External Difference Families over $GF(q^{2^k})$*

Yuan Sun †

Shanghai University of Electric Power

201300 Shanghai China

Abstract: Using subspaces of the finite field $GF(q^{2^k})$ over $GF(q)$, we construct new classes of external difference families.

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

1 Introduction

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

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

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

Difference families are well studied and have applications in coding theory and cryptography. Ogata et al[7] 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,λ,u) external difference family [(v,k,λ,u)-EDF in short] D over G is a collection of u $k-$subsets of G, $D = \{D_1, D_2, \cdots, D_u\}$, such that the multiset union

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

*Project supported by Excellent Youth of Shanghai under Grant No. Z-2009-15, and Science and Technology Commission of Shanghai under Grant No. 071605123

†combmathe@163.com

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, λ, u)-EDF over G exists, then

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

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

A difference system of sets (DSS) with parameters $(n, \tau_0, \tau_1, \cdots, \tau_{l-1}, \delta)$ is a collection of l disjoint subsets $Q_i \subseteq \{1, 2, \cdots, n\}$, $|Q_i| = \tau_i$, $0 \leq i \leq l-1$, such that the multiset

$$\{a - b (\mathrm{mod} n) | a \in Q_i, b \in Q_j, 0 \leq i, j \leq l-1, i \neq j\} \tag{2}$$

contains every number i, $1 \leq i \leq n-1$ at least δ times. A DSS is *perfect* if every number i, $1 \leq i \leq n-1$, 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[5], and were used to construct codes that allow for synchronization in the presence of errors[6]. Tonchev[3][4][2], Mutoh and Tonchev[10], and Mutoh[11] presented further constructions of DSSs and studied their applications in code synchronization. Chang and Ding[1] using cyclotomic classes of order 4 and 6 presented some constructions of EDFs and disjoint difference families. Recently, Sun and Shen[8] constructed new classes of external difference family from lines.

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

$$Z[G] = \{\sum_{g \in G} a_g X^g | a_g \in Z\},$$

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

$$c \sum_{g \in G} a_g X^g + d \sum_{g \in G} b_b X^g = \sum_{g \in G} (c a_g + b d_g) X^g$$

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 $\sum_{g \in G} 0 X^g$ 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 notation, we can rephrase the definition of a (v, k, λ, u)-EDF $D = \{D_1, D_2, \cdots, D_u\}$ in G as

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

The following proposition follows directly from (3).

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

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

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

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 2 [1] *Let $(G,+)$ be an Abelian group of order v, and let $D = \{D_1, D_2, \cdots, D_u\}$ 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.*

2 Construction

In the following, let q be an odd prime power and $GF(q^{2^k})$ be the finite field of order q^{2^k}, where $k \ge 1$ is an integer. r is an integer, $1 \le r \le k$. G is the additive group of $GF(q^{2^k})$. For convenience, we select and fix a primitive element g of $GF(q^{2^k})$. We view $GF(q^{2^k})$ as a 2^k-dimensional vector space over $GF(q)$.

Let

$$L_{i_1} = \{g^{(q^{2^{k-1}}+1)t+i_1} | t = 0, 1, \cdots, q^{2^{k-1}} - 2\},$$

where $i_1 = 0, 1, 2, \cdots, q^{2^{k-1}}$. Then $|L_{i_1}| = q^{2^{k-1}} - 1$ and $GF(q^{2^k}) \backslash \{0\} = \cup_{i_1=0}^{q^{2^{k-1}}} L_{i_1}$. Let $S_{i_1} = L_{i_1} \cup \{0\}$, then $|S_{i_1}| = q^{2^{k-1}}$.

For L_{i_1}, $0 \le i_1 \le q^{2^{k-1}}$, let

$$L_{i_1 i_2} = \{g^{(q^{2^{k-1}}+1)((q^{2^{k-2}}+1)t+i_2)+i_1} | t = 0, 1, \cdots, q^{2^{k-2}} - 2\},$$

where $i_2 = 0, 1, 2, \cdots, q^{2^{k-2}}$. Then $|L_{i_1 i_2}| = q^{2^{k-2}} - 1$ and $L_{i_1} = \cup_{i_2=0}^{q^{2^{k-2}}} L_{i_1 i_2}$. Let $S_{i_1 i_2} = L_{i_1 i_2} \cup \{0\}$, then $|S_{i_1 i_2}| = q^{2^{k-2}}$.

