HIROSHIMA MATH. J.
25 (1995), 475–485

Difference families with applications to resolvable designs

Sanpei KAGEYAMA and Ying MIAO

(Received November 10, 1993)
(Revised March 25, 1994)

Abstract. Some block disjoint difference families are constructed in rings with the property that there are k distinct units u_i, $0 \leq i \leq k-1$, such that differences $u_i - u_j$ $(0 \leq i < j \leq k-1)$ are all units. These constructions are utilized to produce a large number of classes of resolvable block designs.

1. Introduction

A *balanced incomplete block design* (or, *design*) $B(k, \lambda; v)$ is a pair $(\mathscr{V}, \mathscr{B})$ where $\mathscr{V}$ is a set of v *points* (called *treatments*), and $\mathscr{B}$ is a collection of subsets (called *blocks*) of $\mathscr{V}$, each of size k, such that every pair of distinct points from $\mathscr{V}$ is contained in exactly λ blocks. Note that λ is called the *index*.

One way of investigating the structure of a design is to look at its "symmetry", which can be formalized as the automorphism group of the design. Let $(\mathscr{V}, \mathscr{B})$ be a design and let $\phi: \mathscr{V} \to \mathscr{V}$ be a bijection. The mapping Φ *induced by* ϕ has domain $\mathscr{B}$ and is defined by $\Phi(B) = \{\phi(x): x \in B\}$. An *automorphism* of the design $(\mathscr{V}, \mathscr{B})$ is a pair of bijections $\phi: \mathscr{V} \to \mathscr{V}$ and $\psi: \mathscr{B} \to \mathscr{B}$ which preserves incidence, that is, $\psi(B) = \Phi(B)$ for all $B \in \mathscr{B}$. The set of all automorphisms of $(\mathscr{V}, \mathscr{B})$ forms a group under composition called the *automorphism group* of the design.

Let G be an additive abelian group and $B = \{b_1, \ldots, b_k\}$ be a subset of G. Define the *development* of B as

$$\text{dev}\, B = \{B + g: g \in G\},$$

where $B + g = \{b_1 + g, \ldots, b_k + g\}$ for $g \in G$.

Let $\mathscr{F} = \{B_1, \ldots, B_t\}$ be a family of subsets of G and define the *development* of $\mathscr{F}$ as

$$\text{dev}\, \mathscr{F} = \bigcup_{i=1}^{t} \text{dev}\, B_i.$$

If dev $\mathscr{F}$ is a $B(k, \lambda; v)$, it is said that $\mathscr{F}$ is a $(k, \lambda; v)$ *difference family*, denoted by $DF(k, \lambda; v)$, and the sets $B_1, \ldots, B_t$ are called *base blocks* (or *initial blocks*). The group G is contained in the automorphism group of dev $\mathscr{F}$.

A type of internal structure stems from the notion of parallel lines in the Euclidean plane. A design $B(k, \lambda; v)$ is said to be *resolvable* if the collection of blocks can be partitioned into *parallel classes* which in turn partition the point set. The design is denoted by $RB(k, \lambda; v)$. An $RB(k, \lambda; v')$ $(\mathscr{V}', \mathscr{B}')$ is called a *subdesign* of an $RB(k, \lambda; v)$ $(\mathscr{V}, \mathscr{B})$ if $\mathscr{V}' \subset \mathscr{V}$ and each of the parallel classes of the former one is a subset of one parallel class of the latter one.

A connection between difference families and resolvable designs is stated in the following theorem. By a ring R we mean a commutative ring with an identity in which the identity does not equal zero. Recall that $U(R)$, the units of R, forms a group under ring multiplication.

THEOREM 1.1 (Miao and Zhu [4]). *Let $\lambda \le k - 1$. Suppose there is a $DF(k, \lambda; v)$ over a ring R such that the base blocks are mutually disjoint. If there are k distinct units u_i, $0 \le i \le k - 1$, such that differences $u_i - u_j$ $(0 \le i < j \le k - 1)$ are all units of R, then there exists an $RB(k, \lambda; kv)$ containing a subdesign $RB(k, \lambda; k)$.*

The block disjoint difference families over the ring with the property required as in Theorem 1.1 will be denoted by $DF^*(k, \lambda; v)$. The present paper will focus on the construction problem of $DF^*(k, \lambda; v)$, and then provide some infinite classes of resolvable designs.

