AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **42** (2008), Pages 69–82

Doubly near resolvable m-cycle systems

Jinhua Wang

School of Sciences
Nantong University
Nantong 226007
P.R. China
jhwang@ntu.edu.cn

Abstract

An m-cycle system $\mathfrak{C}$ of λK_n is said to be near resolvable if the m-cycles in $\mathfrak{C}$ can be partitioned into near parallel classes $R_1, R_2, \ldots, R_{\lambda n/2}$, each one of which is a 2-factor of $\lambda K_n - v$ for some vertex v in λK_n. If an NR(n, m, λ)-CS has a pair of orthogonal resolutions, it is said to be doubly resolvable and is denoted by DNR(n, m, λ)-CS. For $m = 2, 3$, DNR$(n, m, 2)$-CSs are known as Room frames of type 1^n and DNR$(n, 3, 2)$-BIBDs, respectively. The spectra for Room frames of type 1^n and DNR$(n, 3, 2)$-BIBDs have been completed. To our knowledge, very little is known about the existence of DNR(n, m, λ)-CSs with $m \geq 4$. In this paper, we use Weil's theorem on character sum estimates to give an implicit lower bound about the existence of DNR$(mt + 1, m, \lambda)$-CSs, where $mt + 1$ is a prime power. From this result, we also show that there exists a DNR$(n, 4, \lambda)$-CS for any prime power $n \equiv 1 \pmod 4$ and $n \geq 13$.

1 Introduction

Let λK_n be the graph on n vertices in which each pair of vertices is joined by exactly λ edges. An m-cycle system of a graph G is a collection $\mathfrak{C}$ of cycles of length m whose edges partition the edges of G. A near (or almost) parallel class of a graph G is a 2-factor of $G - v$ for some vertex v in G. An m-cycle system $\mathfrak{C}$ of λK_n is said to be near (or almost) resolvable if the m-cycles in $\mathfrak{C}$ can be partitioned into near parallel classes $R_1, R_2, \ldots, R_{\lambda n/2}$ and $\mathfrak{C}$ is denoted by NR(n, m, λ)-CS. The near parallel classes $R_1, R_2, \ldots, R_{\lambda n/2}$ form a resolution of $\mathfrak{C}$. It is well-known that there exists an NR(n, m, λ)-CS if and only if $\lambda \equiv 0 \bmod 2$ and $n \equiv 1 \bmod m$ [2, Table 9.18].

A near resolvable m-cycle system $(V, \mathfrak{C})$, where V is the set $V(\lambda K_n)$ of vertices of λK_n, is said to be doubly resolvable if there exist two near resolutions R and R' of the m-cycles in $\mathfrak{C}$ such that $|R_i \cap R_j| \leq 1$ for all $R_i \in R$ and $R_j \in R'$. (It should be noted that the m-cycles of the m-cycle system are considered as labelled so that if a subset of the elements occurs as a cycle more than once the cycles are

treated as distinct.) We refer to the m-cycle system $(V, \mathfrak{C})$ as a doubly near resolvable m-cycle system, denoted by DNR(n, m, λ)-CS. It is easy to see that if there exists a DNR$(n, m, 2)$-CS, then by repeating each cycle in this design $\lambda/2$ times, we can obtain a DNR(n, m, λ)-CS. So, we only consider the $\lambda = 2$ case in the rest of this paper.

We can use a pair of orthogonal resolutions of a DNR$(n, m, 2)$-CS to construct an $n \times n$ array. For convenience, we often refer to this array as a DNR$(n, m, 2)$-CS. We index the rows and columns of the array with the pair of orthogonal resolutions R and R'. In the cell labelled (R_i, R'_j), we place $R_i \cap R'_j$ for all $R_i \in R$ and $R'_j \in R'$. If $R_i \cap R'_j = \emptyset$, the cell is left empty. The rows of the array will contain the resolution classes of the resolution R and the columns will contain the resolution classes of the orthogonal resolution R'. If the DNR$(n, m, 2)$-CS has the additional property that under an appropriate ordering of the resolution classes R and R', $R_i \cup R'_i$ contains precisely $n-1$ distinct elements of the design and $R_i \cap R'_i = \emptyset$ for all i, then the array is called an $(m, 2)$-cycle frame of type 1^n. The diagonal of an $(m, 2)$-cycle frame of type 1^n is empty and a unique element of the design can be associated with each cell (i, i). The DNR$(10, 3, 2)$-CS in Figure 1 is a $(3, 2)$-cycle frame of type 1^{10}. The element associated with cell (i, i) is i for $i = 0, 1, \ldots, 9$.

Figure 1: A DNR$(10, 3, 2)$-CS is a $(3, 2)$-cycle frame of type 1^{10} [4]

		(8,3,4)	(6,7,1)				(9,5,2)		
			(9,4,0)	(7,8,2)				(5,6,3)	
(8,9,3)				(5,0,1)					(6,7,4)
(6,1,2)	(9,5,4)				(7,8,0)				
	(7,2,3)	(5,6,0)				(8,9,1)			
		(7,9,1)					(6,8,4)		(3,2,0)
			(8,5,2)		(4,3,1)			(7,9,0)	
				(9,6,3)		(0,4,2)			(8,5,1)
(5,7,4)					(9,6,2)		(1,0,3)		
	(6,8,0)					(5,7,3)		(2,1,4)	

We also note that it is not always possible to permute the rows and columns of a DNR$(n, m, 2)$-CS to form a $(m, 2)$-cycle frame of type 1^n; we refer to [9] for examples of DNR$(n, m, 2)$-CSs which are not $(m, 2)$-cycle frames of type 1^n. (The distinction between DNR$(n, m, 2)$-CS and $(m, 2)$-cycle frames of type 1^n is important in recursive constructions.) The DNR$(13, 3, 2)$-CS (where cycles are denoted in an abbreviated form, omitting the braces and the commas of the contained cycles) in Figure 2 is not a $(3, 2)$-cycle frame of type 1^{13}. It is not possible to permute the rows and columns of the DNR$(13, 3, 2)$-CS to form a $(3, 2)$-cycle frame 1^{13}.

