# External Difference Families from Lines *

*Yuan Sun* †
Department of Mathematics and Physics
Shanghai University of Electric Power
201300 Shanghai China
*Hao Shen*
Department of Mathematics
Shanghai Jiaotong University
200240 Shanghai China

**Abstract:** Using lines in a two-dimensional vector space $GF(q^2)$ over $GF(q)$, we construct some classes of external difference families over $GF(q^2)$.

**Key words:** difference families, external difference families, disjoint difference families, difference systems of sets, lines.

## 1 Introduction

Let $(G,+)$ be an Abelian group of order $v$. A $(v,k,\lambda)$ difference family [$(v,k,\lambda)$-DF in short] over $G$ is a collection of $k-$subsets of G, $D = \{D_1, D_2, \cdots, D_m\}$, such that the multiset union

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

A $(v,k,\lambda)$-DF $D$ is called *disjoint*, denoted by $(v,k,\lambda)$-DDF, if the base blocks of $D$ are mutually disjoint and $\bigcup_{i=1}^{m} D_i = G \setminus \{0\}$.

Difference families are well studied and have applications in coding theory and cryptography. Ogata et al[6] introduced a type of combinatorial designs, *external difference families*, which related to difference families and have applications in authentication codes and secret sharing.

*Project supported by Science and Technology Commission of Shanghai under Grant No. 071605123

†sunyuan@sjtu.edu.cn

Let $(G,+)$ be an Abelian group of order $v$. A $(v,k,\lambda,m)$ external difference family [$(v,k,\lambda,m)$-EDF in short] $D$ over $G$ is a collection of $m$ $k-$subsets of G, $D=\{D_1,D_2,\cdots,D_m\}$, such that the multiset union

$$\bigcup_{1\le i\neq j\le m}(D_i-D_j)=\lambda(G\setminus\{0\})$$

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

It is easy to prove that if a $(v,k,\lambda,m)$-EDF over $G$ exists, then

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

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

A difference system of sets (DSS) with parameters $(v,k_0,k_1,\cdots,k_{l-1},\delta)$ is a collection of $l$ disjoint subsets $D_i\subseteq\{1,2,\cdots,v\}$, $|D_i|=k_i$, $0\le i\le l-1$, such that the multiset

$$\{a-b(\mathrm{mod}v)|a\in D_i,b\in D_j,0\le i,j\le l-1,i\neq j\} \tag{2}$$

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

Difference systems of sets were introduced by Levenshtein[3], and were used to construct codes that allow for synchronization in the presence of errors[4]. Tonchev [7][8][9], Mutoh and Tonchev[5] presented further constructions of DSSs and studied their applications in code synchronization. Chang and Ding[2] using cyclotomy of order 4 and 6 presented some constructions of EDFs and disjoint difference families.

A convenient way to study an external difference family is to use a group ring. Let $(G,+)$ be an additive Abelian group and $Z$ be the ring of all integers. Let $Z[G]$ denote the ring of formal polynomials

$$Z[G]=\left\{\sum_{g\in G}a_gX^g|a_g\in Z\right\}$$

where $X$ is an indeterminate. The ring $Z[G]$ has operations given by

$$c\sum_{g\in G}a_gX^g+d\sum_{g\in G}b_bX^g=\sum_{g\in G}(ca_g+bd_g)X^g$$

and

$$(\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g) = \sum_{h\in G}(\sum_{g\in G} a_g b_{h-g} X^h)$$

for $c, d \in Z$. The zero and unit of $Z[G]$ are $\sum_{g\in G} 0X^g$ and $X^0 := 1$, respectively. If $S \subset G$ is a subset of $G$, we will identify $S$ with the group ring element $S(X) = \sum_{g\in S} X^g$. With the above notations, we can rephrase the definition of a $(v, k, \lambda, u)$-EDF $D = \{D_1, D_2, \cdots, D_m\}$ in $G$ as

$$\sum_{1\le i\ne j\le m} D_i(X)D_j(X^{-1}) = -\lambda + \lambda G(X). \tag{3}$$

The following proposition follows directly from (3).