For $0 \le i_1 \le q^{2^{k-1}}$, $0 \le i_2 \le q^{2^{k-2}}$, $\cdots$,$0 \le i_{r-1} \le q^{2^{k-r+1}}$. We can sperate

$$L_{i_1 i_2 \cdots i_{r-1}} = \{g^{(q^{2^{k-1}}+1)(q^{2^{k-2}}+1)\cdots(q^{2^{k-r+1}}+1)t+\sum_{j_1=2}^{r-1}(i_{j_1}\prod_{j_2=1}^{j_1-1}(q^{2^{k-j_2}}+1))+i_1} | t = 0,1,2,\cdots,q^{2^{k-r+1}}\}$$

into $q^{2^{k-r}}+1$ sets

$$L_{i_1 i_2 \cdots i_{r-1} i_r} = \{g^{(q^{2^{k-1}}+1)(q^{2^{k-2}}+1)\cdots(q^{2^{k-r+1}}+1)(q^{2^{k-r}}+1)t+\sum_{j_1=2}^{r}(i_{j_1}\prod_{j_2=1}^{j_1-1}(q^{2^{k-j_2}}+1))+i_1} | t = 0,1,2,\cdots,q^{2^{k-r}}\},$$

where $i_r = 0,1,2,\cdots,q^{2^{k-r}}$.

Now we will construct new classes of external difference families.

At first, we have

Lemma 1 For $0 \le i_1 \le q^{2^{k-1}}$, $0 \le i_2 \le q^{2^{k-2}}$, $\cdots$,$0 \le i_{r-1} \le q^{2^{k-r+1}}$. Let

$$S_{i_1 i_2 \cdots i_{r-1} i_{r_1}} = \{g^{(q^{2^{k-1}}+1)(q^{2^{k-2}}+1)\cdots(q^{2^{k-r}}+1)t+\sum_{j_1=2}^{r-1}(i_{j_1}\prod_{j_2=1}^{j_1-1}(q^{2^{k-j_2}}+1))+i_{r_1}\prod_{j_2=1}^{r-1}(q^{2^{k-j_2}}+1)+i_1} |$$
$$i_j = 0,1,2,\cdots,q^{2^{k-j}}, j = 1,2,\cdots,r-1.0 \le r_1 \le q^{2^{k-r}}\} \cup \{0\},$$

$$S_{i_1 i_2 \cdots i_{r-1} i_{r_2}} = \{g^{(q^{2^{k-1}}+1)(q^{2^{k-2}}+1)\cdots(q^{2^{k-r}}+1)t+\sum_{j_1=2}^{r-1}(i_{j_1}\prod_{j_2=1}^{j_1-1}(q^{2^{k-j_2}}+1))+i_{r_2}\prod_{j_2=1}^{r-1}(q^{2^{k-j_2}}+1)+i_1} |$$
$$i_j = 0,1,2,\cdots,q^{2^{k-j}}, j = 1,2,\cdots,r-1.0 \le r_2 \le q^{2^{k-r}}\} \cup \{0\}.$$ Then

$$S_{i_1 i_2 \cdots i_{r-1} i_{r_1}}(X) S_{i_1 i_2 \cdots i_{r-1} i_{r_2}}(X) = \begin{cases} q^{2^{k-r}} S_{i_1 i_2 \cdots i_{r-1} i_{r_1}}(X) & r_1 = r_2 \\ S_{i_1 i_2 \cdots i_{r-1}}(X) & r_1 \ne r_2 \end{cases}.$$

Proof: When $r_1 \ne r_2$, let $s_1, s_2 \in S_{i_1 i_2 \cdots i_{r-1} i_{r1}}, s_3, s_4 \in S_{i_1 i_2 \cdots i_{r-1} i_{r2}}$.