2. Some known $DF^*(k, \lambda; v)$'s

A *difference set* $D(k, \lambda; v)$ is a difference family $DF(k, \lambda; v)$ consisting of a single base block. All difference sets can be regarded as block disjoint difference families. It is obvious that a block disjoint $DF(k, \lambda; q)$ over a field $GF(q)$ is a $DF^*(k, \lambda; q)$. Hence a $D(k, \lambda; q)$ over a field $GF(q)$ is a $DF^*(k, \lambda; q)$. We here mainly concern the construction of the difference families with more than one base blocks.

Ray-Chaudhuri and Wilson [5] constructed a $DF^*(k, 1; q)$ in $GF(q)$ to prove the asymptotical sufficiency for the existence of resolvable designs with index unity. The following generalized form was given by Schellenberg [6] (see also [4]).

THEOREM 2.1. *Let $q = k(k - 1)t + 1$ be a prime power and w be a primitive element of $GF(q)$. Let H be the multiplicative subgroup of order $m = k(k - 1)/2$ of the group $GF(q) - \{0\}$. If $a_1, \dots, a_k$ lie in distinct cosets of H and the $k(k - 1)/2$ differences $a_i - a_j$, $1 \le i < j \le k$, are further in distinct cosets of H, then the t blocks $\{w^{mr} a_1, \dots, w^{mr} a_k\}$, $0 \le r < t$, constitute a $DF^*(k, 1; q)$.*

The following difference families can be found in [4].

THEOREM 2.2 ([4, Lemma 3.3]). *Let* $q = ke + 1$ *be a prime power. Further let* w *be a primitive element and* H *the multiplicative subgroup of order* k *of* $GF(q)$. *Then* $\{A_0, \ldots, A_{e-1}\}$ *gives a* $DF^*(k, k-1; q)$ *with* $A_j = w^j H$ *for* $j = 0, 1, \ldots, e-1$.

THEOREM 2.3 ([4, Lemma 3.4]). *Let* k *be odd and* $q = 2ks + 1$ *a prime power. Further let* w *be a primitive element and* H *the multiplicative subgroup of order* k *of* $GF(q)$. *Then* $\{A_1, \ldots, A_s\}$ *gives a* $DF^*(k, (k-1)/2; q)$ *with* $A_j = w^j H$ *for* $j = 1, 2, \ldots, s$.

In the next section, we shall construct more $DF^*(k, \lambda; v)$'s which will be used to produce new resolvable designs.

3. More $DF^*(k, \lambda; v)$'s

Recursive methods of construction will be presented at first.

By a *list* we mean a collection of elements in which each element occurs non-negative times. We use the notation $(x_1, \ldots, x_s)$. The order is not taken into account in our lists. If X_i, $i = 1, 2, \ldots, t$, are lists, then the notation $\sum_{i=1}^{t} X_i$ is used to denote the concatenation of the lists. In some case it can be determined whether or not an arbitrary collection of blocks $\mathscr{F}$ will be a difference family, by the following procedure: Let B be a subset of G. Then define the *list of differences* from B to be the list $\Delta B = (a - b\colon a, b \in B, a \neq b)$. When $\mathscr{F} = \{B_i\colon i \in I\}$ is a family of subsets of G, we define $\Delta\mathscr{F} = \sum_{i \in I} \Delta B_i$. If $\Delta\mathscr{F}$ contains every non-zero element of G exactly λ times, then dev $\mathscr{F}$ is a $B(k, \lambda; v)$, and thus $\mathscr{F}$ is a $DF(k, \lambda; v)$ if $|\mathrm{dev}\, B_i| = |G|$ for each $i \in I$. Note that we here consider difference families without short orbits.

First, we consider the construction of difference families in $G(q)$, the additive group of $GF(q)$. For convenience, we select and fix, for each prime power q, a primitive element w of the $GF(q)$. When $e\,|\,(q-1)$, we define the *cosets modulo the eth power*, $H_0^e = H^e, H_1^e, \ldots, H_{e-1}^e$, by

$$H_m^e = \{w^t\colon t \equiv m \bmod e\}$$

(cf. Wilson [7]). We read the subscripts modulo e, so that if $a \in H_m^e$ and $b \in H_n^e$, then $a \cdot b \in H_{m+n}^e$. Denote by $\mathscr{H}^e$ the class of cosets $\{H_0^e, \ldots, H_{e-1}^e\}$.

Note that if q is even, then $-1 = 1$ is always an eth power in $GF(q)$. If q is odd, then $-1 \in H^e$ if and only if $2e\,|\,(q-1)$. In fact, $-1 = w^{(q-1)/2}$ is an eth power if and only if $(q-1)/2 \equiv 0 \bmod e$.

