数理解析研究所講究録
第 607 巻 1987 年 22-32

CONSTRUCTIONS FOR CYCLIC STEINER 2-DESIGNS

*Rudolf Mathon**

Department of Computer Science
University of Toronto
Toronto, Ontario, Canada M5S 1A4

ABSTRACT

This paper surveys direct and recursive constructions for cyclic Steiner 2-designs. A new method is presented for cyclic designs with blocks having a prime number of elements. Several new constructions are given for designs with block size 4 which are based on perfect systems of difference sets and additive sequences of permutations.

1. Introduction

A *balanced incomplete block design* (briefly BIBD) with parameters (v,k,λ) is a pair (V,B) where V is a v-set and B is a collection of k-subsets of V (called *blocks*) such that every 2-subset of V is contained in exactly λ blocks. A *Steiner 2-design* is a (v,k,λ) BIBD with $\lambda = 1$. An *automorphism* of a BIBD (V,B) is a bijection $\phi: V \to V$ such that the induced mapping $\Phi: B \to B$ is also a bijection. The set of all such mappings forms a group under composition called the automorphism group of the design.

A (v,k,λ) BIBD is *cyclic* if it has an automorphism consisting of a single cycle of length v. Cyclic (v,k,λ) BIBD's will be denoted by $C(v,k,\lambda)$. A (v,k,λ) *difference family* (briefly DF) is a collection of k-subsets $D_1,\ldots,D_t$ of the integers Z_v modulo v such that for each nonzero $x \in Z_v$ the congruence $d_i - d_j \equiv x \pmod v$ has exactly λ solution pairs (d_i,d_j) with $d_i,d_j \in D_l$, for some l. A (v,k,λ) DF is called *simple* if $\lambda = 1$. It is easily verified that a necessary condition for the existence of a (v,k,λ) DF is $\lambda(v-1) \equiv 0 \bmod k(k-1)$. In particular, if a simple DF exists then $v \equiv 1 \bmod k(k-1)$. A (v,k,λ) DF generates a cyclic BIBD $C(v,k,\lambda)$ with $V = Z_v$ and $B = \{\sigma^i D_l \mid 0 \le i < v,\ 1 \le l \le t\}$, where $\sigma: V \to V$, $\sigma(x) = x+1 \bmod v$ and $n = \lambda(v-1)/(k(k-1))$. The t blocks $D_1,\ldots,D_t$ are called *starter* or *base blocks* of the design (V,B) (they are representatives of the orbits of B under σ). An orbit analysis of a cyclic Steiner 2-design $C(v,k)$ yields the following necessary existence condition:

$$v \equiv 1, k \bmod k(k-1). \tag{1}$$

The case $v = k(k-1)t+1$ corresponds to a simple DF. If $v = k(k-1)t+k$ then there are $t+1$ starter blocks $D_0,D_1,\ldots,D_t$, where $D_0 = \{0,m,2m,\ldots,(k-1)m\}$, $m = (k-1)t+1$

* Research supported by NSERC Grant No.A8651.

generates a m-orbit and $D_1, \ldots, D_t$ generate t v-orbits under σ. It is clear, that the differences in $D_1, \ldots, D_t$ cover the elements $Z_v \backslash D_0$ exactly once.

Two difference families $\mathbf{D} = \{D_1, \ldots, D_t\}$ and $\mathbf{D}' = \{D_1', \ldots, D_t'\}$ are said to be *equivalent* if for some integers $r, s_1, \ldots, s_t$

$$\{D_1', \ldots, D_t'\} = \{rD_1 + s_1, \ldots, rD_t + s_t\} \bmod v. \tag{2}$$

If $\mathbf{D}$ is equivalent with itself, then the corresponding r is called a *multiplier* of $\mathbf{D}$ and $\tau: x \to rx$, $x \in Z_v$ is an automorphism of the cyclic design.

Cyclic designs have a nice structure and interesting algebraic properties. Their concise representation makes them attractive in applications and for testing purposes. Cyclic BIBD's and difference systems have been studied by many authors [3], [7], [10], [13]. Results concerning cyclic Steiner 2-designs are surveyed in [5] which also contains a fairly extensive bibliography.