If we review an undirected edge ab as a 2-cycle (a, b) (i.e., a loop ab) with a pair of parallel edge ab's, then a Room frame of type 1^n (see, e.g., [5, 6]) is equivalent to a DNR$(n, 2, 2)$-CS. We also know that a Room frame of type 1^n is equivalent to a well-known design called a Room square of order n [5, 6]. The spectrum of Room

Figure 2: A DNR$(13, 3, 2)$-CS is not a $(3, 2)$-cycle frame of type 1^{13}

013			28C				49B					56A
67B	124			390				5AC				
	78C	235			4A1				6B0			
		890	346			5B2				7C1		
			9A1	457			6C3				802	
				AB2	568			704				913
A24					BC3	679			815			
	B35					C04	78A			926		
		C46					015	89B			A37	
			057					126	9AC			B48
C59				168					237	AB0		
	06A				279					348	BC1	
		17B				38A					459	C02

squares had been completed by Mullin and Wallis [11].

Theorem 1.1 (Mullin and Wallis [11]) *A Room square of order n exists if and only if n is odd and $n \neq 3$ or 5.*

The existence of DNR$(n, 2, 2)$-CSs follows immediately from the existence of Room squares.

Theorem 1.2 *A DNR$(n, 2, 2)$-CSs exists if and only if n is odd and $n \neq 3$ or 5.*

A DNR$(n, 3, 2)$-CS is well known as a DNR$(n, 3, 2)$-BIBD. The existence of DNR$(n, 3, 2)$-BIBDs has been made extensive research by several authors [7, 9, 8, 1]. Recently, Abel, Lamken and Wang [1] have completed the spectrum of DNR$(n, 3, 2)$-BIBDs.

Theorem 1.3 (Lamken [8], Abel, Lamken and Wang [1]) *Let n be a positive integer, $n \equiv 1 \bmod 3$ and $n \geq 10$. Then there exists a DNR$(n, 3, 2)$-BIBD.*

In this paper, we continue to investigate the existence of DNR$(n, m, 2)$-CSs for $m \geq 4$. In Section 2, we first introduce a cycle starter-adder construction for DNR$(n, m, 2)$-CSs and an algebraic construction for cycle starters and adders. Then, applying Weil's theorem on character sum estimates, we give an implicit lower bound for the existence of DNR$(q, m, 2)$-CSs, where $q = mt + 1$ is a prime power. In Section 3, by using the result with $m = 4$ in Section 2, we also show that there exists a DNR$(n, 4, 2)$-CS for any prime power $n \equiv 1 \bmod 4$ and $n \geq 13$.

2 DNR$(q, m, 2)$-CS for prime power q

In what follows, we will use the notation $(x_1, x_2, \ldots, x_m)$ to denote a cycle with undirected edges $x_1x_2, x_2x_3, \ldots, x_{m-1}x_m, x_mx_1$. Our construction for DNR$(n, m, 2)$-CSs is mainly a cycle starter-adder construction, which is similar to the standard frame starter-adder construction [3, 4, 12].

Let G be an additive abelian group of order n. An m-cycle starter in G is a set of $t = (n-1)/m$ m-cycles $S = \{C_i = (x_{i1}, x_{i2}, \ldots, x_{im}) | 1 \le i \le t\}$ which satisfies the following two properties:

(1) $\bigcup_{i=1}^{t} \{x_{i1}, x_{i2}, \ldots, x_{im}\} = G \setminus \{0\}$;

(2) $\bigcup_{i=1}^{t} \triangle C_i = 2 \cdot (G \setminus \{0\})$.

where $\triangle C_i$ is a set of differences in C_i, namely, $\triangle C_i = \{\pm(x_{i(j+1(mod m))} - x_{ij}) | j = 1, 2, \ldots, m\}$.

An adder $A(S)$ for m-cycle starter S is a set of elements $(a_1, a_2, \ldots, a_t) \subseteq G \setminus \{0\}$ such that $\bigcup_{i=1}^{t} \{x_{i1} + a_i, x_{i2} + a_i, \ldots, x_{im} + a_i\} = G \setminus \{0\}$.

Construction 2.1 (Starter-Adder) *If an abelian group G of order n admits an m-cycle starter S and an adder $A(S)$, then there exists a $(m, 2)$-cycle frame of type 1^n, and hence there exist a DNR$(n, m, 2)$-CS.*

Proof: Let $G = \{g_0 = 0, g_1, \ldots, g_{n-1}\}$. We label the rows $g_0, g_1, \ldots, g_{n-1}$ and the columns $g_0, g_{n-1}, g_{n-2}, \ldots, g_1$. In row g_j and column $a_i - g_j$ place the m-cycle $C_i + g_j$ for all $i = 1, 2, \ldots, (n-1)/m$. By the definition of S and $A(S)$, it is easy to verify that the resultant array is a $(m, 2)$-cycle frame of type 1^n. □

For m-cycle starter S and adder $A(S)$, we have the following algebraic construction over finite field $GF(q)$, which is similar to the algebraic construction for DNR$(q, 3, 2)$-BIBDs in [12].