It will be convenient to introduce a multiplication of lists as follows:

$$(a^i\colon i \in I) \cdot (b^j\colon j \in J) = (a_i \cdot b_j\colon i \in I, j \in J).$$

THEOREM 3.1. *The existence of a* $DF^*(k, \lambda; q)$ *in* $G(q)$ *implies the existence of a* $DF^*(k, \lambda; q^n)$ *in* $G(q^n)$ *for* $n \geq 1$.

PROOF. Let $\mathscr{B} = \{B_i : i \in I\}$ be a $DF^*(k, \lambda; q)$ in $G(q)$, so that $\Delta\mathscr{B} = \sum_{i\in I} \Delta B_i = \lambda(GF(q) - \{0\})$. Since $GF(q)$ is considered as a subfield of $GF(q^n)$, $GF(q) - \{0\}$ is the group H^e of eth powers in $GF(q^n)$ where $e = (q^n - 1)/(q - 1)$. Now let S be any system of representatives for the cosets $\mathscr{H}^e$ modulo H^e in $GF(q^n)$. Then S is a set of e field elements and $S \cdot H^e = G(q) - \{0\}$. Consider the family $\mathscr{B}^* = \{sB_i : i \in I, s \in S\}$. All of the elements of B_i, $i \in I$, are in H^e, thus the blocks of $\mathscr{B}^*$ are mutually disjoint since distinct elements of S belong to different cosets of $\mathscr{H}^e$. Noting that the list of differences from the set sB_i is $(s) \cdot \Delta B_i$, we have $\Delta\mathscr{B}^* = \sum_{s\in S} \sum_{i\in I} (s) \cdot \Delta B_i = S \cdot \Delta\mathscr{B} = S \cdot \lambda(H^e) = \lambda(G(q^n) - \{0\})$. Hence, $\mathscr{B}^*$ is the required $DF^*(k, \lambda; q^n)$. □

PROPOSITION 3.1. *There exists a* $DF^*(6, 1; 121^n)$ *for* $n \geq 1$.

PROOF. The four base blocks, $\{(0, 0), (0, 4), (0, 3), (1, 1), (1, 7), (4, 6)\}$, $\{(0, 5), (0, 7), (2, 10), (4, 1), (8, 5), (6, 9)\}$, $\{(0, 8), (1, 2), (2, 8), (4, 9), (7, 10), (6, 8)\}$, $\{(0, 6), (1, 6), (4, 3), (9, 0), (3, 4), (6, 7)\}$, form a $DF^*(6, 1; 121)$ in $G(121) = Z_{11} \oplus Z_{11}$. By Theorem 3.1, there exists a $DF^*(6, 1; 121^n)$ for $n \geq 1$. □

THEOREM 3.2. *There exists a* $DF^*((q - 1)/2, (q - 3)/2; q^n)$ *for an odd prime power* q *and a positive integer* n.

PROOF. Let $A = \{x^2 : x \in GF(q) - \{0\}\}$ and $B = GF(q) - \{0\} - A$. Then $S = \{A, B\}$ is a $DF^*((q - 1)/2, (q - 3)/2; q)$, which, by Theorem 3.1, implies the existence of a $DF^*((q - 1)/2, (q - 3)/2; q^n)$ for $n \geq 1$. □

Given a list T of elements of $GF(q)$ and a divisor e of $q - 1$, T is said to be *evenly distributed* over the eth power cosets $\mathscr{H}^e$ if and only if T has the same number of entries, counting multiplicities, in each of the cosets $H_0^e, H_1^e, \ldots, H_{e-1}^e$.

THEOREM 3.3. *Let* e *be a divisor of* $q - 1$, $tk \leq e \leq tk(k - 1)$, *and* $B_1, \ldots, B_t$ *be* t k*-subsets of* $GF(q)$ *such that the elements of* B_i, $1 \leq i \leq t$, *are in different cosets of* $H_0^e, \ldots, H_{e-1}^e$, *and* $\sum_{i=1}^{t} \Delta B_i$ *is evenly distributed over* $H_0^e, \ldots, H_{e-1}^e$, *that is,* $\sum_{i=1}^{t} \Delta B_i$ *has* r *entries in each coset* H_x^e. *Then* $re = tk(k - 1)$ *and there exists a* $DF^*(k, r; q^n)$ *in* $GF(q^n)$ *for* $n \geq 1$. *Furthermore, if* $2e \mid (q - 1)$, *then there exists a* $DF^*(k, r/2; q^n)$ *for* $n \geq 1$.

