AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **50** (2011), Pages 201–205

A note on balanced $(q, \{3, 4\}, \lambda)$-DFs with q a prime power

M. Cheng

Department of Mathematics
Guangxi Normal University
Guilin 541004
China

Z. Mo

Department of Mathematics
Hechi University
Yizhou 546300
China

D. Wu*

Department of Mathematics
Guangxi Normal University
Guilin 541004
China
dhwu@gxnu.edu.cn

Abstract

In this note, it is proved that the necessary and sufficient conditions for the existence of a balanced $(q, \{3, 4\}, \lambda)$-DF over $GF(q)$ are $q \geq 4$ and $q \equiv 1 \pmod{\frac{18}{\gcd(18,\lambda)}}$.

1 Introduction

Let v, λ be positive integers, K a set of positive integers. A (v, K, λ) pairwise balanced design (PBD) is a pair $(\mathcal{V}, \mathcal{B})$ where $\mathcal{V}$ is a v-set whose elements are called

* Corresponding author. The work was supported in part by NSFC (No. 10961006), Guangxi Science Foundation (No. 0991089), Program for Excellent Talents in Guangxi Higher Education Institutions.

points and $\mathcal{B}$ is a family of subsets of $\mathcal{V}$ (blocks) with sizes from K such that any 2-subset of $\mathcal{V}$ is contained in exactly λ blocks. A (v, K, λ)-PBD with $K = \{k\}$ is a balanced incomplete block design and is denoted by (v, k, λ)-BIBD. A $(v, k, 1)$-BIBD is also called a Steiner 2-design.

Given an additive group G of order v and a set K of positive integers, a (v, K, λ)-DF over G is a family of subsets of G (*base blocks*) having sizes belonging to K and such that each non-zero element of G can be represented as the difference of two elements of some base block in exactly λ ways. When $K = \{k\}$, we simply speak of a $(v, k, 1)$-DF. If K contains at least two distinct elements, and the number of base blocks of size k is a constant for each $k \in K$, then the (v, K, λ)-DF is called *balanced* in [7]. The following result is known.

Lemma 1.1 *Let $\mathcal{A}$ be a (v, K, λ)-DF over G and $\mathcal{B} = \{A + g \mid A \in \mathcal{A}, g \in G\}$. Then $(G, \mathcal{B})$ is a (v, K, λ)-PBD, where $v = |G|$.*

Much work had been done for the existence of (v, k, λ)-DFs (see [1]–[13] for the examples). When $|K| \geq 2$, some results were obtained in [7]. It is easy to see that the necessary condition for the existence of a balanced $(v, \{3, 4\}, 1)$-DF is $v \equiv 1 \pmod{18}$. We have the following result.

Lemma 1.2 ([7, 14]) *Let $q = 18t+1$ be a prime power. Then there exists a balanced $(q, \{3, 4\}, 1)$-DF.*

It is not difficult to prove the following lemma.

Lemma 1.3 *The necessary conditions for the existence of a balanced $(v, \{3, 4\}, \lambda)$-DF are $v \geq 4$ and $v \equiv 1 \pmod{\frac{18}{\gcd(18,\lambda)}}$.*

Throughout this note q will always denote a prime power and it is understood that all DFs are over the additive group of a finite field. The main purpose of this paper is to prove the following theorem.

Theorem 1.4 *If q is a prime power, then the necessary and sufficient conditions for the existence of a balanced $(q, \{3, 4\}, \lambda)$-DF are $q \geq 4$ and $q \equiv 1 \pmod{\frac{18}{\gcd(18,\lambda)}}$.*

2 Proof of Theorem 1.4

The following lemma is clear.

Lemma 2.1 *If there exists a balanced (v, K, λ)-DF, then there exists a balanced $(v, K, n\lambda)$-DF for each positive integer n.*

To prove the sufficiency of Theorem 1.4, from Lemmas 1.3 and 2.1, one needs only to prove that Theorem 1.4 is true for $\lambda = 1, 2, 3, 6, 9$, and 18. The case of $\lambda = 1$ is solved in Lemma 1.2. Suppose $q \equiv 1 \pmod{e}$, and θ is a primitive element of

$GF(q)$. Let H^e be the multiplicative subgroup of index e, while $C_j^e = \theta^j C_0^e$, denotes the coset of C_0^e $(= H^e)$ in $GF(q)^* = GF(q) \setminus \{0\}$, $0 \le j \le e-1$. For $B \subset GF(q)$, define $\Delta B = \{x - y : x, y \in B, x \ne y\}$. For a set $\mathcal{B}$ of subsets of $GF(q)$, define $\Delta\mathcal{B} = \bigcup_{B \in \mathcal{B}} \Delta B$.

Similar to the proof of Theorem 1 in [13], we have the following result.

Lemma 2.2 *Let q be a prime power. If there exists a balanced (q, K, λ)-DF in $GF(q)$, then there exists a balanced (q^n, K, λ)-DF in $GF(q^n)$ for any positive integer n.*

We first deal with the cases of $\lambda = 3,\ 6$. From Lemma 1.3, the necessary conditions for the existence of a balanced $(q, \{3,4\}, 3)$-DF, $(q, \{3,4\}, 6)$-DF are $q \equiv 1 \pmod 6$, $q \equiv 1 \pmod 3$, respectively.