Theorem 2.2 *Let $q = mt + 1$ be a prime power and $F = GF(q)$. Let T be the multiplicative subgroup of order t in $F^* = F - \{0\}$ and ξ be a primitive element of F. Let M be an m-cycle whose elements form a system of distinct representatives for the cosets of T and whose differences are evenly distributed over the cosets of T. Then, $S = \{M, M\xi^m, M\xi^{2m}, \cdots, M\xi^{(t-1)m}\}$ is a starter. Furthermore, $A(S) = (\xi^n, \xi^{m+n}, \cdots, \xi^{m(t-1)+n})$ is an adder for S if and only if the elements of $\{a + \xi^n | a \in M\}$ lie in distinct cosets of T.*

Proof: Suffice it to check that S and $A(S)$ satisfy the conditions in the definition of m-cycle starter and adder. Let $M = (x_1, x_2, \ldots, x_m)$ and $H_i = \xi^i T, 0 \le i \le m-1$. Then $\cup_{i=0}^{t-1} \{x_1\xi^{im}, x_2\xi^{im}, \ldots, x_m\xi^{im}\} = \cup_{i=0}^{m-1} H_i = F^*$, and $\cup_{i=0}^{t-1} \triangle M\xi^{im} = 2 \cdot \cup_{i=0}^{m-1} H_i = 2 \cdot F^*$. So, S is an m-cycle starter. Since $\cup_{i=0}^{t-1} \{(x_1 + \xi^n)\xi^{im}, (x_2 + \xi^n)\xi^{im}, \ldots, (x_m + \xi^n)\xi^{im}\} = \cup_{i=0}^{m-1} H_i = F^*$, hence $A(S)$ is an adder for S. This completes the proof. □

From Construction 2.1 and Theorem 2.2, in order to construct a DNR(q, m, 2)-CS, we need only to find a pair of m-cycle M and ξ^n in $GF(q)$ satisfying the conditions in Theorem 2.2. Next, we will apply Weil's theorem on character sum estimates to show that if q is sufficient large, then there exist a pair of m-cycle M and ξ^n in $GF(q)$ satisfying the conditions in Theorem 2.2.

Let $q = mt + 1$ be a prime power. Let $F = GF(q)$ and T be the multiplication subgroup of order t in $F^* = F - \{0\}$ and ξ be a primitive element of F, $H_i = \xi^i T, 0 \leq i \leq m-1$. We have the following result.

Lemma 2.3 *Let $M = (1, x, x^2, \ldots, x^{m-1})$ be an m-cycle on F.*

(i) If $x \in H_1$, $h(x) = x^{m-2} + x^{m-3} + \ldots + x + 1 \in H_{m-1}$, then $S = \{M, M\xi^m, \ldots, M\xi^{(t-1)m}\}$ is an m-cycle starter. Furthermore

(ii) If the elements of $\{a + y : a \in M\}$ lie in distinct cosets of T, then $A(S) = (y, y\xi^m, \ldots, y\xi^{(t-1)m}), y \in F^*$ is an adder for S.

Proof: The differences of M are as follows

$$\pm(x-1)\{1, x, \ldots, x^{m-2}, h(x)\}$$

If condition (i) is satisfied, then the differences of M appear in each coset of T twice. Hence S is an m-cycle starter from Theorem 2.2. If condition (ii) is satisfied, then it is clear that $A(S)$ is an adder from Theorem 2.2 again. □

Let

$$f_0(x) = \xi^{-1}x, f_1(x) = \xi^{1-m}h(x)$$

Then condition (i) stated in Lemma 2.3 can be derived if there exists an element a satisfying the following condition:

(C1) $f_i(a) \in H_0, i = 0, 1$.

In $GF(q)$, let χ be an an nontrivial multiplicative character of order m, that is, $\chi(x) = \omega^j$ if $x \in H_j, 0 \leq j \leq m-1$, where $\omega = exp(2\pi i/m)$ is the mth root of unity. Let $B_i = \chi(f_i(a)), i = 0, 1$.

Let

$$D_i = 1 + B_i + \cdots + B_i^{m-1}$$

for $i = 0, 1$. Then

$$D_i = \begin{cases} m, & \text{if } f_i(a) \in H_0 \\ 1, & \text{if } f_i(a) = 0 \\ 0, & \text{if } f_i(a) \notin H_0 \cup \{0\} \end{cases}$$

From these, form the sum

$$S_1 = \sum_{x \in GF(q)} \prod_{i=0}^{1} (1 + B_i + \cdots + B_i^{m-1}) \tag{1}$$

This sum is equal to $n_1 m^2 + d_1$ where n_1 is the number of elements a in $GF(q)$, satisfying the condition C1, and d_1 is the contribution when one of $f_i(a)$ is 0, $i = 0, 1$.

For each $i, i = 0, 1$, there is only 1 value of $a = 0$ for which $f_0(a) = 0$ and there are at most $m - 2$ values of a for which $f_1(a) = 0$ (since $f_1(x)$ is a polynomial of degree $m - 2$). Hence the contribution to S_1 when $f_0(a)$ or $f_1(a)$ is zero is at most $(m-1)m = m^2 - m$. Therefore, if we can show that $|S_1| > m^2 - m$, then there exists at least one element a in F^* satisfying the condition C1.

Expanding S_1, we obtain

$$S_1 = \sum_{a \in GF(q)} 1 + \sum_{i=0}^{1} \sum_{k=1}^{m-1} \sum_{a \in GF(q)} B_i^k + \sum_{0 \le k_0, k_1 \le m-1} \sum_{a \in GF(q)} B_0^{k_0} B_1^{k_1} \tag{2}$$

In order to estimate the inner sum in (2), we may use Weil's theorem on multiplication character sums, which can be found in [10]