PROOF. With $S' = \{B_i x : i \in \{1, 2, \ldots, t\}, x \in H^e\}$, we can get a $DF^*(k, r; q)$. If $2e \mid (q - 1)$, then $-1 \in H^e$, i.e. $-1 = w^{em}$ with $m = (q - 1)/(2e)$. Then $S = \{B_i w^{ej} : i \in \{1, 2, \ldots, t\}, j \in \{0, 1, \ldots, m - 1\}\}$ is the required $DF^*(k, r/2; q)$. To check this, take $\Delta\mathscr{B} = \{x_i^j : i \in \{0, 1, \ldots, e - 1\}, j \in \{1, 2, \ldots, r/2\}\}$ with $x_i^j \in H_i^e$.

Then $\Delta S = \pm (1, w^e, \ldots, w^{(m-1)}) \cdot (x_i^j: i \in \{0, 1, \ldots, e-1\}, j \in \{1, 2, \ldots, r/2\}) = H^e \cdot (x_i^j: i \in \{0, 1, \ldots, e-1\}, j \in \{1, 2, \ldots, r/2\}) = (r/2) \cdot (GF(q) - \{0\})$. This together with Theorem 3.1 completes the proof. □

COROLLARY 3.1. *If $q \equiv 1 \bmod k(k-1)$ and there exists a set $B = \{b_1, \ldots, b_k\} \subset GF(q)$ with b_i's in different cosets modulo $H^{k(k-1)/2}$ such that $\{b_i - b_j: 1 \le i < j \le k\}$ is a system of representatives for the cosets $\mathscr{H}^{k(k-1)/2}$, then there exists a $DF^*(k, 1; q^n)$ in $G(q^n)$ for $n \ge 1$.*

Now we consider a more general problem of finding blocks $B \subset GF(q)$ whose list of differences is distributed in some given manner. Let P_r be a set of ordered pairs $\{(i, j): 1 \le i < j \le r\}$. Then define a *choice* to be any map $C: P_r \to \mathscr{H}^e$, assigning to each pair $(i, j) \in P_r$ a coset $C(i, j)$ modulo the eth powers in $GF(q)$. An r-tuple $(a_1, \ldots, a_r)$ of elements of $GF(q)$ is said to be *consistent* with the choice C if and only if $a_j - a_i \in C(i, j)$ for all $1 \le i < j \le r$.

In this case, Wilson [7] proved the following.

LEMMA 3.1. *If $q \equiv 1 \bmod e$ is a prime power and $q > e^{r(r-1)}$, then for any choice $C: P_r \to \mathscr{H}^e$, there exists an r-tuple $(a_1, \ldots, a_r)$ of elements of $GF(q)$ consistent with C.*

Using this lemma, the following can be given.

THEOREM 3.4. *Let λ be a factor of $k(k-1)$, and q a prime power.*

(1) *If $k(k-1)/\lambda$ is even, $q \equiv 1 \bmod k(k-1)/(2\lambda)$ and $q > (k(k-1)/(2\lambda))^{k(k+1)}$, then there exists a $DF^*(k, 2\lambda; q^n)$ whenever $\lambda \le (k-1)/2$ and $n \ge 1$. Furthermore, if $q \equiv 1 \bmod k(k-1)/\lambda$, then there exists a $DF^*(k, \lambda; q^n)$ whenever $\lambda \le k-1$ and $n \ge 1$.*

(2) *If $k(k-1)/\lambda$ is odd, $q \equiv 1 \bmod k(k-1)/\lambda$ and $q > (k(k-1)/\lambda)^{k(k+1)}$, then there exists a $DF^*(k, \lambda; q^n)$ whenever $\lambda \le k-1$ and $n \ge 1$.*

PROOF. It is sufficient to consider only the case $n = 1$.

Case (1): $k(k-1)/\lambda$ is even. Let $e = k(k-1)/(2\lambda)$ and let $C: P_{k+1} \to \mathscr{H}^e$ be any choice that maps precisely λ of the $k(k-1)/2$ ordered pairs (i, j), $1 \le i < j \le k$, onto each coset H_m^e modulo the eth powers in $GF(q)$ and the k cosets $C(i, k+1)$, $1 \le i \le k$, are mutually different. Since $q > e^{k(k+1)}$, we can find by Lemma 3.1 a $(k+1)$-tuple $(a_1, \ldots, a_{k+1})$ consistent with the choice C. Let $b_i = a_{k+1} - a_i$, $1 \le i \le k$, then $b_1, \ldots, b_k$ are in different cosets of $\mathscr{H}^e$, and $b_j - b_i = (a_{k+1} - a_j) - (a_{k+1} - a_i) = -(a_j - a_i)$. Hence the block $B = \{b_1, \ldots, b_k\} \subset GF(q)$ is such that precisely 2λ of the differences of ΔB are in each coset $H_0^e, \ldots, H_{e-1}^e$. Then there exists a $DF^*(k, 2\lambda; q)$. Furthermore, if $2e \mid (q-1)$, then there exists a $DF^*(k, \lambda; q)$ in $G(q)$ by Theorem 3.3.