The present paper addresses the problem of existence of cyclic Steiner 2-designs $C(v,k,1)$. In the next two sections we discuss direct and recursive constructions for general block sizes k. In addition to known techniques, several new constructions are presented for $k = 4$ and 5. We conclude with a list of open problems. The paper significantly extends the existence results given in [5] for cyclic Steiner 2-designs with block sizes $k > 3$.

2. Direct Constructions

The majority of direct methods for constructing cyclic designs are based on finite fields. In this section we survey those constructions which apply to Steiner 2-designs and apply them to generate some new designs with blocks of prime size.

We begin with two general constructions of Wilson for $(v,k,1)$ difference families [13].

Theorem 1 Let $p = k(k-1)t + 1$ be a prime and α a primitive root of Z_p. Let H^m be the multiplicative subgroup of $Z_p \backslash \{0\}$ generated by α^m and let $\omega = \alpha^{2mt}$.

(i) If $k = 2m + 1$ is odd and $\{\omega-1, \omega^2-1, \ldots, \omega^m-1\}$ is a system of representatives for the cosets $\alpha^i H^m$, $i = 0,1, \ldots, m-1$, then the blocks $D_{i+1} = \{\alpha^{mi}, \omega\alpha^{mi}, \ldots, \omega^{2m}\alpha^{mi}\}$, $i = 0,1, \ldots, t-1$ form a $(p,k,1)$ DF.

(ii) If $k = 2m$ is even and $\{1, \omega-1, \ldots, \omega^{m-1}-1\}$ is a system of representatives for the cosets $\alpha^i H^m$, $i = 0,1, \ldots, m-1$, then the blocks $D_{i+1} = \{0, \alpha^{mi}, \omega\alpha^{mi}, \ldots, \omega^{2m-2}\alpha^{mi}\}$, $i = 0,1, \ldots, t-1$ form a $(p,k,1)$ DF in Z_p.

Theorem 2 Let $p = k(k-1)t + 1$ be a prime and α a primitive root of Z_p. If there exists a set $B = \{b_1, \ldots, b_k\} \subset Z_p$ such that $\{b_j - b_i \mid 1 \le i < j \le k\}$ is a system of representatives for the cosets $\alpha^i H^m$, $i = 0,1, \ldots, m-1$, where $m = k(k-1)/2$ and H^m is the subgroup of $Z_p \backslash \{0\}$ generated by α^m, then $D_{i+1} = \alpha^{2mi} B$, $i = 0,1, \ldots, t-1$ is a $(p,k,1)$ DF in Z_p.

Our next result concerns the case $v \equiv k \mod k(k-1)$.

Theorem 3 Let $k = 2m + 1$ and $p = 2mt + 1$, $n \geq 2$ be two odd primes and let α be a primitive root of Z_p. Define $m - 1$ numbers r_i by the equations $\alpha^{r_i} = \alpha^{ti} - 1$, $i = 1, \ldots, m - 1$. If there exists a $\beta \in Z_k$ such that the $2m$ elements $\pm 1, \pm(\beta^{ti} - 1)\beta^{-r_i}$, $i = 1, \ldots, m - 1$ are all distinct in Z_k, then the blocks

$$\begin{aligned} D_0 &= \{0_0, 0_1, \ldots, 0_{2m}\} \\ D_{i+1} &= \{0_0, \alpha^{i}_{\beta^i}, \alpha^{t+i}_{\beta^{t+i}}, \ldots, \alpha^{2mt-t+i}_{\beta^{2mt-t+i}}\}, \quad i = 0, 1, \ldots, t - 1 \end{aligned} \tag{3}$$

form a $(kp, k, 1)$ DF in Z_{kp}.

