Constructions of Simple Cyclic 2-designs

Shen Hao, Wen Hong
Department of Applied Mathematics
Shanghai Jiao Tong University
Shanghai 200030
People's Republic of China

ABSTRACT. In this paper, constructions of simple cyclic 2-designs are given. As a consequence, we determined the existence of simple $2-(q, k, \lambda)$ designs for every admissible parameter set (q, k, λ) where $q \leq 29$ is an odd prime power, with two undecided parameter sets $(q, k, \lambda) = (29, 8, 6)$ and (29, 8, 10).

1 Introduction

A t-design with parameters v, k and λ , or simply a t- (v, k, λ) design, is a pair (V, B) where V is a v-set and B is a collection of k-subsets (called blocks) of V such that each t-subset of V is contained in exactly λ blocks of V. A t- (v, k, λ) design is called simple if it contains no repeated blocks.

A 2- (v, k, λ) design is also known as a balanced incomplete block design and is denoted $B(k, \lambda; v)$. It can be easily checked that the following conditions are necessary for the existence of a simple 2- (v, k, λ) design:

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

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

$$\lambda \leq \binom{v-2}{k-2} \qquad (1)$$

The parameter set (v, k, λ) is called admissible if it satisfies (1). For given v and k, any λ satisfying (1) is also called admissible.

Since the complement of a simple 2- (v, k, λ) design is a simple 2- $(v, k, \binom{v-2}{k-2} - \lambda)$ design and complementing each block with respect to V yields a 2- $(v, v - k, \lambda(v-2)(v-3)/(k(k-1)))$ design, we need only to consider all the admissible parameter sets (v, k, λ) satisfying $k \le v/2$ and $\lambda \le \binom{v-2}{k-2}/2$.

The existence of simple 2-designs has been studied extensively. But even for $v \leq 30$, there are many admissible parameter sets (v, k, λ) for which the existence of simple 2-designs are still to be determined. The interested reader may refer to [1].

The purpose of this paper is to give new constructions for simple 2-designs and as a consequence, we determined the existence of simple 2- (q, k, λ) designs for every admissible parameter set (q, k, λ) where $q \le 29$ is an odd prime power, with two undecided parameter sets $(q, k, \lambda) = (29, 8, 6)$ and (29, 8, 10).

2 Doubly cyclic 2-designs without repeated blocks

Let v=q be an odd prime power and V=GF(q) be the finite field of order q. For $x\in GF(q)$ and $B=\{a_1,a_2,\ldots,a_k\}$ a k-subset of GF(q), let $B+x=\{a_1+x,\ldots,a_k+x\}$, and let (B) be the set of all the distinct k-subsets of the form B+x, we call (B) an orbit generated by B and say that B is a base block of (B). Let g be a fixed primitive element of GF(q). For $0 \le t \le (q-3)/2$, let $g^t \cdot B = \{g^t \cdot a_1,\ldots,g^t \cdot a_k\}$. Let $\{(B)\}$ be the union of all the distinct orbits of the form $(g^t \cdot B)$, $0 \le t \le (q-3)/2$. $\{(B)\}$ is called the orbit family generated by B. Obviously for any two k-subsets B_1 , and B_2 , we have $(B_1) = (B_2)$ or $(B_1) \cap (B_2) = \phi$ and $\{(B_1)\} = \{(B_2)\}$ or $\{(B_1)\} \cap \{(B_2)\} = \phi$. So all the k-subsets of GF(q) can be partitioned into disjoint orbits and all the k-subsets of GF(q) can be partitioned into disjoint orbit families.

Lemma 1. Let n be the number of orbits contained in $\{(B_1)\}$, then $n \mid (q-1)/2$.

Proof: Since for any $0 \le t_1, t_2 \le (q-3)/2$, we have $g^{t_2} \cdot B = g^{t_2-t_1}g^{t_1} \cdot B$, so any two orbits $(g^{t_1} \cdot B)$ and $(g^{t_2} \cdot B)$ repeat the same times. The conclusion then follows.