Case (2): $k(k-1)/\lambda$ is odd. Necessarily, λ is even. Now take $e =$

$k(k-1)/\lambda$ and let $C: P_{k+1} \to \mathscr{H}^e$ be any choice of mapping $\lambda/2$ elements of P_k onto each coset of $\mathscr{H}^e$ and the k cosets $C(i, k+1)$, $1 \le i \le k$, are mutually different. Since $q > e^{k(k+1)}$, we can also find a $(k+1)$-tuple $(a_1, \dots, a_{k+1})$ consistent with C. Let again $b_i = a_{k+1} - a_i$, $1 \le i \le k$, we have a block $B = \{b_1, \dots, b_k\}$ such that the elements of B are in different cosets of $\mathscr{H}^e$ and ΔB is evenly distributed over $\mathscr{H}^e$, since $b_j - b_i = -(a_i - a_j)$. Hence the same way as (1) completes the proof. □

Let k be odd, say $k = 2m+1$. A prime power q is said (cf. [7]) to satisfy the *condition* R_k if and only if $q \equiv 1 \bmod k(k-1)$ and for a primitive kth root ξ of unity in $GF(q)$, $\{\xi - 1, \dots, \xi^m - 1\}$ is a system of representatives for the m cosets modulo H^m.

THEOREM 3.5. *If a prime power q satisfies the condition R_k, then there exists a $DF^*(k, 1; q^n)$ for $n \ge 1$.*

PROOF. Assume $q - 1 = tk(k-1) = 2tm(2m+1)$. Let $A = \{1, \xi, \dots, \xi^{k-1}\}$. Then $\xi = w^{2tm}$. Hence

$$\Delta A = \pm A \cdot (\xi - 1, \dots, \xi^m - 1) = H^{tm} \cdot (\xi - 1, \dots, \xi^m - 1).$$

Put $S = \{Aw^{iw}: i = 1, \dots, t\}$. Then the blocks in S are mutually disjoint and $\Delta S = H^m \cdot (\xi - 1, \dots, \xi^m - 1)$, and by the assumption ΔS is the union of all cosets of H^m. By Theorem 3.1, this completes the proof. □

EXAMPLE 3.1. Wilson [7] made a computer search for primes $p \equiv 1 \bmod k(k-1)$ and showed that

$R_7 \supset \{337, 421, 463, 883, 1723, 3067, 3319\}$,
$R_9 \supset \{73, 1153, 1873, 2017\}$,
$R_{15} \supset \{76231\}$.

There is more possibility of using the multiplicative structure of finite fields to ease the task of construction of $DF^*(k, \lambda; q)$'s. For example, we have the following.

THEOREM 3.6. *Let $q = 30t + 1$ be a prime power and ξ be a primitive cube root of unity in $GF(q)$. If there exists an element $c \in GF(q)$ such that $\{\xi - 1, c(\xi - 1), c - 1, c - \xi, c - \xi^2\}$ is a system of representatives for the cosets modulo H^5, then there exists a $DF^*(6, 1; q^n)$ in $G(q^n)$ for $n \ge 1$.*

PROOF. Suppose that there is such an element c and $B = \{1, \xi, \xi^2, c, c\xi, c\xi^2\}$. We have $c \in H_m^5$ for some $m \equiv 0 \bmod 5$ since $\xi - 1$ and $c(\xi - 1)$ are in different cosets of H^5, and $\Delta B = \pm (1, \xi, \xi^2) \cdot (\xi - 1, c(\xi - 1), c - 1, c - \xi, c - \xi^2)$. Now $\pm (1, \xi, \xi^2) = H^{5t}$. Put $S = \{Bw^{5i}: i = 0, 1, \dots, t-1\}$. Then S has t mutually disjoint blocks, and $\Delta S = H^5 \cdot (\xi - 1, c(\xi - 1), c - 1,$

$c - \xi, c - \xi^2)$. Now the assumption shows that S is a $DF^*(6, 1; q)$ which, by Theorem 3.1, completes the proof. □

REMARK. The condition in Theorem 3.6 does not depend on the choice of a primitive cube root. The other primitive cube root of unity is ξ^2. But $\xi - 1$ and $\xi^2 - 1$ are in the same coset modulo H^5 since $\xi^2 - 1 = -\xi^2(\xi - 1)$ and $\xi^2 \in H^5$.