Theorem 2.4 ([10]) *Let ψ be a multiplicative character of $GF(q)$ of order $m > 1$ and let $f \in GF(q)[x]$ be a monic polynomial of positive degree that is not an mth power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $GF(q)$, then for every $\alpha \in GF(q)$, we have*

$$\left| \sum_{c \in GF(q)} \psi(\alpha f(c)) \right| \le (d-1)\sqrt{q}.$$

It is clear that $f_0(x), f_1(x)$ are coprime. In fact, suppose $f_0^{k_0}(x) f_1^{k_1}(x) = p^m(x)$ for some $p(x) \in GF(q)[x]$, then $k_0 \equiv k_1 \equiv 0 \pmod m$, $1 \le k_0, k_1 \le m - 1$, a contradiction. Note that each of the inner product in (2) can be represented as $\psi(cf(a))$ for some c, where $f(x)$ is a monic polynomial. It is easy to see that $deg f_0(x) = 1$, $deg f_1'(x) = m - 2$. So from Theorem 2.4, we have

$$\left| \sum_{i=0}^{1} \sum_{k=1}^{m-1} \sum_{a \in GF(q)} B_i^k \right| \le (m-1)(m-3)\sqrt{q}$$

$$\left| \sum_{1 \le k_0, k_1 \le m-1} \sum_{a \in GF(q)} B_0^{k_0} B_1^{k_1} \right| \le (m-1)^2(m-2)\sqrt{q}$$

Then we have

$$|S_1| \ge q - (m-1)(m^2 - 2m - 1)\sqrt{q}$$

Let $A_1 = (m-1)(m^2 - 2m - 1)$,$B_1 = m^2 - m$, and $E_1 = \lceil \frac{A_1 + \sqrt{A_1^2 + 4B_1}}{2} \rceil$. From the above we see there will be at least one value of a satisfying condition C1 if $q - A_1 \cdot \sqrt{q} > B_1$ or equivalently, if $(\sqrt{q})^2 - A_1 \cdot (\sqrt{q}) - B_1 > 0$. Solving for the bigger root of this quadratic in $\sqrt{q}$, we see that condition C1 holds if $q \ge E_1^2$. Thus this gives the following result.

Lemma 2.5 *Let $q = mt + 1$ be a prime power. If $q \geq E_1^2$, then there is an element $a \in GF(q) \setminus \{0\}$ satisfying condition C1.*

Next, we will find a bound on q such that there is an element $b \in GF(q) \setminus \{0\}$ satisfying condition (ii) stated in Lemma 2.3, where a satisfying condition C1.

For $a \in F^*$, let $r_i(x) = \xi^{-i}(a^i + x), 0 \leq i \leq m-1$. Then condition (ii) stated in Lemma 2.3 can be derived if there is an element $b \neq 0$ satisfying the following condition:

(C2) $r_i(b) \in H_0, 0 \leq i \leq m-1$.

Let $F_i = \chi(r_i(b)), 0 \leq i \leq m-1$

$$G_i = 1 + F_i + \cdots + F_i^{m-1}, 0 \leq i \leq m-1$$

Then

$$G_i = \begin{cases} m, & \text{if } r_i(b) \in H_0 \\ 1, & \text{if } r_i(b) = 0 \\ 0, & \text{if } r_i(b) \notin H_0 \cup \{0\} \end{cases}$$

From these, form the sum

$$S_2 = \sum_{x \in GF(q)} \prod_{i=0}^{m-1} (1 + F_i + \cdots + F_i^{m-1}) \tag{3}$$

This sum is equal to $n_2 m^m + d_2$ where n_2 is the number of elements b in $GF(q)$, satisfying the condition C2, and d_2 is the contribution when one of $r_i(b)$ is 0, $0 \leq i \leq m-1$. For each $i, 0 \leq i \leq m-1$, if $r_i(b) = 0$ then the contribution to S_2 at $x = b$ is at most m^{m-1}. There are at most m values of b in GF(q) for which $r_i(b) = 0$ for any i; hence there is a 2nd value of b (in addition to $b = 0$) satisfying the condition C2 if we can show that $|S_2| > m^m + m^m = 2m^m$.

Expanding S_2, we obtain

$$\begin{aligned} S_2 = \sum_{b \in GF(q)} 1 + \sum_{i=0}^{m-1} \sum_{k=1}^{m-1} \sum_{b \in GF(q)} F_i^k + \sum_{0 \leq i_1 < i_2 \leq m-1} \sum_{1 \leq k_1, k_2 \leq m-1} \sum_{b \in GF(q)} F_{i_1}^{k_1} F_{i_2}^{k_2} \\ + \cdots + \sum_{0 \leq i_1 < i_2 < \cdots < i_u \leq m-1} \sum_{1 \leq k_1, k_2, \ldots, k_u \leq m-1} \sum_{b \in GF(q)} F_{i_1}^{k_1} F_{i_2}^{k_2} \cdots F_{i_u}^{k_u} \\ + \cdots + \sum_{1 \leq k_1, k_2, \ldots, k_{m-1} \leq m-1} \sum_{b \in GF(q)} F_0^{k_1} F_1^{k_2} \cdots F_{m-1}^{k_{m-1}} \end{aligned} \tag{4}$$

It is clear that $r_0(x), r_1(x), \ldots, r_{m-2}(x)$ are pairwise coprime. Suppose that

$$K(b) = r_0(b)^{\beta_0} r_1(b)^{\beta_1} \cdots r_{m-2}(b)^{\beta_{m-1}}$$

with positive degree, we can show that if $\beta_j \le m-1, 0 \le j \le m-2$, then $K(b)$ is not an mth power of a polynomial in $GF(q)[x]$. In fact, if $K(b) = p(b)^m$, since $r_0(x), r_1(x), \ldots, r_{m-1}(x)$ are pairwise coprime, then $\beta_0 \equiv \beta_1 \equiv \cdots \equiv \beta_{m-1} \equiv 0 \pmod m$ and $\beta_j \le m-1, 0 \le j \le m-1$, we have $\beta_0 = \beta_1 = \cdots = \beta_{m-1} = 0$, a contradiction. Note that each of the inner product in (4) can be represented as $\psi(cr(b))$ for some c, where $r(x)$ is a monic polynomial. It is easy to see that $deg(r_i(x)) = 1, 0 \le i \le m-1$. So, from Theorem 2.4, we have

$$\left|\sum_{i=0}^{m-1}\sum_{k=1}^{m-1}\sum_{b\in GF(q)} F_i^k\right| \le \binom{m}{1}(m-1)(1-1)\sqrt{q}$$

$$\left|\sum_{0\le i_1<i_2\le m-1}\ \sum_{1\le k_1,k_2\le m-1}\ \sum_{b\in GF(q)} F_{i_1}^{k_1}F_{i_2}^{k_2}\right| \le \binom{m}{2}(m-1)^2(2-1)\sqrt{q}$$

