chi^{-l},\psi_r)}\chi^k(\gamma)\sum_{i=0}^{\frac{N}{2}-1}\chi^{-l+k}(\gamma^{2i})+$$
$$\frac{1}{N^2}\sum_{l=1}^{N-1}q\sum_{i=0}^{\frac{N}{2}-1}\chi^{-l}(\gamma)+\frac{1}{N^2}\sum_{l=1}^{N-1}q\sum_{i=0}^{\frac{N}{2}-1}\chi^l(\gamma)$$
$$= \frac{1-q}{N}+\frac{1}{N^2}\sum_{l=1}^{N-1}g(\chi^{-l},\psi_r)\overline{g(\chi^{-l-\frac{N}{2}},\psi_r)}\chi^{-l-\frac{N}{2}}(\gamma)\sum_{i=0}^{\frac{N}{2}-1}\chi^{-\frac{N}{2}}(\gamma^{2i})+$$
$$\frac{1}{N^2}\sum_{l=1}^{N-1}g(\chi^{-l-\frac{N}{2}},\psi_r)\overline{g(\chi^{-l},\psi_r)}\chi^{l+\frac{N}{2}}(\gamma)\sum_{i=0}^{\frac{N}{2}-1}\chi^{\frac{N}{2}}(\gamma^{2i})$$

$$
\begin{aligned}
&= \tfrac{1-q}{N} + \tfrac{1}{2N}\sum_{l=1}^{N-1} g(\chi^{-l},\psi_r)\chi^{l+\frac{N}{2}}(-1)g(\chi^{l+\frac{N}{2}},\psi_r)\chi^{-l-\frac{N}{2}}(\gamma)+ \\
&\quad \tfrac{1}{2N}\sum_{l=1}^{N-1} g(\chi^{l},\psi_r)\chi^{l}(-1)g(\chi^{-l-\frac{N}{2}},\psi_r)\chi^{l+\frac{N}{2}}(\gamma) \\
&= \tfrac{1-q}{N} + \tfrac{1}{2N}\sum_{l=1}^{N-1} g(\chi^{l},\psi_r)\chi^{l+\frac{N}{2}}(-1)g(\chi^{-l-\frac{N}{2}},\psi_r)\chi^{l+\frac{N}{2}}(\gamma)+ \\
&\quad \tfrac{1}{2N}\sum_{l=1}^{N-1} g(\chi^{l},\psi_r)\chi^{l}(-1)g(\chi^{-l-\frac{N}{2}},\psi_r)\chi^{l+\frac{N}{2}}(\gamma) \\
&= -\frac{q-1}{N}.
\end{aligned}
$$

Note that in the last step of the above calculations we used $\chi^{\frac{N}{2}}(-1) = (-1)^{\frac{q-1}{N}\cdot\frac{N}{2}} = -1$, since both $\frac{q-1}{N}$ and $\frac{N}{2}$ are odd.

Theorem 1 Let $N \equiv 2 \pmod 4$, $N \geq 6$, and $N|q-1$, $q \equiv 3 \pmod 4$, $D_0 = C_0 \cup C_1$, $D_i = \gamma^{2i}D_0$, for $1 \leq i \leq N/2-1$. Then $D = \{D_0, D_1, \ldots, D_{N/2-1}\}$ is a $(q,(2q-2)/N, q-(2q-2)/N-1; N/2)$–EDF and a $(q,(2q-2)/N,(2q-2)/N-1)$–DDF over $\mathbb{F}_q$.

Proof: For $r \in \mathbb{F}_q^*$, we have

$$
\begin{aligned}
&\sum_{0\leq i,j\leq \frac{N}{2}-1, i\neq j} \psi_r(D_i)\overline{\psi_r(D_j)} \\
&= \sum_{i=0}^{\frac{N}{2}-1} \psi_r(D_i) \sum_{i=0, i\neq j}^{\frac{N}{2}-1} \overline{\psi_r(D_j)} \\
&= \sum_{i=0}^{\frac{N}{2}-1} \psi_r(D_i)\Big(\sum_{i=0}^{\frac{N}{2}-1} \overline{\psi_r(D_j)} - \overline{\psi_r(D_i)}\Big) \\
&= \sum_{i=0}^{\frac{N}{2}-1} \psi_r(D_i)(-1-\overline{\psi_r(D_i)}) \\
&= -\sum_{i=0}^{\frac{N}{2}-1} \psi_r(D_i) - \sum_{i=0}^{\frac{N}{2}-1} \psi_r(D_i)\overline{\psi_r(D_i)} \\
&= 1 - \sum_{i=0}^{\frac{N}{2}-1} (\eta_{r,2i}+\eta_{r,2i+1})(\overline{\eta_{r,2i}}+\overline{\eta_{r,2i+1}}) \\
&= 1 - \sum_{i=0}^{N-1} \eta_{r,i}\overline{\eta_{r,i}} - \sum_{i=0}^{\frac{N}{2}-1} (\eta_{r,2i}\overline{\eta_{r,2i+1}} + \eta_{r,2i+1}\overline{\eta_{r,2i}}) \\
&= -q + \frac{2q-2}{N} + 1.
\end{aligned}
$$

By Proposition 1 and Lemma 3, D is a $(q,(2q-2)/N, q-(2q-2)/N-1; N/2)$–EDF and a $(q,(2q-2)/N,(2q-2)/N-1)$–DDF over $\mathbb{F}_q$. In [3], the authors proved that Theorem 1 in the case where when $N = 6$. We generalized the result and proved that the result is valid when $N \equiv 2$ (mod 4).

3 Concluding Remark

In this paper, we have used Gauss sums to construct DDFs and EDFs. Several results are presented. The following problem was asked in [2].

Problem 3.1 Give more constructions $(v, k, k-1)-$ DDFs and $(v, k, v-k-1, (v-1)/k)$ in Abelian groups G.

In this paper, Theorem 1 gives answer to Problem 3.1.

References

[1] L. D. Berndt, R. J. Evans, and K. S. Williams, Gauss and Jacobi sums, A WileyInterscience Publication, 1998.

[2] Y. Chang and C. Ding, Constructions of external difference families and disjoint difference families, Des Codes Crypt 40(2006), 167-185.

[3] B.Huang, D. Wu, Cyclotomy constructions of external difference families and disjoint difference families, Journal of Combinatorial Designs 17 (2009), 333-341.

[4] Levenshtein V.I., One method of constructing qu asi codes providing synchronization in the presence of errors. Prob. Infor. Transm 7(3) (1971), 215-222.

[5] Levenshtein V.I., Combinatorial problems motivated by comma-free codes. J. Combin. Des. 12 (2004), 184-196.

[6] Mutoh Y., Tonchev V.D., Difference systems of sets and cyclotomy. 308(14) (2008), 2959-2969.

[7] Mutoh Y., Difference systems of sets and cyclotomy II, preprint.

[8] W. Ogata, K. Kurosawa, D. R. Stinson and H. Saido, New combinatorial designs and their applications to authentication codes and secret sharing schemes, Discrete Math 279 (2004), 383-405.

[9] Tonchev D.V., Difference systems of sets and code synchronization. Rendiconti del Seminario Matematico di Messna Ser II 9 (2003), 217-226.