Proof We note, that since in the family of blocks $\mathbf{B} = \{B_1, \ldots, B_t\}$, $B_{i+1} = \{0, \alpha^i, \ldots, \alpha^{2mt-t+i}\}$ each nonzero difference appears exactly $k - 2m + 1$ times, $\mathbf{B}$ forms a (p, k, k) DF in Z_p. To complete the proof, it suffices to show that for any fixed difference in $\mathbf{B}$ the corresponding subscript differences cover every non-zero element of Z_k exactly once. Since for each i, $(\alpha^{ti} - 1)\alpha^{-r_i} = 1$ this is equivalent to the assumption that $\pm 1, \pm(\beta^{ti} - 1)\beta^{-r_i}$, $i = 1, \ldots, m - 1$ are distinct in Z_k. Finally, since k and p are distinct primes the design is cyclic in Z_{kp}. $\square$

We will apply Theorem 3 to blocksize $k = 7$. Then $m = 3$ and p is a prime of the form $p = 6t + 1$, $t \geq 2$. If α is a primitive root of Z_p, then $\alpha^{3t} = -1$ and since

$$(\alpha^t + 1)\alpha^{2t} = \alpha^{2t} - 1 = (\alpha^t + 1)(\alpha^t - 1)$$

we have $\alpha^t - 1 = \alpha^{2t}$. Let r be the solution of $\alpha^r = \alpha^{2t} - 1$. We require that for some $\beta \in Z_7$ the 6 numbers

$$\pm\beta^{2t}, \ \pm(\beta^t - 1), \ \pm\beta^{2t-r}(\beta^{2t} - 1) \tag{4}$$

cover the non-zero elements of Z_7. Since β^{2t} cannot be congruent to 1 modulo 7, we see that $t \equiv 1$ or $2 \mod 3$. If $t \equiv 1 \mod 3$, then (4) are distinct if either $\beta = 2$ and $r \equiv 0 \mod 3$, or $\beta = 4$ and $r \equiv 2 \mod 3$. If $t \equiv 2 \mod 3$, then we need either $\beta = 2$ and $r \equiv 1 \mod 3$, or $\beta = 4$ and $r \equiv 0 \mod 3$. Combining all these conditions we obtain the following result.

Corollary 4 Let $p = 6t + 1$ be a prime, $t \geq 2$, $t \not\equiv 0 \mod 3$, and let α be a primitive root in Z_p. Then the blocks (3) form a $(7p, 7, 1)$ DF for some $\beta \in Z_7$ if and only if $t \not\equiv r \mod 3$, where r satisfies $\alpha^r = \alpha^{2t} - 1$.

We note, that for some values of t we obtain two non-isomorphic cyclic designs. If $t \equiv 4 \mod 6$, then (4) are distinct also if either $\beta = 3$ and $r \equiv 2 \mod 3$, or $\beta = 5$ and $r \equiv 0 \mod 3$. If $t \equiv 2 \mod 6$, then (4) are distinct also if either $\beta = 3$ and $r \equiv 0 \mod 3$, or $\beta = 5$ and $r \equiv 1 \mod 3$.

For $k = 7$ solutions exist when t = 2*, 5, 7, 13, 16*, 26*, 35, 37, 38*, 40*, 46*, 47, etc. The base blocks for $t = 2^*$, 5 and 7 are

$$
\begin{array}{ccccccc}
0_0 & 1_1 & 4_4 & 3_2 & 12_1 & 9_4 & 10_2 \\
0_0 & 2_2 & 8_1 & 6_4 & 11_2 & 5_1 & 7_4
\end{array}
\qquad
\begin{array}{ccccccc}
0_0 & 1_1 & 4_4 & 3_2 & 12_1 & 9_4 & 10_2 \\
0_0 & 2_5 & 8_6 & 6_3 & 11_5 & 5_6 & 7_3
\end{array}
$$