Lemma 2.3 *If $q \equiv 1 \pmod 6$ is a prime power, then there exists a balanced $(q, \{3,4\}, 3)$-DF. For each prime power $q = 3t+1$, there exists a balanced $(q, \{3,4\}, 6)$-DF.*

Proof For $\lambda = 3$, we have $q \equiv 1 \pmod 6$. Let ξ be a cubic primitive root of unity of $GF(q)$ (so that $\langle -\xi \rangle$ is the group of 6th roots of unity of $GF(q)$). Let S be a complete system of representatives for the cosets of $\langle -\xi \rangle$ in $GF(q)^*$, and $\mathcal{F} = \{\{s, s\xi, s\xi^2\}, \{0, s, s\xi, s\xi^2\} : s \in S\}$. Since $\Delta\{1, \xi, \xi^2\} = \{\xi - 1\}\langle -\xi \rangle$, $\Delta\{0, 1, \xi, \xi^2\} = \{1, \xi - 1\}\langle -\xi \rangle$, it follows that $\mathcal{F}$ forms a $(q, \{3,4\}, 3)$-DF.

For $\lambda = 6$, $q = 3t+1$. If t is even, then the balanced $(q, \{3,4\}, 6)$-DF comes from the existence of a balanced $(q, \{3,4\}, 3)$-DF and Lemma 2.1.

If t is odd, then $q = 2^n$, and $2|n$. From Lemma 2.2, we need only to consider the case of $q = 2^2 = 4$. It is obvious that $\mathcal{F} = \{GF(4), GF(4)^*\}$ forms a balanced $(q, \{3,4\}, 6)$-DF. ∎

For $\lambda = 2$, the necessary condition for a balanced $(q, \{3,4\}, 2)$-DF is $q \equiv 1 \pmod 9$.

Lemma 2.4 *Let $q = 9t+1$ be a prime power. Then there exists a balanced $(q, \{3,4\}, 2)$-DF.*

Proof If t is even, then $q \equiv 1 \pmod{18}$ and the result follows from Lemma 1.2 and Lemma 2.1.

If t is odd, then $q = 2^n$ and $6|n$. From Lemma 2.2, we need only to consider the case of $q = 2^6 = 64$. Let $f(x) = 1 + x + x^6$ be a primitive polynomial in $GF(64)$, and let θ be a primitive element of $GF(64)$. Let $\mathcal{A} = \{A_1, A_2\}$, where $A_1 = \{0, 1, \theta, \theta^2\}$, $A_2 = \{0, \theta^4, \theta^{44}\}$.

Then the conclusion can be obtained as follows. It is easy to check that $\Delta\mathcal{A}$ has exactly two entries in each coset of H^9 and hence $\mathcal{F} = \{sA_1, sA_2 : s \in H^9\}$ is a balanced $(64, \{3,4\}, 2)$-DF. ∎

The necessary conditions for the existence of a balanced $(q, \{3, 4\}, 9)$-DF are $q \equiv 1 \pmod 2$ and $q \geq 5$. For a balanced $(q, \{3, 4\}, 18)$-DF, the necessary condition is $q \geq 4$.

Lemma 2.5 *For each prime power $q \equiv 1 \pmod 2$ and $q \geq 5$, there exists a balanced $(q, \{3, 4\}, 9)$-DF. For each prime power $q \geq 4$, there exists a balanced $(q, \{3, 4\}, 18)$-DF.*

Proof Let $\mathcal{A} = \{A_1, A_2\}$, where A_1, A_2 contain three, four distinct elements of $GF(q)$, respectively.

For each prime power $q \equiv 1 \pmod 2$ and $q \geq 5$, let S be a complete system of representatives for the cosets of $\{1, -1\}$ in $GF(q)^*$. Then $\mathcal{F} = \{sA_i : s \in S, i = 1, 2\}$ is a balanced $(q, \{3, 4\}, 9)$-DF.

For each prime power $q \geq 4$, $\mathcal{F} = \{sA_i : s \in GF(q)^*, i = 1, 2\}$ is a balanced $(q, \{3, 4\}, 18)$-DF. This completes the proof. □

We are now in a position to prove Theorem 1.4.

Proof of Theorem 1.4: From Lemma 1.3, we need only to prove the sufficiency of Theorem 1.4. The result comes from Lemmas 1.2, 2.3-2.5, and 2.1. □

Acknowledgements

The authors wish to thank the anonymous referees for their constructive comments and suggestions that much improved the quality of this paper.

References

[1] R. J. R. Abel and M. Buratti, Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes, *J. Combin. Theory Ser. A* 106 (2004), 59–75.

[2] M. Buratti, A powerful method for constructing difference families and optimal optical orthogonal codes, *J. Combin. Des.* 5 (1995), 13–25.

[3] M. Buratti, Cyclic designs with block size 4 and related optimal optical orthogonal codes, *Des. Codes Cryptogr.* 26 (2002), 111–125.

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

[5] M. Buratti, From a $(G, k, 1)$ difference family to a $(C_k \oplus G, k, 1)$ difference family, *Des. Codes Cryptogr.* 11 (1997), 5–9.

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

[7] M. Buratti, Pairwise balanced designs from finite fields, *Discrete Math.* 208/209 (1999), 103–117.

[8] M. Buratti and A. Pasotti, Further progress on difference families with block size 4 or 5, *Des. Codes Cryptogr.* 56 (2010), 1–20.

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

[10] K. Chen and L. Zhu, Existence of $(q, 6, 1)$ difference families with q a prime power, *Des. Codes Cryptogr.* 15 (1998), 167–174.

[11] K. Chen, R. Wei and L. Zhu, Existence of $(q, 7, 1)$ difference families with q a prime power, *J. Combin. Des.* 10 (2002), 126–138.

[12] K. Chen and L. Zhu, Improving Wilson's bound on difference families, *Utilitas Math.* 55 (1999), 189–200.

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

[14] D. Wu, Z. Chen and M. Cheng, A note on the existence of balanced $(q, \{3, 4\}, 1)$ difference families, *Australas. J. Combin.* 41 (2008), 171–174.

(Received 25 Nov 2010; revised 11 Apr 2011)