Let (GF(q), B) be a 2- (v, k, λ) design. It is called cyclic if $(B) \subset B$ for every $B \in B$. A simple cyclic 2-design (GF(q), B) is called doubly cyclic if $B = \bigcup_{0 \le i \le c} B_i$ such that there exists a $B_i \in B$ for each $0 \le i \le c$, such that $B_c \subset \{(B_c)\}$ and $B_i = \{(B_i)\}$, $0 \le i \le c-1$.

In this paper, we always use λ_0 to denote the smallest value of λ satisfying (1). The following lemma is obvious:

Lemma 2. For any admissible λ , we have $\lambda \equiv 0 \pmod{\lambda_0}$.

Since q is an odd prime power, then k(k-1)/2 is always admissible if v = q. Thus, by Lemma 2, $k(k-1)/2 \equiv 0 \pmod{\lambda_0}$.

Now we use the difference method to give the following construction for doubly cyclic 2-designs. For undefined concepts, the reader may refer to [6].

Theorem 1. For given q and k, let $k(k-1)/2 = e\lambda_0$. If there exist e-1 disjoint doubly cyclic $2-(q, k, \lambda_0)$ designs. Then there exists a simple $2-(q, k, \lambda)$ design for every admissible λ .

Proof: Let $B = \{a_1, a_2, \ldots, a_k\}$ be a k-subset of GF(q). For any $d_1, d_2 \in GF(q) \setminus \{0\}$, there must exist $0 \le t \le (q-3)/2$ such that $d_2 = g^t d_1$, or $d_2 = -g^t d_1$. If $d_1 = a_i - a_j$, then $d_2 = g^t (a_i - a_j)$ or $d_2 = g^t (a_j - a_i)$. Thus, if we let B be the collection of (q-1)/2 orbits $(g^t \cdot B)$, $0 \le t \le (q-3)/2$, then (GF(q), B) is a cyclic $2 \cdot (q, k, k(k-1)/2)$ design, but it is not necessarily simple. By the proof of Lemma 1, if some orbit appears m times in B, then each orbit appears m times in B. Let B_0 be the set of all distinct blocks of B, then $(GF(q), B_0)$ is a doubly cyclic $2 \cdot (q, k, \lambda)$ design for some $\lambda | (k(k-1)/2)$. Since all the k-subsets of GF(q) can be partitioned into disjoint orbit families and each orbit family is the block set of some doubly cyclic $2 \cdot (q, k, s, \lambda_0)$ design with $1 \le s \le e$. Let $B_1, B_2, \ldots, B_{e-1}$ be the e-1 disjoint cyclic $2 \cdot (q, k, \lambda_0)$ design. Obviously if an orbit family contains all the orbits of one or more disjoint doubly cyclic 2-designs, the remaining orbits also form the block set of some doubly cyclic 2-design.

Now for an admissible λ , we always have $\lambda \equiv 0 \pmod{\lambda_0}$ by Lemma 2. If $\lambda \leq \binom{q-2}{k-2} - k(k-1)/2$, we choose approprietely some of the disjoint doubly cyclic 2-designs which are disjoint with B_i for $1 \leq i \leq e-1$, to form a simple cyclic 2- (q, k, λ') design, denoted $(GF(q), B_0)$, such that $\lambda - \lambda' = s\lambda_0$ where $1 \leq s \leq e-1$. Let $B = \bigcup_{i=0}^s B_i$, then (GF(q), B) is a simple cyclic 2- (q, k, λ) design. If $\lambda > \binom{q-2}{k-2} - k(k-1)/2$, let $\lambda = \binom{q-2}{k-2} - s\lambda_0$, $1 \leq s \leq e-1$. Let B be the set of k-subsets obtained by taking out all the blocks of B_1, B_2, \ldots, B_s from the set of all k-subsets of GF(q), then (GF(q), B) is a simple cyclic 2- (q, k, λ) design. This completes the proof.

As a direct consequence, we have the following corollary:

Corollary. If $\lambda_0 = k(k-1)/2$, then there exists a simple cyclic 2- (q, k, λ) design for each admissible λ .

Similar to Theorem 1, we can prove the following theorem:

Theorem 2. For given q and k, let $k(k-1)/2 = e \lambda_0$, $2^{c-1} < e \le 2^c$. If there exists a doubly cyclic 2- $(q, k, 2^i \lambda_0)$ design for $0 \le i \le c-1$ such that these c 2-designs are disjoint, then there exists a simple cyclic 2- (q, k, λ) design for each admissible λ .