$$
\begin{array}{ccccccc}
0_0 & 1_1 & 26_4 & 25_2 & 30_1 & 5_4 & 6_2 \\
0_0 & 3_2 & 16_1 & 13_4 & 28_2 & 15_1 & 18_4 \\
0_0 & 9_4 & 17_2 & 8_1 & 22_4 & 14_2 & 23_1 \\
0_0 & 27_1 & 20_4 & 24_2 & 4_1 & 11_4 & 7_2 \\
0_0 & 19_2 & 29_1 & 10_4 & 12_2 & 2_1 & 21_4
\end{array}
\qquad
\begin{array}{ccccccc}
0_0 & 1_1 & 37_2 & 36_4 & 42_1 & 6_2 & 7_4 \\
0_0 & 3_2 & 25_4 & 22_1 & 40_2 & 18_4 & 21_1 \\
0_0 & 9_4 & 32_1 & 23_2 & 34_4 & 11_1 & 20_2 \\
0_0 & 27_1 & 10_2 & 26_4 & 16_1 & 33_2 & 17_4 \\
0_0 & 38_2 & 30_4 & 35_1 & 5_2 & 13_4 & 8_1 \\
0_0 & 28_4 & 4_1 & 19_2 & 15_4 & 39_1 & 24_2 \\
0_0 & 41_1 & 12_2 & 14_4 & 2_1 & 31_2 & 29_4
\end{array}
$$

The solutions for $t = 5$ and 7 are first examples of BIBD's with the parameters (217,7,1) and (301,7,1), respectively. For $k = 11$ solutions exist when t = 33, 54*, 57, 91, 94*, etc. and for $k = 13$, t = 13, 19, 59, etc. (* indicates 2 solutions).

We conclude this section with a well-known result in finite geometries [6].

Theorem 5 Let q be a prime power. Then the lines in the projective geometry $PG(n,q)$, $n \geq 2$ form a cyclic design with parameters $((q^{n+1} - 1)/(q - 1), q + 1, 1)$.

3. Recursive Constructions

Given two difference families it is sometimes possible to combine them to construct a new one. Several such constructions are known for general cyclic BIBD's [4] [8] [14]. To apply them, various conditions on the block sizes are usually required.

We begin with a construction by C.J. Colbourn and M.J. Colbourn [4].

Theorem 6 Let $A^t_i = \{0, a^i_1, \ldots, a^i_{k-1}\}$, $i = 1, \ldots, t$ be a $(v,k,1)$ DF in Z_v and let $B^s_j = \{0, b^j_1, \ldots, b^j_{k-1}\}$, $j = 1, \ldots, s$ be a $(w,k,1)$ DF in Z_w.

(i) If $v = k(k-1)t + 1$ and w is relatively prime to $(k-1)!$, then for $i = 1, \ldots, t$, $j = 1, \ldots, s$ and $l = 0, 1, \ldots, w-1$

$$
\left.\begin{array}{l}
\{0, a^i_1 + lv, a^i_2 + 2lv, \ldots, a^i_{k-1} + (k-1)lv\} \\
\{0, vb^j_1, vb^j_i, \ldots, vb^j_{k-1}\}
\end{array}\right\} \qquad (5)
$$

is a $(vw,k,1)$ DF in Z_{vw}.

(ii) If $v = k\alpha$, $w = k\beta$ and β is relatively prime to $(k-1)!$, then for $i = 1, \ldots, t$, $j = 1, \ldots, s$ and $l = 0, 1, \ldots, w-1$

$$\left.\begin{array}{l} \{0, a^i_1 + lv, a^i_2 + 2lv, \ldots, a^i_{k-1} + (k-1)lv\} \\ \{0, \alpha b^{j_1}, \alpha b^{j_2}, \ldots, \alpha b^{j_{k-1}}\} \\ \{0, \alpha\beta, 2\alpha\beta, \ldots, (k-1)\alpha\beta\} \end{array}\right\} \qquad (6)$$

is a $(k\alpha\beta, k, 1)$ DF in $Z_{k\alpha\beta}$. Here $\alpha = (k-1)t + 1$, $\beta = (k-1)s + 1$, and only full orbit base blocks A^t_i, B^s_j are considered.