**Proposition 1** [2] *Let $(G,+)$ be an Abelian group of order $v$, and let $D = \{D_1, D_2, \cdots, D_m\}$ be a collection of pairwise disjoint $k$-subsets of $G$. Then $D$ is a $(v, k, \lambda, m)$-EDF in $G$ if and only if*

$$D(X)D(X^{-1}) - \sum_{i=1}^{m} D_i(X)D_i(X^{-1}) = -\lambda + \lambda G(X) \tag{4}$$

*where $D = \bigcup_{i=1}^{m} D_i$.*

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

**Proposition 2** [2] *Let $(G,+)$ be an Abelian group of order $v$, and let $D = \{D_1, D_2, \cdots, D_m\}$ 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 $G$.*

# 2 Construction

In the following, let $q$ be an odd prime power and $GF(q^2)$ be the finite field of order $q^2$. $G$ is the additive group of $GF(q^2)$. For convenience, we select and fix a primitive element g of $GF(q^2)$. If we view $GF(q^2)$ as a two-dimensional vector space over $GF(q)$, then the one-dimensional subspaces of $GF(q^2)$ over $GF(q)$ are $S_j = \{g^{(q+1)t+j} | t = 0, 1, 2, \cdots, (q-2)\} \cup \{0\}$, $|S_j| = q$, $0 \le j \le q$. Let $L_j = S_j\backslash\{0\}$, $|L_j| = q-1$, $0 \le j \le q$. These $L_j$s will be called lines in the rest of this paper. Actually, These $L_i$s are also called the cyclotomy classes of order $q+1$ over $G$. Let $e$ be a divisor of $q+1$, the cyclotomic numbers of order $e$ over $GF(q^2)$ are uniform[1]. We will construct some classes of external difference families by lines.

At first, we have

**Lemma 1**

$$S_i(X)S_j(X) = \begin{cases} qS_i(X) & \text{if } i = j \\ G(X) & \text{otherwise} \end{cases}$$

**Proof:** Let $s_{i_1}, s_{i_2} \in S_i$, $s_{j_1}, s_{j_2} \in S_j$. $s_{i_1} = g^{t_1(q+1)+i}$, $s_{i_2} = g^{t_2(q+1)+i}$, $s_{j_1} = g^{t_3(q+1)+j}$, $s_{j_2} = g^{t_4(q+1)+j}$, and $t_1 \neq t_2$, $t_3 \neq t_4$.

If

$$s_{i_1} + s_{j_1} = s_{i_2} + s_{j_2}, \tag{5}$$

then

$$s_{i_1} - s_{i_2} = s_{j_2} - s_{j_1}.$$

We have

$$g^i(g^{t_1(q+1)} - g^{t_2(q+1)}) = g^j(g^{t_4(q+1)} - g^{t_3(q+1)}),$$

$$(g^{t_1(q+1)} - g^{t_2(q+1)})(g^{t_4(q+1)} - g^{t_3(q+1)})^{-1} = g^{j-i}. \tag{6}$$

Because of $(g^{q+1})^{q-1} = 1$, $g^{q+1} \in GF(q)$. The left side of (6) is an element of $GF(q)$. Since $0 \leq i < j \leq q$, $1 \leq j - i \leq q$. $g^{j-i} \notin GF(q)$. There is a contradiction. Therefore, the assumption (5) is impossible. □

Let $m, n \in Z$ and $m|(q+1)$, $q+1 = mn$. Let $D = \{D_1, D_2, \cdots, D_m\}$ over $G$ be a collection of $n(q-1)$-subsets of $G$, each $D_i = L_{i_1} \cup L_{i_2} \cup \cdots \cup L_{i_n}$ is a union of $n$ different lines, $1 \leq i \leq m$. $D_i \cap D_j = \emptyset$, $i \neq j$. Then $D_1, D_2, \cdots, D_m$ form a partition of $G \backslash \{0\}$.

**Theorem 1** *$D = \{D_1, D_2, \cdots, D_m\}$ is a $(q^2, n(q-1), q^2 - nq + n - 1, m)$-EDF over $G = (GF(q^2), +)$.*

Proof: Since $-1 = g^{\frac{q-1}{2}(q+1)} \in L_0$, we see that $L_j(X^{-1}) = L_j(X)$, $0 \leq j \leq q$. Now it suffices to check that $D = \{D_1, D_2, \cdots, D_m\}$ satisfies the difference family equation (3) or (4) in $Z[G]$.