3 Existence of simple cyclic 2-designs of small orders

As an application of the theorems proved in the previous section, we give constructions of a series of simple 2-designs whose existence are previously unknown.

Theorem 3. There exists a simple cyclic $2 - (q, k, \lambda)$ design for each admissible parameter set (q, k, λ) if (q, k) = (25, 11), (27, 4), (27, 5), (27, 7), (27, 8), (27, 10), (27, 11), (29, 6), (29, 10), and (29, 11).

Proof: It can be checked that in each case, we have $\lambda_0 = k(k-1)/2$. The conclusion then follows from the corollary of Theorem 1.

Theorem 4. There exists a simple cyclic 2- (q, k, λ) design for each admissible parameter set (q, k, λ) if (q, k) = (29, 9), (29, 12), and (29, 13).

Proof: In each case, we have $\lambda_0 = k(k-1)/4$. By Theorem 1, we prove the theorem by constructing a doubly cyclic 2-(29, 9, 18) design and a doubly cyclic 2-(29, 12, 33) design as follows:

A doubly cyclic 2-(29, 9, 18) design:

A doubly cyclic 2-(29, 12, 33) design:

For (q, k) = (29, 13), since $\binom{27}{11} \equiv 39 \pmod{78}$, then there must exist a doubly cyclic 2-(29, 13, 39) design. The conclusion then follows.

Theorem 5. If k = 6 or 7 then there exists a simple cyclic 2-(25, k, λ) design for each admissible parameter set.

Proof: In these cases, we have $\lambda_0 = k(k-1)/6$, by Theorem 2, we need only to construct a doubly cyclic 2-(25, k, k(k-1)/6) design and a doubly cyclic 2-(25, k, k(k-1)/3) design. Let g be a primitive element of GF(25)

with $g^2 + 4g + 2 = 0$. Base blocks:

$$\begin{split} (k,\lambda) &= (6,5) \colon \\ &\{1,g^4,g^8,g^{12},g^{16},g^{20}\}, \quad \{g,g^5,g^9,g^{13},g^{17},g^{21}\}, \\ &\{g^2,g^6,g^{10},g^{14},g^{18},g^{22}\}, \quad \{g^3,g^7,g^{11},g^{15},g^{19},g^{23}\}. \end{split}$$

$$(k,\lambda) &= (6,10) \colon \\ &\{1,g,g^8,g^9,g^{16},g^{17}\}, \qquad \{g,g^2,g^9,g^{10},g^{17},g^{18}\}, \\ &\{g^2,g^3,g^{10},g^{11},g^{18},g^{19}\}, \quad \{g^3,g^4,g^{11},g^{12},g^{19},g^{20}\}, \\ &\{g^4,g^5,g^{12},g^{13},g^{20},g^{21}\}, \quad \{g^5,g^6,g^{13},g^{14},g^{21},g^{22}\}, \\ &\{g^6,g^7,g^{14},g^{15},g^{22},g^{23}\}, \quad \{g^7,g^8,g^{15},g^{16},g^{23},1\}. \end{split}$$

$$\begin{aligned} (k,\lambda) &= (7,7) \colon \\ \{0,1,g^4,g^8,g^{12},g^{16},g^{20}\}, & \{0,g,g^5,g^9,g^{13},g^{17},g^{21}\}, \\ \{0,g^2,g^6,g^{10},g^{14},g^{18},g^{22}\}, & \{0,g^3,g^7,g^{11},g^{15},g^{19},g^{23}\}. \end{aligned}$$

$$\begin{aligned} (k,\lambda) &= (7,14) \colon \\ &\{0,1,g,g^8,g^9,g^{16},g^{17}\}, & \{0,g,g^2,g^9,g^{10},g^{17},g^{18}\}, \\ &\{0,g^2,g^3,g^{10},g^{11},g^{18},g^{19}\}, & \{0,g^3,g^4,g^{11},g^{12},g^{19},g^{20}\}. \\ &\{0,g^4,g^5,g^{12},g^{13},g^{20},g^{21}\}, & \{0,g^5,g^6,g^{13},g^{14},g^{21},g^{22}\}. \\ &\{0,g^6,g^7,g^{14},g^{15},g^{22},g^{23}\}, & \{0,g^7,g^8,g^{15},g^{16},g^{23},1\}. \end{aligned}$$

This completes the proof.