$$s_l = g^{(q^{2^{k-1}}+1)(q^{2^{k-2}}+1)\cdots(q^{2^{k-r+1}}+1)(q^{2^{k-r}}+1)t_l+ \sum_{j_1=2}^{r-1}(i_{j_1}\prod_{j_2=1}^{j_1-1}(q^{2^{k-j_2}}+1))+i_{r_1}\prod_{j_2=1}^{r-1}(q^{2^{k-j_2}}+1)+i_1}, \text{ where } l = 1, 2.$$

$$s_l = g^{(q^{2^{k-1}}+1)(q^{2^{k-2}}+1)\cdots(q^{2^{k-r+1}}+1)(q^{2^{k-r}}+1)t_l+ \sum_{j_1=2}^{r-1}(i_{j_1}\prod_{j_2=1}^{j_1-1}(q^{2^{k-j_2}}+1))+i_{r_2}\prod_{j_2=1}^{r-1}(q^{2^{k-j_2}}+1)+i_1}, \text{ where } l = 3, 4.$$

If

$$s_1 + s_3 = s_2 + s_4, \tag{5}$$

then

$$s_1 - s_2 = s_3 - s_4.$$

We have

$$g^{i_{r_1}\prod_{j=1}^{r-1}(q^{2^{k-j}}+1)}(g^{t_1\prod_{j=1}^{r}(q^{2^{k-j}}+1)} - g^{t_2\prod_{j=1}^{r}(q^{2^{k-j}}+1)}) = g^{i_{r_2}\prod_{j=1}^{r-1}(q^{2^{k-j}}+1)}(g^{t_3\prod_{j=1}^{r}(q^{2^{k-j}}+1)} - g^{t_4\prod_{j=1}^{r}(q^{2^{k-j}}+1)}),$$

$$g^{(i_{r_1}-i_{r_2})\prod_{j=1}^{r-1}(q^{2^{k-j}}+1)}(g^{t_1\prod_{j=1}^{r}(q^{2^{k-j}}+1)} - g^{t_2\prod_{j=1}^{r}(q^{2^{k-j}}+1)}) = (g^{t_3\prod_{j=1}^{r}(q^{2^{k-j}}+1)} - g^{t_4\prod_{j=1}^{r}(q^{2^{k-j}}+1)}). \tag{6}$$

Because of $(g^{j=1})^{(q^{2^{k-r}}-1)} = 1$, $g^{j=1} \in GF(q^{2^{k-r}})$. The left side of (6) is an element of $GF(q^{2^{k-r}})$.

Since $0 \le i_{r_2} < i_{r_1} \le q^{2^{k-r}}$, $1 \le i_{r_1} - i_{r_2} \le q^{2^{k-r}}$, we have

$$g^{(i_{r_2}-i_{r_1})\prod_{j=1}^{r-1}(q^{2^{k-j}}+1)} \notin GF(q^{2^{k-r}}).$$

There is a contradiction. Therefore, Assumption (5) is impossible. □

We sperate $GF(q^{2^k})$ into $(q^{2^{k-1}}+1)(q^{2^{k-2}}+1)\cdots(q^{2^{k-r}}+1)$ $(q^{2^{k-r}}-1)$−subsets, each of which is a line of some $GF(q^{2^{k-r+1}})$. $GF(q^{2^{k-r+1}})$ has $q^{2^{k-r}}+1$ lines. We sperate these $q^{2^{k-r}}+1$ lines of $GF(q^{2^{k-r+1}})$ into m parts. Each part is a union of n lines, where $mn = q^{2^{k-r}}+1$. Now we are going to construct external difference families over $GF(q^{2^k})$.

Let m, n be two positive integers, $m|(q^{2^{k-r}}+1)$, and $q^{2^{k-r}}+1 = mn$. Let

$$D = \{D_{i_1 i_2 \cdots i_r} | i_j = 0, 1, 2, \cdots, q^{2^{k-j}}, j = 1, 2, \cdots, r\},$$

where

$$D_{i_1 i_2 \cdots i_r} = \{D_{1 i_1 i_2 \cdots i_r}, D_{2 i_1 i_2 \cdots i_r}, \cdots, D_{m i_1 i_2 \cdots i_r}\},$$