We note that the construction can be used if either w or β are prime. Then the existence of a $(w, k, 1)$ DF implies the existence of a $(w^n, k, 1)$ DF for every $n \geq 1$. Similarly, from a $(k\beta, k, 1)$ DF we obtain a $(k\beta^n, k, 1)$ DF. Also, if a $(v, k, 1)$ DF exists with $v \equiv 1 \bmod k(k-1)$ and prime k then there exists a $(vk, k, 1)$ DF.

In [8] M. Jimbo and S. Kuriki have introduced a more general construction for cyclic BIBD's which is based on orthogonal arrays. Applying it to Steiner 2-designs we obtain the following typical result.

Theorem 7 Suppose there exists a $C(v, k, 1)$ and a $C(w, k, 1)$, where $v \equiv 1 \bmod k(k-1)$ and k is an odd prime. Then there exists a $C(vw, k, 1)$. If, in addition, $w \equiv 1 \bmod k(k-1)$, then the conclusion holds for k a prime power.

So, for example, if k is an odd prime not dividing v, then the existence of a $C(v, k, 1)$ implies the existence of both $C(v^n, k, 1)$ and $C(kv^n, k, 1)$ for any $n \geq 1$.

The next construction employs cyclic pairwise balanced designs. A *pairwise balanced design* (briefly PBD) is a pair (V, B) where V is a v-set and B is a collection of subsets of V (blocks) such that every 2-subset of V is contained in exactly one block. A PBD will be denoted by $(v, K, 1)$, where $K = \{k_1, \ldots, k_n\}$ is the set of block sizes.

Theorem 8 Suppose there exists a cyclic $(v, K, 1)$ PBD with $K = \{k_1, \ldots, k_n\}$ and that for each k_i there exists a $(k_i, k, 1)$ Steiner 2-design. Then there exists a $C(v, k, 1)$.

Proof Replace each base block in the PBD by the blocks of the corresponding Steiner 2-design to obtain the base blocks of the final $C(v, k, 1)$. □

In the next section we shall give some other recursive constructions for cyclic designs with blocks of size 4 and 5 which are based on the concepts of perfect systems of difference sets and additive sequences of permutations.

4. Special Constructions

The existence question for cyclic Steiner triple systems has been completely settled by Peltesohn [10], who constructed $C(v,3,1)$ for all $v \equiv 1,3 \bmod 6$, $v \neq 9$.

For block sizes $k > 3$ the existence problem for $C(v,k,1)$ remains unsolved. The state of affairs is most promising for the cases $k = 4$ and 5.

In order to present additional recursive constructions we require a few more definitions.

A collection of t k-subsets $D_i = \{d^i{}_0, d^i{}_1, \ldots, d^i{}_{k-1}\}$, $0 = d^i{}_0 < d^i{}_1 < \cdots < d^i{}_{k-1}$, $i = 1, \ldots, t$ is said to be a *perfect difference family* (PDF) in Z_v, $v = k(k-)t + 1$, if the $tk(k-1)/2$ differences $d^i{}_l - d^i{}_j$, $0 \le j < l < k$ cover the set $\{1,2, \ldots, tk(k-1)/2\}$. PDF's are equivalent to regular perfect systems of difference sets starting with 1, which have been studied by many authors (see [1] for a recent survey). It has been shown [2] that PDF's can exist only when k is 3,4 or 5. For $k = 3$ the existence of a PDF is related to Skolem's partitioning problem [1].

Let X^1 be the m-vector $(-r, -r+1, \ldots, -1, 0, 1, \ldots, r-1, r)$, $m = 2r + 1$ and let $X^2, \ldots, X^n$ be permutations of X^1. Then $X^1, \ldots, X^n$ is an *additive sequence of permutations* (ASP) of order m and length n if the vector sum of every subsequence of consecutive permutations is again a permutation of X^1. ASP's play an important role in recursive constructions for PDF's and vice versa [1] [11] [12].

Block size 4

We begin with two direct constructions.

Theorem 9 let $p = 12t + 1$, $t \ge 1$ be a prime and let α be a primitive root of Z_p.

