Elementary Abelian Difference Families with Block Size ≤ 6 *

Kejun Chen[†] and Zhenfu Cao
Department of Computer Science
Shanghai Jiao Tong University
Shanghai 200030, China

Ruizhong Wei
Department of Computer Science
Lakehead University
Thunder Bay, ON, P7B 5E1 Canada

1 Introduction

Let G be an additive abelian group of order v and let $\mathcal{F} = \{B_1, B_2, \cdots, B_t\}$ be a family of k-subsets of G, where

$$B_i = \{b_{i1}, b_{i2}, \cdots, b_{ik}\}, i = 1, 2, \cdots, t.$$

Such a family is called a (v, k, λ) *elementary abelian difference family* (denoted as (v, k, λ)-EADF) in G if the following conditions are hold:

1. Any nonzero element of G occurs exactly λ times in the list of differences
$$b_{ij} - b_{ih} : 1 \leq i \leq t,\ 1 \leq j \neq h \leq k;$$
2. For any $g \in G$,
$$B_i + g = B_i \Leftrightarrow g = 0 \text{ for } i = 1, 2, \cdots, t,$$

*Research supported by the Fund for Postdoctors grant 2003033312 and the NSF of Jiangsu Province Education Commission (KC), NSF for distinguished Young Scholars grant 60225007 (ZC), and NSERC grant 239135-01 (RW)

†Present address: Department of Mathematics, Yancheng Teachers College, Jiangsu 224002, China

where $B_i + g = \{b_{ij} + g : 1 \leq j \leq k\}$.

The members of a difference family $\mathcal{F}$ are called *base blocks*. A (v, k, λ)-EADF is called *cyclic* when G is a cyclic group. A necessary condition for the existence of a (v, k, λ)-EADF is

$$\lambda(v-1) \equiv 0 \pmod{k(k-1)}.$$

Let $\mathcal{F} = \{B_1, B_2, \cdots, B_t\}$ be a family of nonempty subsets of an additive group G; the *development* of $\mathcal{F}$ is defined by $dev\mathcal{F} = \{B_i + g : i = 1, 2, \cdots, t,\ g \in G\}$. For other definitions in design theory, see [5]. The following theorem explains the relationship between difference families and 2-designs.

Theorem 1.1 *Let G be an additive group of order v and let $\mathcal{F}$ be a (v, k, λ)-EADF in G. Then $(G, dev\mathcal{F})$ is a 2-(v, k, λ) design having G as a group of automorphisms which is sharply transitive on the points.*

In particular, a cyclic (v, k, λ)-EADF gives rise to a 2-(v, k, λ) design with an automorphism consisting of a single cycle of length v, i.e. a cyclic 2-(v, k, λ) design. As pointed out in [4], a $(v, k, 1)$ cyclic difference family leads to a $(v, k, 1)$ optimal optical orthogonal code.

When $\lambda = 1$, the known results about EADF with block size $k \leq 6$ can be summarized as follows:

Theorem 1.2 ([1, 2, 3, 6, 8, 9])

1. *For any prime power $q \equiv 1 \pmod{6}$, there exists a $(q, 3, 1)$-EADF.*
2. *For any prime power $q \equiv 1 \pmod{12}$, there exists a $(q, 4, 1)$-EADF.*
3. *For any prime power $q \equiv 1 \pmod{20}$, there exists a $(q, 5, 1)$-EADF.*
4. *For any prime power $q \equiv 1 \pmod{30}$, there exists a $(q, 6, 1)$-EADF with exception of $q = 61$.*

For general λ, fundamental results on the existence of (q, k, λ)-EADF have been given by Wilson in [9], which can be summarized as follows.

Theorem 1.3 ([9]) *Let $q \geq k$ be a prime power, k and λ be integers such that $\lambda(q-1) \equiv 0 \pmod{k(k-1)}$. Then there exists a (q, k, λ)-EADF if one of the following conditions is satisfied.*

1. $q > (\frac{k(k-1)}{2})^{k(k-1)}$;

2. 2λ *is a multiple of either* k *or* $k-1$; *or*

3. $\lambda \geq k(k-1)$.

In this note, we observe that Theorems 1.3 can be used to solve most cases of the existence of EADFs with $\lambda > 1$ from the existence of EADFs with $\lambda = 1$. By constructing some small difference sets, the following result can be easily obtained.

Theorem 1.4 *Let* q *be a prime power and* $\lambda > 1$ *be a positive integer. Then for each* $k \in \{3, 4, 5, 6\}$ *there exists a* (q, k, λ)*-EADF in* $GF(q)$ *if and only if* $\lambda(q-1) \equiv 0 \pmod{k(k-1)}$.

For general background on difference families and related block designs, see [5].

2 Proof of Theorem 1.4

The following result is immediate.

Lemma 2.1 *If there exists a* (q, k, λ_1)*-EADF and a* (q, k, λ_2)*-EADF in* $GF(q)$*, then there exists a* $(q, k, s\lambda_1 + t\lambda_2)$*-EADF in* $GF(q)$*, for any positive integers* s *and* t.

The following lemma follows from Theorem 1.3.2 and Theorem 1.2.

Lemma 2.2 *Let* $\lambda > 1$ *be a given positive integer. Then there exists a* $(q, 3, \lambda)$*-EADF in* $GF(q)$ *for any prime power* q *such that* $\lambda(q-1) \equiv 0 \pmod 6$.

Note that if $\gcd(\lambda, k(k-1)) = 1$, then $\lambda(q-1) \equiv 0 \pmod{k(k-1)}$ if and only if $q - 1 \equiv 0 \pmod{k(k-1)}$. In this case, the existence of (q, k, λ)-EADF in $GF(q)$ follows from the existence of $(q, k, 1)$-EADF in $GF(q)$ by Lemma 2.3. So, by Theorems 1.2, we have the following.