is a collection of $n(q^{2^{k-r}}-1)$-subsets of $GF(q^{2^{k-r+1}})$, each $D_{l i_1 i_2 \cdots i_r} = L_{i_1 i_2 \cdots i_{r l_1}} \cup L_{i_1 i_2 \cdots i_{r l_2}} \cup \cdots \cup L_{i_1 i_2 \cdots i_{r l_n}}$ is a union of n different $L_{i_1 i_2 \cdots i_r}$, where $0 \le i_1 \le q^{2^{k-1}}$, $0 \le i_2 \le q^{2^{k-2}}$, $\cdots$,$0 \le i_{r-1} \le q^{2^{k-r+1}}$, $i_r = 0, 1, 2, \cdots, q^{2^{k-r}}$, where $l = 1, 2, \cdots, m$. When $1 \le j_1 \ne j_2 \le m$, $D_{j_1 i_1 i_2 \cdots i_r} \cap D_{j_2 i_1 i_2 \cdots i_r} = \emptyset$. Then $D_{1 i_1 i_2 \cdots i_r}, D_{2 i_1 i_2 \cdots i_r}, \cdots, D_{m i_1 i_2 \cdots i_r}$ form a partition of $L_{i_1 i_2 \cdots i_{r-1}}$.

Theorem 1 *$D = \{D_{i_1 i_2 \cdots i_r} | i_j = 0, 1, 2, \cdots, q^{2^{k-j}}, j = 1, 2, \cdots, r\}$ constructed above is a*
$(q^{2^k}, n(q^{2^{k-r}}-1), q^{2^k} - nq^{2^{k-r}} + n - 1, m\prod_{j=1}^{r-1}(q^{2^{k-j}}+1))$-EDF over $G = (GF(q^{2^k}), +)$.

Proof: Since $-1 = g^{(q^{2^{k-1}}+1)(q^{2^{k-2}}+1)\cdots(q^{2^{k-r}}+1)\frac{q^{2^{k-r}}-1}{2}} \in L_{\underbrace{00\cdots0}_{r}}$, we see that $L_{i_1 i_2 \cdots i_r}(X^{-1}) = L_{i_1 i_2 \cdots i_r}(X)$, where $i_j = 0, 1, 2, \cdots, q^{2^{k-j}}$ and $j = 1, 2, \cdots, r$. Now it suffices to check that $D = \{D_{i_1 i_2 \cdots i_r} | i_j = 0, 1, 2, \cdots, q^{2^{k-j}}, j = 1, 2, \cdots, r\}$ satisfies the difference family equation (3) or (4) in $Z[G]$.

$$\begin{aligned}
& \sum_{i_1, i_2, \cdots, i_{r-1}} \sum_{l=1}^{m} D_{l i_1 i_2 \cdots i_r}(X) D_{l i_1 i_2 \cdots i_r}(X^{-1}) \\
= & \sum_{i_1, i_2, \cdots, i_{r-1}} \sum_{l=1}^{m} (\sum_{j=1}^{n} L_{i_1 i_2 \cdots i_{r l_j}}(X))^2 \\
= & \sum_{i_1, i_2, \cdots, i_{r-1}} \sum_{l=1}^{m} (\sum_{j=1}^{n} S_{i_1 i_2 \cdots i_{r l_j}}(X) - n)^2 \\
= & \sum_{i_1, i_2, \cdots, i_{r-1}} \sum_{l=1}^{m} ((\sum_{j=1}^{n} S_{i_1 i_2 \cdots i_{r l_j}}(X))^2 \\
& -2n \sum_{j=1}^{n} S_{i_1 i_2 \cdots i_{r l_j}}(X) + n^2) \\
= & \sum_{i_1, i_2, \cdots, i_{r-1}} \sum_{l=1}^{m} (\sum_{j=1}^{n} (q^{2^{k-r}} - 2n) S_{i_1 i_2 \cdots i_{r l_j}}(X) \\
& +n(n-1) S_{i_1 i_2 \cdots i_{r-1}}(X) + n^2) \\
= & \sum_{i_1, i_2, \cdots, i_{r-1}} ((q^{2^{k-r}} - 2n) S_{i_1 i_2 \cdots i_{r-1}}(X) + q^{2^{k-r}}(q^{2^{k-r}} - 2n) \\
& +mn(n-1) S_{i_1 i_2 \cdots i_{r-1}}(X) + mn^2) \\
= & \sum_{i_1, i_2, \cdots, i_{r-1}} ((nq^{2^{k-r}} - n - 1) S_{i_1 i_2 \cdots i_{r-1}}(X) \\
& +(q^{2^{k-r+1}} - nq^{2^{k-r}} + n))
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i_1,i_2,\cdots,i_{r-1}} (L_{i_1 i_2 \cdots i_{r-1}}(X) \\
&\quad +(q^{2^{k-r+1}}-1)) \\
&= (nq^{2^{k-r}}-n-1)(G(X)\backslash\{1\}) + (q^{2^{k-r+1}}-1)) \prod_{l=1}^{r-1}(q^{2^{k-l}}+1) \\
&= (nq^{2^{k-r}}-n-1)(G(X)\backslash\{1\}) + (q^{2^k}-1),
\end{aligned}
$$