(i) ([3] [13]) If $p \neq x^2 + 36y^2$ for any integers x and y then

$$\{0, \alpha^{2i}, \alpha^{4t+2i}, \alpha^{8t+2i}\} \quad i = 0,1, \ldots, t-1 \tag{7}$$

is a $(p,4,1)$ DF in Z_p.

(ii) ([5]) If $\alpha \equiv 3 \bmod 4$ (and such an α always exists in Z_p) then

$$\left.\begin{array}{l} \{0, \alpha^{4i}, \alpha^{4i+3}, \alpha^{4i+6}\} \quad i = 0, \ldots, 3t-1\} \\ \{0, \alpha^{4j+1}, \alpha^{4t+4j+1}, \alpha^{8t+4j+1}\} \quad j = 0, \ldots, t-1\} \\ \{0, p, 2p, 3p\} \end{array}\right\} \tag{8}$$

form a $(4p,4,1)$ DF in Z_{4p}.

The next two constructions will exhibit the relationship between PDF's and ASP's.

Theorem 10 ([3] [13]) Let $D_i = \{0, a_i, b_i, c_i\}$, $i = 1, \ldots, t$ be a PDF in Z_{12t+1} and let X^1, X^2, X^3 be an ASP of order $m = 2r + 1$, $r \ge 2$ and length 3. Then

(i) For $i = 1, \ldots, t$ and $j = 1, \ldots, m$ the $6tm$ positive differences in the family

$$\Delta_{mi-m+j} = \{0, ma_i + \alpha_j, mb_i + \beta_j, mc_i + \gamma_j\} \tag{9}$$

cover the set $\{r+1, r+2, \ldots, r+6tm\}$. Here α, β and γ are the m-vectors X^1, $X^1 + X^2$, $X^1 + X^2 + X^3$, respectively.

(ii) For $i = 1, \ldots, t$

$$\left.\begin{aligned} X_i^1 &= (-c, a-c, -b, b-c, a-b, -a, a, b-a, c-b, b, c-a, c)_i \\ X_i^2 &= (c-b, c, b-a, c-a, b-c, a-c, -b, a, b, -c, a-b, -a)_i \\ X_i^3 &= (b-a, -b, a-c, a, c, c-b, b-c, -c, -a, c-a, b, a-b)_i \end{aligned}\right\} \tag{10}$$

the $(12t+1)$-vectors $X^j = (0, X^j_1, \ldots, X^j_t)$, $j = 1,2,3$ form an ASP of order $12t + 1$ and length 3.

In order to utilize products of the form (9) for constructing new difference families we need to find additional base blocks with differences covering the set $\{1, \ldots, r\}$ and possibly $\{r + 6tm + 1, \ldots, 6x\}$ for some $x \geq 1$.

We list now the known recursive constructions for $1 \leq m \leq 25$.

Theorem 11 Let $D(t) = \{D_1, \ldots, D_t\}$ be a PDF and let $\Delta(mt) = \{\Delta_1, \ldots, \Delta_{mt}\}$ be defined by (9), where $m = 2r + 1$ and $\alpha = (-r, -r+1, \cdots, -1, 0, 1, \ldots, r-1, r)$. Then

1. For $r = 2$

   $\beta = (-2,0,2,-1,1)$, $\gamma = (0,-2,1,-1,2)$

   $$D(5t+1) = \Delta(5t) \cup \{0,1,30t+4,30t+6\}$$

   is a PDF in Z_{60t+13}.

2. For $r = 3$

   $\beta = (-1,-2,-3,3,2,1,0)$, $\gamma = (-2,1,-3,0,3,-1,2)$

   $$D(7t+1) = \Delta(7t) \cup \{0,2,3,42t+7\}$$

   is a DF in Z_{84t+13}.

3. For $r = 6$

   $\beta = (-4,-5,-1,-2,3,-6,6,5,1,-3,0,2,4)$

   $\gamma = (-1,-5,-6,3,-3,-4,4,2,5,-2,6,1,0)$

   $$D(13t+1) = \Delta(13t) \cup \{0,1,4,6\}$$

   is a PDF in $Z_{156t+13}$.