EXAMPLE 3.2. Wilson [7] gave the following values of c as in Theorem 3.6:

q	181	211	241	271	421	541	571	601	661	751	811	991
c	4	9	80	9	74	100	20	46	6	56	6	2

q	1021	1051	1171	1201	1231	1321	1471	1531	1621	1831	1861
c	29	11	112	19	53	11	12	79	8	63	22

We can also construct $DF^*(k, \lambda; v)$ from rings. The following is basic in this manner.

THEOREM 3.7. *Let R be a ring and $B = \{b_1, \ldots, b_k\}$ be a subgroup of $U(R)$ with ΔB a subset of $U(R)$. Then there exists a $DF^*(k, k-1; |R|)$ over the ring R.*

PROOF. The relation defined by the following "x is related to y if and only if there exists a $b_i \in B$ such that $x \cdot b_i = y$" is an equivalence relation (see, for example, [1, Lemma 3.1]). Consider $\mathscr{F} = \{sB : s \in S\}$, where S is a system of distinct representatives for the equivalence classes modulo B of $R - \{0\}$. It is easy to see that the blocks in $\mathscr{F}$ are mutually disjoint and that $|sB| = |B| = k$ for each $s \in S$. Since $\Delta B = \sum_{b \in B - \{1\}} (b-1)B$, we have $\Delta\mathscr{F} = \sum_{s \in S} s\Delta B = \sum_{s \in S} \sum_{b \in B - \{1\}} (b-1)B = \sum_{b \in B - \{1\}} (b-1) \sum_{s \in S} sB = \sum_{b \in B - \{1\}} (R - \{0\}) = (k-1)(R - \{0\})$. Hence every non-zero element of R ocurs exactly $k-1$ times in $\Delta\mathscr{F}$. □

We have other constructions.

THEOREM 3.8. *Let $\mathscr{F} = \{sB : s \in S\}$ be a $DF^*(k, k-1; v)$ constructed by Theorem 3.7. If there is no $s \in S$ such that $sB = -sB$, then $\mathscr{F}$ can be partitioned into two $DF^*(k, (k-1)/2; v)$'s.*

PROOF. The base blocks sB and $-sB$ possess the same set of differences. Note that $-sB = -s'B$ where s' is a representative of the equivalence class containing $-s$. In fact, $-sB$ is a base block. Separate the blocks of $\mathscr{F}$ into two sets, $\mathscr{F}_1$ and $\mathscr{F}_2$, such that $sB \in \mathscr{F}_1$ if and only if

$-sB \in \mathscr{F}_2$. □

The condition that $sB \neq -sB$ is always satisfied when k is odd and the additive group of the ring contains no non-zero elements which are their own inverse. This can be given in the following form.

COROLLARY 3.2. *Let $\mathscr{F} = \{sB: s \in S\}$ be a $DF^*(k, k-1; v)$ constructed by Theorem 3.7. If k is odd and the additive group of the ring contains no non-zero elements which are their own inverse, then $\mathscr{F}$ can be partitioned into two $DF^*(k, (k-1)/2; v)$'s.*

COROLLARY 3.3. *Let $v = \prod_{i=1}^{m} p_i^{n_i}$, p_i a prime, n_i a positive integer, $1 \le i \le m$. If k is odd and $k \mid (p_i^{n_i} - 1)$ for all i, $1 \le i \le m$, and at least one of $p_i^{n_i}$ is odd, then there exists a $DF^*(k, (k-1)/2; v)$.*

PROOF. Consider the Galois ring $GR(v) = \bigoplus_{i=1}^{m} GF(p_i^{n_i})$. Let $B_i = (\beta_{i1}, \beta_{i2}, \ldots, \beta_{ik})$ be the subgroup of order k in $GF(p_i^{n_i}) - \{0\}$. Apply Corollary 3.2 with $B = \{(\beta_{1j}, \beta_{2j}, \ldots, \beta_{mj}): j = 1, 2, \ldots, k\}$. □

4. Resolvable designs

For convenience, let $RB_w(k, \lambda; v)$ denote an $RB(k, \lambda; v)$ containing a subdesign $RB(k, \lambda; w)$.