Theorem 2.3 *Let* $k \in \{4, 5, 6\}$ *and* $\lambda > 1$ *be a given positive integer. If* $\gcd(\lambda, k(k-1)) = 1$*, then there exists a* (q, k, λ)*-EADF in* $GF(q)$ *for any prime power* q *such that* $\lambda(q-1) \equiv 0 \pmod{k(k-1)}$ *with possible exception of* $(q, k) = (61, 6)$.

Lemma 2.4 *Let $\lambda > 1$ be a given positive integer. Then there exists a $(q, 4, \lambda)$-EADF in $GF(q)$ for any prime power q such that $\lambda(q-1) \equiv 0 \pmod{12}$.*

Proof If $\lambda \geq 12$, then by Theorem 1.3.3, there exists a $(q, 4, \lambda)$-EADF in $GF(q)$. If $\lambda \in \{2, 3, 4, 6, 8, 9, 10\}$, then 2λ is a multiple of 4 or 3. So, by Theorem 1.3.2, there exists a $(q, 4, \lambda)$-EADF in $GF(q)$. If $\lambda \in \{5, 7, 11\}$, then we have $gcd(\lambda, 12) = 1$. By Theorem 2.3 there exists a $(q, 4, \lambda)$-EADF in $GF(q)$. □

By a similar argument we have the following lemma.

Lemma 2.5 *Let $\lambda > 1$ be a given positive integer. Then there exists a $(q, 5, \lambda)$ difference family in $GF(q)$ for any prime power q such that $\lambda(q-1) \equiv 0 \pmod{20}$.*

By Theorem 1.2 we know that there does not exist a $(61, 6, 1)$ difference family in $GF(61)$. However we have the following constructions (see [5, pp. 273 and 301]).

Lemma 2.6 *There exist a $(61, 6, 2)$-EADF in $GF(61)$ and a $(2^4, 6, 2)$-EADF in $GF(2^4)$.*

To prove Lemma 2.8, we need the following lemma.

Lemma 2.7 [9] *If there exists a (q, k, λ)-EADF is $GF(q)$, then there exists a (q^n, k, λ)-EADF in $GF(q)$ for any $n \geq 1$.*

Lemma 2.8 *Let $\lambda \geq 2$ be a given positive integer. Then there exists a $(q, 6, \lambda)$-EADF in $GF(q)$ for any prime power q such that $\lambda(q-1) \equiv 0 \pmod{30}$.*

Proof For $(q, 6, 2)$-EADF, the necessary condition is $q \equiv 1 \pmod{15}$. If prime power $q \equiv 16 \pmod{30}$, then q must be the form of 2^{4n} with $n \geq 1$. So the conclusion follows from Lemmas 2.7 and 2.6.

If $\lambda \geq 30$, then by Theorem 1.3.3, there exists a $(q, 6, \lambda)$-EADF in $GF(q)$.

If $\lambda \in \{3s : 1 \leq s \leq 9\} \cup \{5t : 1 \leq t \leq 5\}$, then 2λ is a multiple of 6 or 5. By Theorem 1.3.2, there exists a $(q, 6, \lambda)$-EADF in $GF(q)$.

If $\lambda \in M = \{7, 11, 13, 17, 19, 23, 29\}$, then $\gcd(\lambda, 30) = 1$. By Theorem 2.3, there exists a $(q, 6, \lambda)$-EADF in $GF(q)$, where $q \neq 61$. For $q = 61$, let $\lambda_1 = 2$, $\lambda_2 = 3$. Then for each $\lambda \in M$, we can write $\lambda = s\lambda_1 + t\lambda_2$ with $s \in \{2, 4, 5, 7, 8, 10, 13\}$ and $t = 1$. From the above proof we know that there exists a $(61, 6, 3)$-EADF in $GF(61)$. Also, there exists a $(61, 6, 2)$-EADF in $GF(61)$. So, by Lemma 2.1, there exists a $(61, 6, \lambda)$-EADF in $GF(61)$.

If $\lambda \in E = \{4, 8, 14, 16, 22, 26, 28\}$, then it is easy to see that $\lambda(q-1) \equiv 0 \pmod{30}$ if and only if $q \equiv 1 \pmod{15}$. Since there exists a $(q, 6, 2)$-EADF in $GF(q)$, there exists a $(q, 6, \lambda)$-EADF in $GF(q)$. □

Combining all of the lemmas in this section, we complete the proof of Theorem 1.4.

References

[1] R. C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* **9** (1939), 353-399.

[2] M. Buratti, Constructions for $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, *Discrete Math.* **138** (1995), 169-175.

[3] M. Buratti, Improving two theorems of Bose on difference families, *J. Combin. Designs* **3** (1995), 15-24.

[4] M. Buratti, A powerful method for constructing difference families and optimal optical orthogonal codes, *Designs, Codes and Cryptography* **5** (1995), 13-25.

[5] C. J. Colbourn and J. H. Dinitz (eds.), CRC Handbook of Combinatorial Designs, CRC Press, New York, 1996.

[6] K. Chen and L. Zhu, Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, *J. Combin. Designs*, **7** (1999), 21-30.

[7] K. Chen and L. Zhu, Existence of $(q, 6, 1)$ difference families with q a prime power, *Designs, Codes and Cryptography* **15** (1998), 167-173.

[8] E. Netto, Zur theorie der tripelsysteme, *Math. Ann.* **42** (1893), 143-152.

[9] R. M. Wilson, Cyclotomy and difference families in elementary abelian groups, *J. Number Theory* **4** (1972), 17-47.