4. For $r = 9$

   $\beta = (-6,-7,1,-2,-3,5,3,-9,-4,7,-8,0,-5,9,-1,6,2,4,8)$

$\gamma=$ (-2,1,-8,-9,3,-1,-5,-6,5,2,-7,7,-3,8,-4,6,0,9,4)

$$D(19t+4) = \Delta(19t) \cup \{0,1,7,x+23\} \cup \{0,2,x+14,x+19\}$$
$$\cup \{0,3,x+13,x+21\} \cup \{0,4,x+15,x+24\}, \ x = 114t$$

is a PDF in $Z_{228t+49}$.

5. For $r = 11$

β =(0,-2,1,-7,2,-6,-1,-5,4,-10,-11,-9,6,-4,-8,-3,11,8,10,3,5,7,9)

$\gamma=$ (9,5,4,-10,0,-7,10,-9,8,-4,-3,1,-5,-11,-8,2,6,-2,11,-6,7,-1,3)

$$D(23t+5) = \Delta(23t) \cup \{0,1,8,x+28\} \cup \{0,2,x+14,x+24\} \cup$$
$$\{0,3,x+18,x+29\} \cup \{0,4,x+17,x+23\} \cup \{0,5,x+21,x+30\}, \ x = 138t$$

is a PDF in $Z_{276t+61}$.

6. For $r = 12$

using α,β,γ and $\Delta(5t)$ from 1 to obtain $\Delta(25t)$

$$D(25t+5) = \Delta(25t) \cup \{0,1,x+18,x+29\} \cup \{0,4,x+20,x+26\}$$
$$\cup \{0,3,8,x+27\} \cup \{0,7,x+21,x+30\} \cup \{0,10,12,x+25\}, \ x = 150t$$

is a PDF in $Z_{300t+61}$, and

$$D(25t+6) = \Delta(25t) \cup \{0,1,x+34,x+36\} \cup \{0,3,x+18,x+29\}$$
$$\cup \{0,4,x+20,x+28\} \cup \{0,5,x+22,x+32\}$$
$$\cup \{0,6,x+19,x+31\} \cup \{0,7,x+21,x+30\}, \ x = 150t$$

is a PDF in $Z_{300t+79}$.

Proof Use (9) to check that the required sets are covered by all differences from the base blocks. ☐

We note that the constructions 2,5,6b are new and that 1,3,4,6a have been known [11]. The ASP with $r = 11$ has been found by P.J. Laufer.

If we apply all methods listed in Sections 2, 3 and 4 and add the computer generated DF's from [5] we obtain the following results for $1 \leq t \leq 50$:

$(12t+1,4,1)$ PDF

t = 1,4-8,14,21,23,26,28,30-31,36,41

$(12t+1,4,1)$ DF

t = 1,3-10,14-15,19-21,23,26,28-31,34-36,38,40-41,43,45,50

$(12t+4,4,1)$ DF

$t = 3\text{-}6,12,20,24,30,32,36,43$.

Block size 5

As before, two direct constructions are known.

Theorem 12 Let $p = 20t + 1$, $t \geq 1$ be a prime and let α be a primitive root of Z_p.

(i) ([3] [13]) If $p \neq x^2 + 100y^2$ for any integers x and y then

$$\{\alpha^{2i}, \alpha^{4t+2i}, \alpha^{8t+2i}, \alpha^{12t+2i}, \alpha^{16t+2i}\} \quad i = 0,1,\ldots,t-1 \tag{11}$$

is a $(p,5,1)$ DF in Z_p.

(ii) ([5]) If $\alpha^r + 1 = \alpha^s(\alpha^r - 1)$ for some odd integers r and s then

$$\{0, \alpha^{2i}, \alpha^{2i+r}, \alpha^{2t+2i}, \alpha^{2t+2i+r}\} \quad i = 0,1,\ldots,t-1 \tag{12}$$

$$\{0, p, 2p, 3p, 4p\}$$

form a $(5p,5,1)$ DF in Z_{5p}.