As mentioned in Section 2, a $D(k, \lambda; q)$ over a finite field is always a $DF^*(k, \lambda; q)$. By Theorem 1.1, when $\lambda \le k-1$, there exists an $RB_k(k, \lambda; kq)$. This observation is here essential to construct resolvable designs. For example, we have the following.

PROPOSITION 4.1. *There exists an $RB_9(9, 1; 9 \cdot 73^n)$ for $n \ge 1$.*

PROOF. The set $\{1, 2, 4, 8, 16, 32, 37, 55, 64\}$ is a $DF^*(9, 1; 73)$ in $G(73)$. By Theorem 3.1, there exists a $DF^*(9, 1; 73^n)$ for $n \ge 1$. Then apply Theorem 1.1. □

THEOREM 4.1. *Let q be a prime power. Then*

(1) *there exists an $RB_{(q-1)/2}((q-1)/2, (q-3)/4; q^n(q-1)/2)$ for $n \ge 1$, whenever $q \equiv 3 \bmod 4$;*

(2) *there exists an $RB_{(q-1)/4}((q-1)/4, (q-5)/16; q^n(q-1)/4)$ for $n \ge 1$, whenever $q = 4t^2 + 1$ with t odd;*

(3) *there exists an $RB_{(q+3)/4}((q+3)/4, (q+3)/16; q^n(q+3)/4)$ for $n \ge 1$, whenever $q = 4t^2 + 9$ with t odd;*

(4) *there exists an $RB_{(q-1)/8}((q-1)/8, (q-9)/64; q^n(q-1)/8)$ for $n \ge 1$, whenever $q = 8a^2 + 1 = 64b^2 + 9$ with a, b odd;*

(5) *there exists an $RB_{(q-1)/8}((q-1)/8, (q+7)/64; q^n(q-1)/8)$ for $n \ge 1$,*

whenever $q = 8a^2 + 49 = 64b^2 + 441$ *with a odd and b even.*

PROOF. The corresponding $DF^*(k, \lambda; q^n)$'s exist from [3, Section 11.6] and then apply Theorem 3.1. □

The following results are immediate consequences of the results described in Section 3 and Theorem 1.1.

PROPOSITION 4.2. *There exists an* $RB_6(6, 1; 6 \cdot 121^n)$ *for* $n \geq 1$.

THEOREM 4.2. *There exists an* $RB_{(q-1)/2}((q-1)/2, (q-3)/2; q^n(q-1)/2)$ *for* $n \geq 1$.

THEOREM 4.3. *Let e be a divisor of* $q-1$, $tk \leq e \leq tk(k-1)$, *and* $B_1, \ldots, B_t$ *be t k-subsets of* $GF(q)$ *such that the elements of* B_i, $1 \leq i \leq t$, *are in different cosets of* $H_0^e, \ldots, H_{e-1}^e$, *that is,* $\sum_{i=1}^t \Delta B_i$ *has r entries in each coset* H_x^e. *Then* $re = tk(k-1)$ *and there exists an* $RB_k(k, r; kq^n)$ *for* $n \geq 1$. *Furthermore, if* $2e \mid (q-1)$, *then there exists an* $RB_k(k, r/2; kq^n)$ *for* $n \geq 1$.

COROLLARY 4.1. *If* $q \equiv 1 \mod k(k-1)$ *and there exists a set* $B = \{b_1, \ldots, b_k\} \subset GF(q)$ *with* b_i*'s in distinct cosets modulo* $H^{k(k-1)/2}$ *such that* $\{b_j - b_i: 1 \leq i < j \leq k\}$ *is a system of representatives for the cosets* $\mathscr{H}^{k(k-1)/2}$, *then there exists an* $RB_k(k, 1; kq^n)$ *for* $n \geq 1$.

THEOREM 4.4. *Let* λ *be a factor of* $k(k-1)$, *and q a prime power.*

(1) *If* $k(k-1)/\lambda$ *is even,* $q \equiv 1 \mod k(k-1)/(2\lambda)$ *and* $q > (k(k-1)/(2\lambda))^{k(k+1)}$, *then there exists an* $RB_k(k, 2\lambda; kq^n)$ *whenever* $\lambda \leq (k-1)/2$ *and* $n \geq 1$. *Furthermore, if* $q \equiv 1 \mod k(k-1)/\lambda$, *then there exists an* $RB_k(k, \lambda; kq^n)$ *whenever* $\lambda \leq k-1$ *and* $n \geq 1$.