$$\begin{aligned}
\sum_{i=1}^{m} D_i(X)D_i(X^{-1}) &= \sum_{i=1}^{m}(\sum_{j=1}^{n} L_{i_j}(X))^2 \\
&= \sum_{i=1}^{m}(\sum_{j=1}^{n} S_{i_j}(X) - n)^2 \\
&= \sum_{i=1}^{m}((\sum_{j=1}^{n} S_{i_j}(X))^2 - 2n\sum_{j=1}^{n} S_{i_j}(X) + n^2) \\
&= \sum_{i=1}^{m}(\sum_{j=1}^{n}(q-2n)S_{i_j}(X) + n(n-1)G(X) + n^2) \\
&= \sum_{i=1}^{m}\sum_{j=1}^{n}(q-2n)S_{i_j}(X) + mn(n-1)G(X) + mn^2 \\
&= (q-2n)G(X) + q(q-2n) + mn(n-1)G(X) + mn \\
&= (nq-n-1)G(X) + (q^2 - nq + n)
\end{aligned}$$

$$D(X)D(X^{-1}) = (G(X)\backslash\{1\})^2 = (q^2-2)G(X)\backslash\{1\} + (q^2-1)$$

Therefore

$$\begin{aligned}\sum_{1\le i\ne j\le m} D_i(X)D_j(X^{-1}) &= D(X)D(X^{-1}) - \sum_{i=1}^{m} D_i(X)D_i(X^{-1}) \\ &= -(q^2-nq+n-1) + (q^2-nq+n-1)G(X)\end{aligned}$$

This completes the proof. □

From the proof of Theorem 1, we have

**Corollary 2** *$D = \{D_1, D_2, \cdots, D_m\}$ is a $(q^2, n(q-1), nq-n-1)$-DDF in $G = (GF(q^2), +)$.*

**Remark :** If $n \ne q+1$, then $D = \{D_1, D_2, \cdots, D_m\}$ is an EDF of type $(v, k, v-k-1, (v-1)/k)$ mentioned in [2]. If $n = q+1$, then $D = G\backslash\{0\}$ is a $(q^2, q^2-1, q^2-2)$ difference set.

**Example:** Let $q = 5$ and g be a root of $x^2 - 2x - 2 = 0 \in GF(5)[x]$. Then g is a primitive element of the finite field $GF(25)$. The cyclotomic classes of order $q+1 = 6 = 2 \times 3$ are

$$\begin{array}{ll} L_0 = \{1, 2, 3, 4\}, & L_1 = \{g, 2g, 3g, 4g\}, \\ L_2 = \{2+2g, 4+4g, 1+g, 3+3g\}, & L_3 = \{4+g, 2+3g, 1+4g, 3+2g\}, \\ L_4 = \{2+g, 1+3g, 3+4g, 4+2g\}, & L_5 = \{2+4g, 1+2g, 3+g, 4+3g\}. \end{array}$$

**case 1:** Let $D_i = L_{i-1}, i = 1, 2, 3, 4, 5, 6$, then $D = \{D_1, D_2, D_3, D_4, D_5, D_6\}$ is a $(25, 4, 18, 6)$ external difference family mentioned in [2].

**case 2:** Let $D_1 = L_0 \cup L_1, D_2 = L_2 \cup L_3, D_3 = L_4 \cup L_5$, then $D = \{D_1, D_2, D_3\}$ is a $(25, 8, 16, 3)$ external difference family mentioned in [2].

**case 3:** Let $D_1 = L_0 \cup L_3, D_2 = L_1 \cup L_2, D_3 = L_4 \cup L_5$, then $D = \{D_1, D_2, D_3\}$ is also a $(25, 8, 16, 3)$ external difference family, but a new kind.

# References


[1] L.D.Baumert, W.H.Mills and Robert L. Ward(1980) Uniform Cyclotomy, Journal of Number Theory 14:67-82.

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

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

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

[5] Mutoh Y, Tonchev V. D. Difference systems of sets and cyclotomy. Discrete Math., vol.308 (2008), 2959-2969.

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

[7] Tonchev V. D. Difference systems of sets and code synchronization. Rendiconti del Seminario Comput., 148(1) (2003), 93-108.

[8] Tonchev V. D. Partitions of difference sets and code synchronization. Finite Fields and Their Applications, 11 (2005), 601-621.

[9] Ryoh Fuji-Hara, Akihiro Munemasa and Vladimir D. Tonchev.Hyperplane partitions and difference systems of sets. Journal of Combinatorial Theory, Series A 113 (2006), 1689-1698.

[10] Qing Xiang. Difference families from lines and half lines. Europ J Combinatorics, 19 (1998), 395-400.