.....

$$\left|\sum_{0\le i_1<i_2<\cdots<i_u\le m-1}\ \sum_{1\le k_1,k_2,\ldots,k_u\le m-1}\ \sum_{b\in GF(q)} F_{i_1}^{k_1}F_{i_2}^{k_2}\cdots F_{i_u}^{k_u}\right| \le \binom{m}{u}(m-1)^u(u-1)\sqrt{q}$$

.....

$$\left|\sum_{1\le k_1,k_2,\ldots,k_{m-1}\le m-1}\ \sum_{b\in GF(q)} F_0^{k_1}F_1^{k_2}\cdots F_{m-1}^{k_{m-1}}\right| \le (m-1)^{m-1}(m-1)\sqrt{q}.$$

Then we have

$$|S_2| \ge q - [\sum_{u=2}^{m}\binom{m}{u}(m-1)^u(u-1)]\sqrt{q}.$$

Let $A_2 = \sum_{u=2}^{m}(u-1)\binom{m}{u}(m-1)^u$, $B_2 = 2m^m$, $E_2 = \lceil\frac{A_2+\sqrt{A_2^2+4B_2}}{2}\rceil$. From the above we see there will be at least one value of $b \ne 0$ satisfying condition C2 if $q - A_2\cdot\sqrt{q} > B_2$ or equivalently, if $(\sqrt{q})^2 - A_2\cdot(\sqrt{q}) - B_2 > 0$. Solving for the bigger root of this quadratic in $\sqrt{q}$, we see that condition C2 holds if $q \ge E_2^2$. Thus this gives the following result.

Lemma 2.6 *Let $q = mt+1$ be a prime power. If $q \ge E_2^2$, then there is an element $b \in GF(q)\setminus\{0\}$ satisfying condition C2.*

In Lemmas 2.5 and 2.6, $E_2 > E_1$ for all positive m. Hence from Lemmas 2.3, 2.5 and 2.6 we obtain our first main result.

Theorem 2.7 *Let $q = mt + 1$ be a prime power. If $q \geq E_2^2$, then there exists a $(m, 2)$-cycle frame of type 1^q, and hence there exists a DNR$(q, m, 2)$-CS.*

Corollary 2.8 *Let $q = mt + 1$ be a prime power and $\lambda \equiv 0 \pmod 2$. Then there exists a DNR(q, m, λ)-CS for $q \geq E_2^2$.*

3 DNR$(q, 4, 2)$-CS for prime power $q \equiv 1 \pmod 4$

In this section, we investigate the existence of DNR$(q, 4, 2)$-CSs for prime power $q \equiv 1 \pmod 4$. Applying Theorem 2.7 with $m = 4$, the following result is obtained.

Lemma 3.1 *Let $q \equiv 1 \pmod 4$ be a prime power and $q \geq 264221$. Then there exists a $(4, 2)$-cycle frame of type 1^q, and hence there exists a DNR$(q, 4, 2)$-CS.*

By Lemma 3.1, we need only to handle with the remaining prime powers $q < 264221$. We first apply Theorem 2.2 to treat the primes.

Lemma 3.2 *Let $p \equiv 1 \pmod 4$ be a prime and $13 \leq p < 264221$. Then there exists a $(4, 2)$-cycle frame of type 1^p, and hence there is a DNR$(p, 4, 2)$-CS.*

Proof: With the aid of computer search, we give a list of the information we need to apply Theorem 2.2 for prime $p \equiv 1 \pmod 4$ and $13 \leq p \leq 1009$ in Table 1 of the Appendix. In order to save space, we omit the information for other values of p. The interested reader may contact the authors to have a copy. □

We still apply Theorem 2.2 to treat the prime power $q = p^2$, where $p \equiv 3 \pmod 4$.

Lemma 3.3 *Let prime $p \equiv 3 \pmod 4$ and $7 \leq p \leq 503$. Then there exists a $(4, 2)$-cycle frame of type 1^{p^2}, and hence there exists a DNR$(p^2, 4, 2)$-CS.*

Proof: We list the information we need to apply Theorem 2.2 for prime $p \equiv 3 \pmod 4$ and $7 \leq p \leq 503$ in Table 2 of the Appendix. □

To treat the remaining prime power cases, we need the following working lemma.

Lemma 3.4 *Let q be a prime power and s, t positive integers. If there exist $(m, 2)$-cycle frames of type 1^{q^s} and 1^{q^t}, then there exists a $(m, 2)$-cycle frame of type $1^{q^{(s+t)}}$, and hence there exists a DNR$(q^{(s+t)}, m, 2)$-CS.*

Proof: Without loss of generality, it can be assumed that $s \leq t$. Then there exists a transversal design TD(q^s, q^t) (which is equivalent to $q^s - 2$ mutually orthogonal latin square of order q^t)(see, e.g.,[2]). Replacing each block B of the TD by a $(m, 2)$-cycle frame of type 1^{q^s} over B gives a $(m, 2)$-cycle frame of type $(q^t)^{q^s}$. Further filling in holes of the resultant frame with a $(m, 2)$-cycle frame of type 1^{q^t} gives a $(m, 2)$-cycle frame of type $1^{q^{s+t}}$. This completes the proof. □

Lemma 3.5 *Let s be an even integer ≥ 4. Then there exists a $(4,2)$-cycle frame of type 1^{3^s}, and hence there exists a DNR$(3^s,4,2)$-CS.*

Proof: For $q = 3^4, 3^6$, applying Theorem 2.2 gives the desired designs, where the required information is listed below.