where $\sum_{i_1,i_2,\cdots,i_{r-1}} = \sum_{i_1=0}^{q^{2^{k-1}}} \sum_{i_2=0}^{q^{2^{k-2}}} \cdots \sum_{i_{r-1}=0}^{q^{2^{k-r+1}}}$.

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

Therefore,

$$
\begin{aligned}
&\sum_{i_1,i_2,\cdots,i_{r-1}} \sum_{1\le l_1\ne l_2\le m} D_{l_1 i_1 i_2 \cdots i_r}(X) D_{l_2 i_1 i_2 \cdots i_r}(X^{-1}) \\
&= D(X)D(X^{-1}) - \sum_{i_1,i_2,\cdots,i_{r-1}} \sum_{l=1}^{m} D_{l i_1 i_2 \cdots i_r}(X) D_{l i_1 i_2 \cdots i_r}(X^{-1}) \\
&= -(q^{2^k} - nq^{2^{k-r}} + n - 1) + (q^{2^k} - nq^{2^{k-r}} + n - 1)G(X)
\end{aligned}
$$

This completes the proof. □

From the proof of Theorem 1, we have

Corollary 2 *$D = \{D_{i_1 i_2 \cdots i_r} | i_j = 0, 1, 2, \cdots, q^{2^{k-j}}, j = 1, 2, \cdots, r\}$ is a $(q^{2^k}, n(q^{2^{k-r}}-1), nq^{2^{k-r}} - n - 1)$-DDF in $G = (GF(q^{2^k}), +)$.*

Example Let $f(x) = x^4 + x^3 + x^2 + 2x + 2 \in F_3[x]$ and g be a root of $f(x)$. Then g is a primitive element of $GF(3^{2^2})$.

Let $L_{i_1} = \{g^{10t+i_1} | t = 0, 1, 2, 3, 4, 5, 6, 7\}$ be lines of $GF(3^{2^2})$, where $i_1 = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Let $10 = mn$ and D_{li_1} be a union of n lines of $GF(3^{2^2})$, where $l = 1, 2, \cdots, n$. Then $D = \{D_{1i1}, D_{2i1}, \cdots, D_{mi1}\}$ is an $(81, 8n, 80 - 8n, m) - EDF$ over $GF(3^{2^2})$.

Let $L_{i_1 i_2} = \{g^{10(4t+i_2)+i_1} | t = 0, 1\}$ be lines of $GF(3^2)$, where $i_1 = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, and $i_2 = 0, 1, 2, 3$. Let $4 = mn$ and $D_{li_1 i_2}$ be a union of n lines of $GF(3^2)$, where $l = 1, 2, \cdots, n$. Let $D_{i_1 i_2} = \{D_{1 i_2 i_2}, D_{2 i_2 i_2}, \cdots, D_{m i_1 i_2}\}$. Then $D = \{D_{i_1 i_2} | i_1 = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, i_2 = 0, 1, 2, 3\}$ is an $(81, 2n, 80 - 2n, 10m) - EDF$ over $GF(3^{2^2})$.

3 Conclusion

In this correspondence, we constructed new classes of external difference families over $GF(q^{2^k})$, where $k \ge 1$. When $k = r = 1$, the main result in [8] is a special case of Theorem 1.

References

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

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

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

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

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

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

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

[8] Yuan Sun and Hao Shen. External difference families from lines. Ars Combinatoria, Accepted.

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

[10] Mutoh Y, Tonchev V.D.(2007) Difference systems of sets and cyclotomy. Discrete Math.

[11] Mutoh Y, Difference systems of sets and cyclotomoy II, Discrete Math., vol. 308 (2008), 2959-2969.