Theorem 6. There exists a simple cyclic 2-(25, 8, λ) design for each admissible λ .

Proof: In this case, $\lambda_0 = 7$, by Theorem 2, we need only to construct a doubly cyclic 2-(25, 8, 7) design, a doubly cyclic 2-(25, 8, 14) design and a doubly cyclic 2-(25, 8, 21) design. Let g be a primitive element of GF(25) with $g^2 + 4g + 2 = 0$. Base blocks:

A doubly cyclic 2-(25, 8, 7) design:

$$\begin{split} &\{1, g^3, g^6, g^9, g^{12}, g^{15}, g^{18}, g^{21}\}, \\ &\{g, g^4, g^7, g^{10}, g^{13}, g^{16}, g^{19}, g^{22}\}, \\ &\{g^2, g^5, g^8, g^{11}, g^{14}, g^{17}, g^{20}, g^{23}\}. \end{split}$$

A doubly cyclic 2-(25, 8, 14) design:

$$\begin{aligned} &\{1,g,g^6,g^7,g^{12},g^{13},g^{18},g^{19}\},\\ &\{g,g^2,g^7,g^8,g^{13},g^{14},g^{19},g^{20}\},\\ &\{g^2,g^3,g^8,g^9,g^{14},g^{15},g^{20},g^{21}\}\\ &\{g^3,g^4,g^9,g^{10},g^{15},g^{16},g^{21},g^{22}\},\\ &\{g^4,g^5,g^{10},g^{11},g^{16},g^{17},g^{22},g^{23}\},\\ &\{g^5,g^6,g^{11},g^{12},g^{17},g^{18},g^{23},1\}. \end{aligned}$$

Since the blocks of the doubly cyclic 2-(25, 8, 7) design and the blocks of the doubly cyclic 2-(25, 8, 14) design are disjoint, then we obtain a doubly cyclic 2-(25, 8, 21) design. This completes the proof.

Theorem 7. There exists a simple cyclic 2-(25, 12, λ) design for each admissible λ .

Proof: In this case, we have $\lambda_0 = 11$, by Theorem 2, we need only to construct a doubly cyclic 2-(25, 12, 11) design, a doubly cyclic 2-(25, 12, 22) design, a doubly cyclic 2-(25, 12, 33) design, a doubly cyclic 2-(25, 12, 44) design, and a doubly cyclic 2-(25, 12, 55) design. Let g be a primitive element of GF(25) with $g^2 + 4g + 2 = 0$. Base blocks:

A doubly cyclic 2-(25, 12, 11) design:

$$\{1, g^2, g^4, g^6, g^8, g^{10}, g^{12}, g^{14}, g^{16}, g^{18}, g^{20}, g^{22}\}, \\ \{g, g^3, g^5, g^7, g^9, g^{11}, g^{13}, g^{15}, g^{17}, g^{19}, g^{21}, g^{23}\}.$$

A doubly cyclic 2-(25, 12, 22) design:

$$\begin{aligned} &\{1,g,g^4,g^5,g^8,g^9,g^{12},g^{13},g^{16},g^{17},g^{20},g^{21}\},\\ &\{g,g^2,g^5,g^6,g^9,g^{10},g^{13},g^{14},g^{17},g^{18},g^{21},g^{22}\},\\ &\{g^2,g^3,g^6,g^7,g^{10},g^{11},g^{14},g^{15},g^{18},g^{19},g^{22},g^{23}\},\\ &\{g^3,g^4,g^7,g^8,g^{11},g^{12},g^{15},g^{16},g^{19},g^{20},g^{23},1\}. \end{aligned}$$

