Designs, Codes and Cryptography, 5, 13–25 (1995)

A Powerful Method for Constructing Difference Families and Optimal Optical Orthogonal Codes

MARCO BURATTI
Facoltà di Ingegneria de L'Aquila, 67040 Poggio di Roio, L'Aquila, Italy

Communicated by: G. Tallini

Received February 1, 1994

Abstract. In this paper we proceed in the way indicated by R. M. Wilson for obtaining simple difference families from finite fields [28]. We present a theorem which includes as corollaries all the known direct techniques based on Galois fields, and provides a very effective method for constructing a lot of new difference families and also new optimal optical orthogonal codes.

By means of our construction—just to give an idea of its power—it has been established that the only primes $p < 10^5$ for which the existence of a cyclic $S(2, 9, p)$ design is undecided are 433 and 1009. Moreover we have considerably improved the lower bound on the minimum v for which an $S(2, 15, v)$ design exists.

1. Introduction

The major reference of the present work is the classic paper by R. M. Wilson published in Journal of Number Theory in 1972 [28]. Although the main result of that paper is the asymptotic existence theorem (a milestone in design theory), some direct constructions of simple difference families—and hence of Steiner 2-designs—are also remarkable; Wilson himself concludes that they are only an indication of the various possibilities for using finite fields to ease the task of constructing difference families. Here we will successfully exploit these possibilities in order to get new difference families and new optimal optical orthogonal codes but, firstly, we need some background.

Definition 1.1. Let G be a group written in additive notation and let $\mathcal{F} = \{B_1, \dots, B_t\}$ be a family of k-subsets of G:

$$B_i = \{b_{i1}, b_{i2}, \dots, b_{ik}\},\ i = 1, 2, \dots, t.$$

Such a family is called a (G, k, λ)-*difference family* (briefly (G, k, λ)-DF) when the following conditions hold:

Any nonzero element of G occurs exactly λ times in the list of differences

$$(b_{ij} - b_{ih} \mid 1 \le i \le t,\ 1 \le j \ne h \le k). \tag{1.1.a}$$

$$[B_i + g = B_i \Leftrightarrow g = 0] \text{ for } i = 1, 2, \dots, t. \tag{1.1.b}$$

The members of a difference family are called *base blocks*. A difference family with a single base block is naturally called a *difference set*. A (G, k, λ)-DF is said to be *simple* when $\lambda = 1$. Finally, a $(\mathbb{Z}_v, k, \lambda)$-DF is called *cyclic* and simply denoted by (v, k, λ)-DF.

Let $\mathcal{F} = \{B_1, \ldots, B_t\}$ be a family of nonempty subsets of an additive group G; recall that the *development* of $\mathcal{F}$ is the incidence structure defined as follows: dev $\mathcal{F} = (G, \mathcal{B}, \epsilon)$ with $\mathcal{B} := \{B_i + g \mid i = 1, 2, \ldots, t; g \in G\}$.

The following proposition explains the reason for which difference families have great importance in design theory:

PROPOSITION 1.2 *Let G be an additive group of order v and consider the class of incidence structures which are the development of some (G, k, λ) difference family. Such a class coincides with the class of 2-(v, k, λ) designs having G as a group of automorphisms acting regularly on the point set and semiregularly on the block set.*

In particular the $(v, k, 1)$-DFs give rise to the class of *cyclic* $S(2, k, v)$ designs without *short orbits*.

Now, we define the concept of optical orthogonal code. We warn the reader that our definition is more general than the original one [12], but coincides with it when G is the cyclic group of residues modulo an integer v.

Definition 1.3. Let G be a group written in additive notation and let C be a subset of $(\mathbb{Z}_2)^G$ whose elements have constant Hamming weight k. In other words any element of C is a map $x : G \to \mathbb{Z}_2 : g \mapsto x_g$ such that $|g \in G : x_g = 1| = k$. The set C is called a (G, k, λ) *optical orthogonal code* (briefly, (G, k, λ)-OOC) when, for any pair of distinct elements x and y of C the following conditions hold:

$$\sum_{g \in G} x_{g+h} \cdot x_{g+h'} \leq \lambda \qquad \forall h, h' \in G,\ h \neq h'; \tag{1.3.a}$$

$$\sum_{g \in G} x_{g+h} \cdot y_{g+h'} \leq \lambda \qquad \forall h, h' \in G. \tag{1.3.b}$$

The cardinality and the elements of C are called the *size* and *codewords* of C respectively.