q	ξ satisfies	M	ξ^n
3^4	$\xi^4+\xi^3+2=0$	$(\xi^0,\xi^1,\xi^{38},\xi^{35})$	ξ^0
3^6	$\xi^6+\xi^5+2=0$	$(\xi^0,\xi^1,\xi^2,\xi^{15})$	ξ^{24}

For $q = 3^s, s \geq 4$, we can write $s = 4k+6l, k, l \geq 0$. By Lemma 3.4 and induction on k, l, we get $(4,2)$-cycle frames of type $1^{3^{4k}}$ and $1^{3^{6l}}$. Applying Lemma 3.4 again gives a $(4,2)$-cycle frame of type 1^{3^s}. □

Lemma 3.6 *Let $s \geq 2$. then there exists a $(4,2)$-cycle frame of type 1^{5^s}, and hence there exists a DNR$(5^s,4,2)$-CS.*

Proof: For $q = 5^2, 5^3$, applying Theorem 2.2 gives the desired designs, where the required information is listed below.

q	ξ satisfies	M	ξ^n
5^2	$\xi^2+\xi+2=0$	$(\xi^0,\xi^1,\xi^{10},\xi^{23})$	ξ^{12}
5^3	$\xi^3+\xi^2+2=0$	$(\xi^0,\xi^{17},\xi^2,\xi^{63})$	ξ^0

For $q = 5^s, s \geq 2$, we can write $s = 2k+3l, k, l \geq 0$. By Lemma 3.4 and induction on k, l, we get $(4,2)$-cycle frames of type $1^{5^{2k}}$ and $1^{5^{3l}}$. Applying Lemma 3.4 again gives a $(4,2)$-cycle frame of type 1^{5^s}. □

Lemma 3.7 *Let $q \equiv 1 \pmod 4$ be a prime power and $13 \leq q < 264221$. Then there exists a $(4,2)$-cycle frame of type 1^q, and hence there exists a DNR$(q,4,2)$-CS.*

Proof: For $q = p^s$, $p \equiv 1 \pmod 4$ and $s \geq 1$, the desired designs follow from Lemmas 3.6, 3.2 and 3.4. For $q = p^s$, $p \equiv 3 \pmod 4$ and $s \geq 2$, the desired designs follow from Lemmas 3.5, 3.3 and 3.4. □

Combing Lemmas 3.1 and 3.7, we obtain our second main result.

Theorem 3.8 *Let $q \equiv 1 \pmod 4$ be a prime power and $q \geq 13$. Then there exists a $(4,2)$-cycle frame of type 1^q, and hence there exists a DNR$(q,4,2)$-CS.*

Corollary 3.9 *Let $q \equiv 1 \pmod 4$ be a prime power and $q \geq 13$. Then there exists a DNR$(q,4,\lambda)$-CS for any positive even λ.*

Acknowledgements

The author is grateful to the referees for their constructive comments and suggestions. The research is partially supported by NSFC under Grant No. 10771193, NSF of Universities of Jiangsu Province under Grant No. 07KJB110090, the Starter Foundation for the Doctors of Nantong University under Grant No. 07B12, and the Program for the Innovation Talents of Nantong University.

References

[1] J. Abel, E.R. Lamken and J. Wang, A few more Kirkman squares and doubly near resolvable BIBDs for block size 3, *Discrete Math.* **308** (2008), 1102–1123.

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

[3] C.J. Colbourn, K.E. Manson, and W.D. Wallis, Frames for twofold triple systems, *Ars Combin.* **17** (1984), 65–74.

[4] C.J. Colbourn and S.A. Vanstone, Doubly resolvable twofold triple systems, Proc. Eleventh Manitoba Conf. Numer. Math. Computing, *Congr. Numer.* **34** (1982), 219–223.

[5] J.H. Dinitz, *Room Squares*, in: The CRC Handbook of Combinatorial Designs (C.J. Colbourn, J.H. Dinitz, eds.), CRC Press, Boca Raton, FL (1996), 437–442.

[6] J.H. Dinitz and D.R. Stinson, Room squares and related designs, in: *Contemporary Design Theory: A collection of surveys*, Wiley, New York (1992) 137–204.

[7] E.R. Lamken, 3-complementary frames and doubly near resolvable $(v, 3, 2)$-BIBDs, *Discrete Math.* **88** (1991), 59–78.

[8] E.R. Lamken, The existence of doubly near resolvable $(v, 3, 2)$-BIBDs, *J. Combin. Des.* **2** (1994), 427–440.

[9] E.R. Lamken and S.A. Vanstone, Existence results for doubly near resolvable $(v, 3, 2)$-BIBDs, *Discrete Math.* **120** (1993), 135–148.

[10] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of mathematics and its applications, Vol. 20, Cambridge, UK: Cambridge University Press, (1983).

[11] R.C. Mullin and W.D. Wallis, The existence of Room squares, *Aequationes Math.* **1** (1975), 1–7.

[12] S.A. Vanstone, On mutually orthogonal resolutions and near resolutions, *Ann. Discrete Math.* **15** (1982), 357–369.