A doubly cyclic 2-(25, 12, 44) design:

$$\{1,g,g^2,g^3,g^8,g^9,g^{10},g^{11},g^{16},g^{17},g^{18},g^{19}\},\\ \{g,g^2,g^3,g^4,g^9,g^{10},g^{11},g^{12},g^{17},g^{18},g^{19},g^{20}\},\\ \{g^2,g^3,g^4,g^5,g^{10},g^{11},g^{12},g^{13},g^{18},g^{19},g^{20},g^{21}\},\\ \{g^3,g^4,g^5,g^6,g^{11},g^{12},g^{13},g^{14},g^{19},g^{20},g^{21},g^{22}\},\\ \{g^4,g^5,g^6,g^7,g^{12},g^{13},g^{14},g^{15},g^{20},g^{21},g^{22},g^{23}\},\\ \{g^5,g^6,g^7,g^8,g^{13},g^{14},g^{15},g^{16},g^{21},g^{22},g^{23},1\},\\ \{g^6,g^7,g^8,g^9,g^{14},g^{15},g^{16},g^{17},g^{22},g^{23},1,g\},\\ \{g^7,g^8,g^9,g^{10},g^{15},g^{16},g^{17},g^{18},g^{23},1,g,g^2\}.$$

Since the block sets of the doubly cyclic 2-(25, 12, 11) design, the doubly cyclic 2-(25, 12, 22) design, and the doubly cyclic 2-(25, 12, 44) design are disjoint, then we obtain a doubly cyclic 2-(25, 12, 33) design, and a doubly cyclic 2-(25, 12, 55) design. This completes the proof.

Theorem 8. There exists a simple cyclic 2-(25, 4, λ) design for each admissible λ . There exists a simple cyclic 2-(25, 5, λ) design for each admissible λ .

Proof: Let g be a primitive element of GF(25) with $g^2 = 2g + 2$. For k = 4, let $\{0, g^i, g^{8+i}, g^{9+i}\}$ and $\{0, g^{6+i}, g^{14+i}, g^{15+i}\}$ be the base blocks of B_i , $0 \le i \le 5$, then $(GF(25), B_i)$, i = 0, 1, 2, 3, 4, 5 are 6 disjoint doubly cyclic 2-(25, 4, 1) designs. Thus, by Theorem 1, there exists a simple cyclic 2-(25, 4, λ) design for each admissible λ . For k = 5, let $g^{6i+t} \cdot \{0, 1, 2, 3, 4\}$, t = 0, 1, 2, 3, 4, 5, be the base blocks of B_i , i = 0, 1, where each orbit contains 5 disjoint blocks. Then $(GF(25), B_0)$ and $(GF(25), B_1)$ are two disjoint doubly cyclic 2-(25, 5, 1) designs. Since $\binom{23}{3} \equiv 9+2 \pmod{10}$, then there must be 9 more disjoint doubly cyclic 2-(25, 5, 1) designs or 4 disjoint doubly cyclic 2-(25, 5, 1) designs and a doubly cyclic 2-(25, 5, 5) design. The conclusion then follows from Theorem 1 or Theorem 2.

4 Existence of simple 2-designs of small orders

To prove our main theorem, the following lemma is also needed:

Lemma 3 [2]. If (V, B) is a simple t- (v, k, λ) design and D is a given set of k-subsets of V such that:

$$v! > |B| \cdot |D| \cdot k!(v-k)! \tag{2}$$

then there exists a simple t- (v, k, λ) design which is disjoint from D.

Theorem 9. For given k and v = q, where q is an odd prime power, let λ_0 be the smallest λ satisfying (1) and $k(k-1)/2 = e\lambda_0$. If there exists a simple $2 - (q, k, \lambda_0)$ design such that

$$2(q-2)! \ge \lambda_0 \cdot q(q-1)(k-2)!(q-k)! \tag{3}$$

and

$$q(q-1)k(k-1) < 2 \cdot \binom{q-2}{k-2} \tag{4}$$

then there exists a simple $2-(q, k, \lambda)$ design for every admissible λ .