Concerning PDF's with blocks of size 5 and ASP of length 4, results can be proved which are similar to those stated in Theorem 10 [1]. They can be used to derive the following construction.

Theorem 13 Let $D(t) = \{D_1, \ldots, D_t\}$ be a PDF in C_{20t+1} and let $D(s) = \{D_1, \ldots, D_s\}$ be a DF in C_{20s+1}. Then a DF $D(r)$ exists in C_{20r+1}, $r = 20st + s + t$ and $D(r)$ is perfect whenever $D(s)$ is perfect.

Proof Use $D(t)$ to construct an ASP of length 4 and order $m = 20t+1$ [1]. With help of this ASP construct the blocks $\Delta(ms)$ in a similar way as in (9). Then $D(r) = \Delta(ms) \cup D(s)$. $\square$

PDF's with $k = 5$ can exist only if t is even and $t \geq 6$ [1]. They have been enumerated for $t = 6$ [9] and examples are known for $t = 8$, 10, 732, 974, etc.

Difference families are known for the following values of t, $1 \leq t \leq 50$:

$(20t+1)$ PDF

$t = 6, 8, 10$

$(20t+1)$ DF

$t = 1\text{-}3,6,8,10,12,14,21\text{-}22,30,32\text{-}33,35,41,43\text{-}44$

$(20t+5)$ DF

$t = 3\text{-}5,7,9\text{-}10,13,15,18,22,24\text{-}25,27\text{-}28,30,34,37,39\text{-}40,42\text{-}43,45,48\text{-}50$.

Open Problems

1. Does there exist a $(12t+1,4,1)$ DF for every $t \geq 3$? Can all of these DF's be perfect if $t \geq 4$?
2. Does there exist a $C(v,4,1)$ for every $v \neq 16, 25$ and 28?
3. Does there exist an ASP of length 3 for every order $m \geq 5$, $m \neq 9,10$?
4. Do there exist $C(v,5,1)$ for $v = 81$ and 85?
5. Construct examples of PDF's $D(t)$ for $k = 5$ and even $t \geq 12$.
6. Construct examples of ASP of length 4 for orders $m \geq 7$.

References

[1] J. Abrham, Perfect systems of difference sets - a survey, *Ars Combinatoria*, 17A (1984), 5-36.

[2] J.-C. Bermond, A. Kotzig, J. Turgeon, On a combinatorial problem of antennas in radioastronomy, *Proc. 18th Hungarian Combinatorial Colloquium*, North Holland, 1976, 135-149.

[3] R.C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* 9 (1939), 353-399.

[4] M.J. Colbourn, C.J. Colbourn, On cyclic block designs, *Math. Report of Canadian Academy of Science* 2 (1980), 21-26.

[5] M.J. Colbourn, R.A. Mathon, On cyclic Steiner 2-designs, *Ann. Discrete Math.* 7 (1980), 215-253.

[6] M. Hall, Jr., Combinatorial Theory, Blaisdell, Waldham, Mass. (1967).

[7] H. Hanani, Balanced incomplete block designs and related designs, *Discrete Math.* 11 (1975), 255-369.

[8] M. Jimbo, S. Kuriki, On a composition of cyclic 2-designs, *Discrete Math.* 46 (1983), 249-255.

[9] P.J. Laufer, Regular perfect systems of difference sets of size 4 and extremal systems of size 3, *Ann. Discrete Math.* 12 (1982), 193-201.

[10] R. Peltesohn, Eine Losung der beiden Heffterschen Differenzenprobleme, *Compositio Math.* 6 (1939), 251-257.

[11] D.G. Rogers, Addition theorems for perfect systems of difference sets, *J. Lond. Math. Soc.* (2), 23 (1981), 385-395.

[12] J.M. Turgeon, Construction of additive sequences of permutations of arbitrary lengths, *Ann. Discrete Math.* 12 (1982), 239-242.

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

[14] R.M. Wilson, Constructions and uses of pairwise balanced designs, *Combinatorics* (eds. M. Hall, Jr. and J.H. van Lint), Mathematical Centre, Amsterdam (1975), 19-42.