(2) *If* $k(k-1)/\lambda$ *is odd,* $q \equiv 1 \mod k(k-1)/\lambda$ *and* $q > (k(k-1)/\lambda)^{k(k+1)}$, *then there exists an* $RB_k(k, \lambda; kq^n)$ *whenever* $\lambda \leq k-1$ *and* $n \geq 1$.

THEOREM 4.5. *If a prime power q satisfies the condition* R_k, *then there exists an* $RB_k(k, 1; kq^n)$ *for* $n \geq 1$.

PROPOSITION 4.3. *Let* $RB_w(k, \lambda) = \{v\colon$ *an* $RB_w(k, \lambda; v)$ *exists*$\}$. *Then*

$RB_7(7, 1) \supset \{7 \cdot q^n: n \geq 1, q = 337, 421, 463, 883, 1723, 3067, 3319\}$;

$RB_9(9, 1) \supset \{9 \cdot q^n: n \geq 1, q = 73, 1153, 1873, 2017\}$;

$RB_{15}(15, 1) \supset \{15 \cdot 76231^n: n \geq 1\}$.

THEOREM 4.6. *Let* $q = 30t + 1$ *be a prime power and* ξ *be a primitive cube root of unity in* $GF(q)$. *If there exists an element* $c \in GF(q)$ *such that* $\{\xi - 1, c(\xi - 1), c - 1, c - \xi, c - \xi^2\}$ *is a system of representatives for the cosets modulo* H^5, *then there exists an* $RB_6(6, 1; 6 \cdot q^n)$ *for* $n \geq 1$.

THEOREM 4.7. *If* $4 \leq t \leq 832$, *and* $6t + 1$ *is a prime power for even t, or*

$5t+1=q^n$ where $n \geq 1$ and $q \in \{121, 181, 211, 241, 271, 421, 541, 571, 601, 661, 751, 811, 991, 1021, 1051, 1171, 1201, 1231, 1321, 1471, 1531, 1621, 1831, 1861\}$. Then there exists an $RB_6(6, 1; 30t+6)$.

PROOF. This follows from [2] and Example 3.2 and Proposition 4.2. □

THEOREM 4.8. *Let R be a ring and $B = \{b_1, \dots, b_k\}$ be a subgroup of $U(R)$ with ΔB a subset of $U(R)$. Then there exists an $RB_k(k, k-1; |R|)$.*

THEOREM 4.9. *Let $\mathscr{F} = \{sB: s \in S\}$ be a $DF^*(k, k-1; v)$ constructed using Theorem 3.8. If there is no $s \in S$ such that $sB = -sB$, then there exists two $RB_k(k, (k-1)/2; kv)$'s.*

COROLLARY 4.1. *Let $\mathscr{F} = \{sB: s \in S\}$ be a $DF^*(k, k-1; v)$ constructed by Theorem 3.8. If k is odd and the additive group of the ring contains no non-zero elements which are their own inverse, then there exists two $RB_k(k, (k-1)/2; kv)$'s.*

COROLLARY 4.2. *Let $v = \prod_{i=1}^{m} p_i^{n_i}$, p_i a prime, n_i a positive integer, $1 \leq i \leq m$. If k is odd and $k \mid (p_i^{n_i} - 1)$ for all i, $1 \leq i \leq m$, and at least one of $p_i^{n_i}$ is odd, then there exists an $RB_k(k, (k-1)/2; kv)$.*

REMARK. A method using difference families is utilized to provide individual examples or infinite classes of resolvable designs, but their index λ and/or number of points v are restricted by k. It is meaningful to find more $DF^*(k, \lambda; v)$ in which v is not large and λ is without such restriction.

Acknowledgement

The authors are grateful to the referee for his helpful comments.

References

[1] S. Furino, Difference families from rings, Discrete Math., **97** (1991), 177–190.

[2] M. Greig, Some group divisible design constructions, preprint.

[3] M. Hall Jr., Combinatorial Theory, 2nd edition, John Wiley, 1986.

[4] Y. Miao and L. Zhu, On resolvable BIBDs with block size five, Ars Combinatoria, **39** (1995), 261–275.

[5] D. K. Ray-Chaudhuri and R. M. Wilson, The existence of resolvable block designs, A Survey of Combinatorial Theory (Ed. by J. N. Srivastava et al.), 361–375, North-Holland Publishing Company, 1973.

[6] P. Schellenberg, Personal communication.

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

Department of Mathematics
Faculty of School Education
Hiroshima University
Higashi-Hiroshima 739, *Japan*
and
Department of Mathematics
Faculty of Science
Hiroshima University
Higashi-Hiroshima 739, *Japan*