Proof: Let $(GF(q), A_1)$ be a simple $2-(q, k, \lambda_0)$ design. For the first step, we let $B = D = A_1$, since we always have $\lambda_0 \le k(k-1)/2$ and each $2-(q,k,\lambda_0)$ design contains $\lambda_0 q(q-1)/k(k-1)$ blocks, then by (3), the condition (2) is satisfied. Thus, by Lemma 3, there exists a simple 2- (q, k, λ_0) design $(GF(q), A_2)$ such that $A_1 \cap A_2 = \phi$. Then we let $B = A_1$ and $D = A_1 \cup A_2$, and so on. In this way we can obtain $e = k(k-1)/(2\lambda_0)$ disjoint simple $2-(q, k, \lambda_0)$ designs. The number of blocks contained in these e 2- (q, k, λ_0) designs is q(q-1)/2. So there are at most q(q-1)/2 doubly cyclic 2-designs with $\lambda \leq k(k-1)/2$, each containing blocks from the above q(q-1)/2 blocks. So, if $\lambda \leq {q-2 \choose k-2}/2$, we can choose those doubly cyclic 2-designs which are disjoint from the e simple $2-(q, k, \lambda_0)$ designs, such that they form a simple $2-(q, k, \lambda')$ design with $\lambda = \lambda' + t\lambda_0$, $0 \le t \le e$. Combining the block set of this $2-(q, k, \lambda')$ design with the block sets of t of the e simple $2-(q, k, \lambda_0)$ designs gives a simple $2-(q, k, \lambda)$ design. This completes the proof.

By Theorem 9, we have the following result:

Theorem 10. If (q, k) = (23, 11), (25, 9), (27, 6), (27, 9), (27, 12), (27, 13), (29, 7), (29, 14), then there exists a simple 2- (q, k, λ) design for each admissible λ .

Proof: In each case, the existence of a simple $2-(q, k, \lambda_0)$ design has already been proved (see [1]). It is an easy calculation to show that the conditions (3) and (4) are satisfied. So the conclusion follows.

There does not exist a simple 2-(25, 10, 3) design by Fisher's condition. The nonexistence of a simple 2-(29, 8, 2) design was proved in [4]. But we have the following result:

Theorem 11. There exists a simple 2- $(25, 10, \lambda)$ design for each admissible $\lambda \geq 6$. There exists a simple 2- $(29, 8, \lambda)$ design for each admissible $\lambda \geq 4$ with two possible exceptions $\lambda = 6$ and 10.

Proof: If there exists a simple $2-(25, 10, \lambda)$ design, then $\lambda \equiv 0 \pmod{3}$. Since there exists a simple 2-(25, 10, 3s) design for s = 2 or 3, (see [1]), then

similar to Theorem 10, we can prove that there exists a simple 2-(25, 10, 3s) design for each admissible $\lambda = 3s \ge 6$.

For (q, k) = (29, 8), since $\binom{27}{6} \equiv 22 \pmod{28}$ and there does not exist a simple 2-(29, 8, 2) design, then there must exist a doubly cyclic 2-(29, 8, 14) design. The existence of a simple 2-(29, 8, 4) design can be found in [5]. Thus, we can prove similarly that there exists a simple 2-(29, 8, λ) design for each admissible $\lambda \neq 2$, 6 or 10.

Combining Theorems 3 - 8, and Theorems 10 - 11, gives our main theorem:

Theorem 12. For any odd prime power $q \le 29$, there exists a simple 2- (q, k, λ) design for each admissible parameter set (q, k, λ) with the nonexistence of a simple 2-(25, 10, 3) design and a simple 2-(29, 8, 2) design and two undecided cases where $(q, k, \lambda) = (29, 8, 6)$ and (29, 8, 10).

Acknowledgement

The authors would like to express their sincere gratitude to Professor L. Zhu. Thanks are also due to the referee who examined the paper carefully and contributed lots of invaluable remarks.

References

- [1] Yeow Meng Chee, Charles J. Colbourn, and Donald L. Kreher, Simple t-designs with $v \le 30$, Ars Combinatoria29(1990),193-258.
- [2] B. Ganter, J. Pelikan and L. Teirlinck, Small sprawling systems of equicardinal sets, Ars Combinatoria 4(1977), 133-142.
- [3] Marshall Hall, Jr. "Combinatorial Theory, second edition", John Wiley & Sons, 1986.
- [4] S.S. Shrikhande, The impossibility of certain symmetrical balanced incomplete block designs, Ann. Math. Statist. 21(1950), 106-111.
- [5] K. Takeuchi, A table of difference sets generating balanced incomplete block designs, Review of Int. Stat. Inst. 30(1962), 361-366.
- [6] Richard M. Wilson, Cyclotomy and difference families in elementary abelian groups, *Journal of Number Theory* 4(1972), 17–47.