AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **41** (2008), Pages 171–174

A note on the existence of balanced $(q, \{3, 4\}, 1)$ difference families

D. Wu* Z. Chen M. Cheng

Department of Mathematics
Guangxi Normal University
Guilin 541004
China

Abstract

A (v, K, λ) difference family ((v, K, λ)-DF in short) can be used to construct a (v, K, λ)-PBD. A lot of work has been done on the existence of $(v, k, 1)$ difference families ($(v, k, 1)$-DF in short) when $K = \{k\}$ is a singleton. For $K = \{3, 4\}$, partial results have been obtained by Buratti. In this paper, it is proved that there exists a balanced $(q, \{3, 4\}, 1)$-DF for each prime power $q \equiv 1 \pmod{18}$.

1 Introduction

Given an additive group G of order v and a set K of positive integers, a (v, K, λ) *difference family* 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, λ) difference family. When K contains at least two distinct elements, we say that a (v, K, λ)-DF is *balanced* if the number of base blocks of size k is constant for each $k \in K$.

Much work has been done on the existence of (v, k, λ)-DFs (see [1, 2, 4, 5, 6, 7, 8]). When $|K| \geq 2$, some results were obtained in [3]. When $K = \{3, 4\}$, it is easy to see that the necessary conditions for the existence of a balanced $(v, K, 1)$-DF is that $v \equiv 1 \pmod{18}$. The following result was stated in [3].

Lemma 1.1 *Let $q = 18t + 1$ be a prime power and let 3^e be the highest power of 3 dividing t. Then, if 3 is not a 3^{e+1}th power in $GF(q)$, there exists a balanced $(q, \{3, 4\}, 1)$-DF.*

* Research supported in part by NSFC (Grant No. 10561002), Guangxi Science Foundation (0640062) and Innovation Project of Guangxi Graduate Education. E-mail: `dhwu@gxnu.edu.cn`

In this paper, the following result is obtained.

Theorem 1.2 *There exists a balanced* $(q, \{3,4\}, 1)$*-DF for each prime power* $q \equiv 1 \pmod{18}$.

2 Proof of Theorem 1.2

The following result was stated in [3].

Lemma 2.1 *Let* $k_1, k_2, \ldots, k_t, \lambda$ *be positive integers such that* $\lambda(q-1) \equiv 0 \pmod{m}$ *where* $m = (1/2\lambda)(k_1(k_1-1) + k_2(k_2-1) + \cdots + k_t(k_t-1))$ *is also an integer. Let* $q \equiv 1 \pmod{m}$ *be an odd prime power and let* $A_h = \{a_{h1}, a_{h2}, \cdots, a_{hk_h}\}$ *be a* k_h*-subset of* $GF(q)$*,* $h = 1, 2, \cdots, t$*. If the list* $L = \{a_{hr} - a_{hs} | 1 \le r < s \le k_h\}$ *is evenly distributed over the* m*th power cosets of* $GF(q)$*, then there exists a balanced* (q, K, λ)*-DF, where* $K = \{k_1, k_2, \cdots, k_t\}$.

Applying Lemma 2.1 with $t = 2$, $k_1 = 4$, $k_2 = 3$, $m = 9$, $A_1 = \{0, 1, c, c^2\}$, $A_2 = \{0, c^3, c^4\}$, one can easily obtain the following result.

Lemma 2.2 *Let* $q = 18t+1$ *be a prime power,* $k_1 = 4$*,* $k_2 = 3$*, and* $A_1 = \{0, 1, c, c^2\}$*,* $A_2 = \{0, c^3, c^4\}$*. If the list* $L = \{1, c, c^2, c-1, c^2-1, c^2-c, c^3, c^4, c^4-c^3\}$ *is evenly distributed over the* 9*th power cosets of* $GF(q)$*, then there exists a balanced* $(q, \{3,4\}, 1)$*-DF.*

Lemma 2.3 *Let* $q = 18t+1$ *be a prime power and* $A_1 = \{0, 1, c, c^2\}$*,* $A_2 = \{0, c^3, c^4\}$*. Let* $c \in GF(q)$ *satisfy one of the following conditions:*
(1) $c \in C_1$*,* $c-1 \in C_5$ *and* $c+1 \in C_2$*;* (2) $c \in C_2$*,* $c-1 \in C_1$ *and* $c+1 \in C_4$*;*
(3) $c \in C_4$*,* $c-1 \in C_2$ *and* $c+1 \in C_8$*;* (4) $c \in C_8$*,* $c-1 \in C_4$ *and* $c+1 \in C_7$*;*
(5) $c \in C_5$*,* $c-1 \in C_7$ *and* $c+1 \in C_1$*;* (6) $c \in C_7$*,* $c-1 \in C_8$ *and* $c+1 \in C_5$*.*
Then, there exists a balanced $(q, \{3,4\}, 1)$*-DF.*

Proof It is not difficult to see that, if one of the conditions stated in this lemma is satisfied, then the list $L = \{1, c, c^2, c-1, c^2-1, c^2-c, c^3, c^4, c^4-c^3\}$ is evenly distributed over the 9th power cosets of $GF(q)$, and hence from Lemma 2.1, there exists a balanced $(q, \{3,4\}, 1)$-DF. ∎

One can apply Weil's theorem as done in [4] to prove that there exist elements c satisfying one of the conditions stated in Lemma 2.3 when $q \ge 1479680$. So, we have the following result.

Theorem 2.4 *If* $q \equiv 1 \pmod{18}$ *is a prime power,* $q \ge 1479680$*, then there exists a balanced* $(q, \{3,4\}, 1)$*-DF.*

For $q < 1479680$, and $q \neq 73, 271$, with the aid of a computer, one can also find elements c satisfying one of the conditions stated in Lemma 2.3. So, we have the following result.

Lemma 2.5 *Suppose that* $q \equiv 1 \pmod{18}$ *is a prime power,* $q \in [19, 1479680)$*, and* $q \neq 73, 271$*. Then there exists a balanced* $(q, \{3, 4\}, 1)$*-DF.*

Lemma 2.6 *There exists a balanced* $(q, \{3, 4\}, 1)$*-DF for* $q = 73$ *and* 271*.*

Proof In the two cases of $q = 73$ and $q = 271$ we have found a quadruple A_1 and a triple A_2 satisfying the conditions of Lemma 2.1:

$q = 73$: $A_1 = \{0, 4, 16, 52\}$, $A_2 = \{0, 1, 3\}$.
$q = 271$: $A_1 = \{0, 2, 13, 34\}$, $A_2 = \{0, 1, 5\}$.

This completes the proof. ∎

We are now in a position to prove Theorem 1.2.

Proof of Theorem 1.2 Lemma 2.4 takes care of all large values of $q \geq 1479680$. The small values are dealt with in Lemmas 2.5 and 2.6. This completes the proof. ∎

Acknowledgements

The authors wish to thank the anonymous referees for their helpful suggestions. In particular, one referee pointed out the construction in Lemma 2.6 which supplied an essential ingredient in the proof of Theorem 1.2.

References

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

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

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

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

[5] 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.

[6] 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.

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

[8] C.J. Colbourn and J.H. Dinitz (eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996. (Edition 2, 2007.)

(Received 30 May 2007; revised 14 Aug 2007)