Appendix

Table 1

p	ξ	M	ξ^n	p	ξ	M	ξ^n
13	2	$(1,2,4,8)$	10	17	3	$(1,3,15,11)$	5
29	2	$(1,2,4,27)$	12	37	2	$(1,2,4,17)$	17
41	6	$(1,6,29,36)$	25	53	2	$(1,2,4,12)$	8
61	2	$(1,2,4,8)$	10	73	5	$(1,5,25,52)$	1
89	3	$(1,3,9,27)$	81	97	5	$(1,5,25,71)$	53
101	2	$(1,2,4,8)$	8	109	6	$(1,6,36,24)$	4
113	3	$(1,3,9,40)$	9	137	3	$(1,3,9,75)$	2
149	2	$(1,2,4,137)$	146	157	5	$(1,5,25,96)$	45
173	2	$(1,2,4,8)$	9	181	2	$(1,2,4,8)$	4
193	5	$(1,5,25,153)$	90	197	2	$(1,2,4,128)$	4
229	6	$(1,6,36,145)$	1	233	3	$(1,3,9,180)$	68
241	7	$(1,7,49,102)$	199	257	3	$(1,3,9,179)$	23
269	2	$(1,2,4,8)$	8	277	5	$(1,5,25,125)$	4
281	3	$(1,3,9,216)$	98	293	2	$(1,2,4,8)$	145
313	10	$(1,10,100,61)$	10	317	2	$(1,2,4,128)$	64
337	10	$(1,10,100,195)$	199	349	2	$(1,2,4,8)$	176
353	3	$(1,3,9,206)$	81	373	2	$(1,2,4,128)$	16
389	2	$(1,2,4,128)$	2	397	5	$(1,5,25,313)$	30
401	3	$(1,3,9,27)$	119	409	21	$(1,21,32,195)$	223
421	2	$(1,2,4,128)$	8	433	5	$(1,5,25,238)$	17
449	3	$(1,3,9,27)$	27	457	13	$(1,13,169,369)$	209
461	2	$(1,2,4,8)$	1	509	2	$(1,2,4,8)$	64
521	3	$(1,3,9,147)$	9	541	2	$(1,2,4,128)$	16
557	2	$(1,2,4,128)$	4	569	3	$(1,3,9,198)$	81
577	5	$(1,5,25,78)$	378	593	3	$(1,3,9,27)$	136
601	7	$(1,7,49,280)$	441	613	2	$(1,2,4,316)$	128
617	3	$(1,3,9,75)$	243	641	3	$(1,3,9,122)$	3
653	2	$(1,2,4,89)$	178	661	2	$(1,2,4,8)$	260
673	5	$(1,5,25,125)$	357	677	2	$(1,2,4,8)$	544
701	2	$(1,2,4,128)$	64	709	2	$(1,2,4,128)$	4
733	6	$(1,6,36,216)$	80	757	2	$(1,2,4,128)$	407
761	6	$(1,6,36,216)$	166	769	11	$(1,11,121,562)$	1
773	2	$(1,2,4,8)$	32	797	2	$(1,2,4,8)$	364
809	3	$(1,3,9,291)$	729	821	2	$(1,2,4,490)$	258
829	2	$(1,2,4,8)$	4	853	2	$(1,2,4,8)$	1
857	3	$(1,3,9,764)$	9	877	2	$(1,2,4,294)$	64
881	3	$(1,3,9,425)$	729	929	3	$(1,3,9,329)$	3
937	5	$(1,5,25,664)$	470	941	2	$(1,2,4,8)$	1
953	3	$(1,3,9,873)$	729	977	3	$(1,3,9,27)$	9
997	7	$(1,7,49,189)$	224	1009	11	$(1,11,121,902)$	121

Table 2

$q : p^2$	ξ satisfies	M	ξ^n
7^2	$\xi^2+\xi+3=0$	$(\xi^0,\xi^1,\xi^2,\xi^7)$	ξ^{29}
11^2	$\xi^2+\xi+7=0$	$(\xi^0,\xi^1,\xi^2,\xi^{91})$	ξ^3
19^2	$\xi^2+\xi+2=0$	$(\xi^0,\xi^1,\xi^2,\xi^{59})$	ξ^2
23^2	$\xi^2+\xi+7=0$	$(\xi^0,\xi^1,\xi^2,\xi^{71})$	ξ^1
31^2	$\xi^2+\xi+12=0$	$(\xi^0,\xi^1,\xi^2,\xi^{83})$	ξ^{10}
43^2	$\xi^2+\xi+3=0$	$(\xi^0,\xi^1,\xi^2,\xi^{35})$	ξ^0
47^2	$\xi^2+\xi+13=0$	$(\xi^0,\xi^1,\xi^2,\xi^{11})$	ξ^8
59^2	$\xi^2+\xi+2=0$	$(\xi^0,\xi^1,\xi^2,\xi^{31})$	ξ^1
67^2	$\xi^2+\xi+12=0$	$(\xi^0,\xi^1,\xi^2,\xi^{23})$	ξ^0
71^2	$\xi^2+\xi+11=0$	$(\xi^0,\xi^1,\xi^2,\xi^{71})$	ξ^{18}
79^2	$\xi^2+\xi+3=0$	$(\xi^0,\xi^1,\xi^2,\xi^{63})$	ξ^8
83^2	$\xi^2+\xi+2=0$	$(\xi^0,\xi^1,\xi^2,\xi^{91})$	ξ^{14}
103^2	$\xi^2+\xi+5=0$	$(\xi^0,\xi^1,\xi^2,\xi^{11})$	ξ^1
107^2	$\xi^2+\xi+5=0$	$(\xi^0,\xi^1,\xi^2,\xi^7)$	ξ^{10}
127^2	$\xi^2+\xi+3=0$	$(\xi^0,\xi^1,\xi^2,\xi^{63})$	ξ^0
131^2	$\xi^2+\xi+14=0$	$(\xi^0,\xi^1,\xi^2,\xi^{47})$	ξ^1
139^2	$\xi^2+\xi+2=0$	$(\xi^0,\xi^1,\xi^2,\xi^{31})$	ξ^2
151^2	$\xi^2+\xi+12=0$	$(\xi^0,\xi^1,\xi^2,\xi^{11})$	ξ^0
163^2	$\xi^2+\xi+11=0$	$(\xi^0,\xi^1,\xi^2,\xi^7)$	ξ^1
167^2	$\xi^2+\xi+5=0$	$(\xi^0,\xi^1,\xi^2,\xi^{11})$	ξ^2
179^2	$\xi^2+\xi+7=0$	$(\xi^0,\xi^1,\xi^2,\xi^{59})$	ξ^1
191^2	$\xi^2+\xi+19=0$	$(\xi^0,\xi^1,\xi^2,\xi^{67})$	ξ^4
199^2	$\xi^2+\xi+6=0$	$(\xi^0,\xi^1,\xi^2,\xi^{27})$	ξ^{17}
211^2	$\xi^2+\xi+3=0$	$(\xi^0,\xi^1,\xi^2,\xi^7)$	ξ^3
223^2	$\xi^2+\xi+5=0$	$(\xi^0,\xi^1,\xi^2,\xi^{11})$	ξ^0
227^2	$\xi^2+\xi+5=0$	$(\xi^0,\xi^1,\xi^2,\xi^{43})$	ξ^2
239^2	$\xi^2+\xi+13=0$	$(\xi^0,\xi^1,\xi^2,\xi^{11})$	ξ^{14}
251^2	$\xi^2+\xi+19=0$	$(\xi^0,\xi^1,\xi^2,\xi^{11})$	ξ^5
263^2	$\xi^2+\xi+7=0$	$(\xi^0,\xi^1,\xi^2,\xi^{31})$	ξ^5
271^2	$\xi^2+\xi+21=0$	$(\xi^0,\xi^1,\xi^2,\xi^{31})$	ξ^1
283^2	$\xi^2+\xi+3=0$	$(\xi^0,\xi^1,\xi^2,\xi^{15})$	ξ^2
307^2	$\xi^2+\xi+5=0$	$(\xi^0,\xi^1,\xi^2,\xi^{43})$	ξ^{22}
311^2	$\xi^2+\xi+17=0$	$(\xi^0,\xi^1,\xi^2,\xi^{47})$	ξ^2
331^2	$\xi^2+\xi+11=0$	$(\xi^0,\xi^1,\xi^2,\xi^{51})$	ξ^3
347^2	$\xi^2+\xi+7=0$	$(\xi^0,\xi^1,\xi^2,\xi^{123})$	ξ^1
359^2	$\xi^2+\xi+7=0$	$(\xi^0,\xi^1,\xi^2,\xi^{11})$	ξ^1
367^2	$\xi^2+\xi+6=0$	$(\xi^0,\xi^1,\xi^2,\xi^{35})$	ξ^7
379^2	$\xi^2+\xi+10=0$	$(\xi^0,\xi^1,\xi^2,\xi^{19})$	ξ^4
383^2	$\xi^2+\xi+5=0$	$(\xi^0,\xi^1,\xi^2,\xi^{79})$	ξ^{24}
419^2	$\xi^2+\xi+2=0$	$(\xi^0,\xi^1,\xi^2,\xi^{19})$	ξ^1
431^2	$\xi^2+\xi+7=0$	$(\xi^0,\xi^1,\xi^2,\xi^7)$	ξ^5

Table 2 ***(continued)***

$q:p^2$	ξ satisfies	M	ξ^n
439^2	$\xi^2+\xi+23=0$	$(\xi^0,\xi^1,\xi^2,\xi^{27})$	ξ^2
443^2	$\xi^2+\xi+7=0$	$(\xi^0,\xi^1,\xi^2,\xi^7)$	ξ^{22}
463^2	$\xi^2+\xi+11=0$	$(\xi^0,\xi^1,\xi^2,\xi^{35})$	ξ^1
467^2	$\xi^2+\xi+6=0$	$(\xi^0,\xi^1,\xi^2,\xi^{47})$	ξ^{34}
479^2	$\xi^2+\xi+34=0$	$(\xi^0,\xi^1,\xi^2,\xi^{71})$	ξ^8
487^2	$\xi^2+\xi+10=0$	$(\xi^0,\xi^1,\xi^2,\xi^{47})$	ξ^8
491^2	$\xi^2+\xi+8=0$	$(\xi^0,\xi^1,\xi^2,\xi^7)$	ξ^{22}
499^2	$\xi^2+\xi+10=0$	$(\xi^0,\xi^1,\xi^2,\xi^{35})$	ξ^5
503^2	$\xi^2+\xi+19=0$	$(\xi^0,\xi^1,\xi^2,\xi^{143})$	ξ^{18}
383^2	$\xi^2+\xi+5=0$	$(\xi^0,\xi^1,\xi^2,\xi^{79})$	ξ^{24}
419^2	$\xi^2+\xi+2=0$	$(\xi^0,\xi^1,\xi^2,\xi^{19})$	ξ^1
431^2	$\xi^2+\xi+7=0$	$(\xi^0,\xi^1,\xi^2,\xi^7)$	ξ^5
439^2	$\xi^2+\xi+23=0$	$(\xi^0,\xi^1,\xi^2,\xi^{27})$	ξ^2
443^2	$\xi^2+\xi+7=0$	$(\xi^0,\xi^1,\xi^2,\xi^7)$	ξ^{22}
463^2	$\xi^2+\xi+11=0$	$(\xi^0,\xi^1,\xi^2,\xi^{35})$	ξ^1
467^2	$\xi^2+\xi+6=0$	$(\xi^0,\xi^1,\xi^2,\xi^{47})$	ξ^{34}
479^2	$\xi^2+\xi+34=0$	$(\xi^0,\xi^1,\xi^2,\xi^{71})$	ξ^8
487^2	$\xi^2+\xi+10=0$	$(\xi^0,\xi^1,\xi^2,\xi^{47})$	ξ^8
491^2	$\xi^2+\xi+8=0$	$(\xi^0,\xi^1,\xi^2,\xi^7)$	ξ^{22}
499^2	$\xi^2+\xi+10=0$	$(\xi^0,\xi^1,\xi^2,\xi^{35})$	ξ^5
503^2	$\xi^2+\xi+19=0$	$(\xi^0,\xi^1,\xi^2,\xi^{143})$	ξ^{18}

(Received 16 July 2007; revised 16 Dec 2007)