A (G, k, λ)-OOC is called *optimal* (briefly (G, k, λ)-OOOC) when there exists no (G, k, λ)-OOC having larger size.

A (G, k, λ)-OOC is said to be *simple* when $\lambda = 1$. Finally, a $(\mathbb{Z}_v, k, \lambda)$-OOC is called *cyclic* and denoted by (v, k, λ)-OOC.

Note that when $G = \mathbb{Z}_v$ conditions (1.3.a) and (1.3.b) say that the ordinary inner product between two distinct cyclic shifts of a codeword (two cyclic shifts of distinct codewords respectively) is at most λ.

Let C be a (G, k, λ)-OOC of size t. Identify any codeword x of C with the k-subset B of G whose characteristic function is just x:

$$B := \{g \in G \mid x_g = 1\}.$$

In such a way, C can be identified as a family $\mathcal{F} = \{B_1, \dots, B_t\}$ of k-subsets of G (*codeword-sets*) satisfying the following conditions:

$$|(B_i + h) \cap (B_i + h')| \le \lambda \qquad \forall i \in \{1, 2, \dots, t\},\ \forall h \neq h' \in G; \tag{1.3.c}$$

$$|(B_i + h) \cap (B_j + h')| \le \lambda \qquad \forall i \neq j \in \{1, 2, \dots, t\}, \forall h, h' \in G. \tag{1.3.d}$$

On the other hand conditions (1.3.c) and (1.3.d) are equivalent to the following:

Any nonzero element of G occurs at most λ times in the list of differences $(b - b' \mid b, b' \in B_i, 1 \le i \le t)$. (1.3.e)

Any nonzero element of G occurs at most λ times in the list of differences $(b - b' \mid b \in B_i, b' \in B_j, 1 \le i \neq j \le t)$. (1.3.f)

From now on we agree to consider a (G, k, λ)-OOC as a family $\{B_i\}$ of k-subsets of G satisfying conditions (1.3.e, f). With this convention, it is easy to see that any $(G, k, 1)$ difference family can be regarded as a $(G, k, 1)$ optimal optical orthogonal code.

The study of (v, k, λ) optical orthogonal codes was originally motivated by an application in optical code-division multiple-access communications systems. The main reason which induced us to generalize the concept of (v, k, λ)-OOC to that of (G, k, λ)-OOC is the sake of uniformity of language. On the other hand we think that this generalization is also justified, at least in the case $\lambda = 1$, by the following proposition (note the analogy with Proposition 1.2):

PROPOSITION 1.4 *The class of incidence structures which are the development of some $(G, k, 1)$-OOC coincides with the class of k-uniform semilinear spaces admitting G as a group of automorphisms acting regularly on the point set and semiregularly on the line set.*

Notation 1.5. For a subset B of an additive group G, we will denote by ΔB the set (not the list!) of all the nonzero differences in B:

$$\Delta B := \{b - b' \mid b, b' \in B, b \neq b'\}.$$

We will use the following elementary proposition about simple OOCs:

PROPOSITION 1.6 *Let G be a group written in additive notation and let $\mathcal{F} = \{B_1, B_2, \dots, B_t\}$ be a family of k-subsets of G. In order that $\mathcal{F}$ be a $(G, k, 1)$-OOC it suffices that:*

$$|\Delta B_i| = k(k-1) \qquad \textit{for } 1 \le i \le t. \tag{1.6.a}$$

$$\Delta B_i \cap \Delta B_j = \varnothing \qquad \textit{for } 1 \le i < j \le t. \tag{1.6.b}$$

If, in addition to this, the following condition also holds,

$$t = \left\lfloor \frac{v-1}{k^2-k} \right\rfloor \quad \textit{(the integer part of } (v-1)/(k^2-k)\textit{)}, \qquad (1.6.c)$$

then the code is optimal.

The difference families and the optical orthogonal codes which are considered in this paper are all simple and found in the additive group of a finite field.

Notation 1.7. Let q be a prime power and let d be any divisor of $q-1$. Set:

$GF(q)$:= the Galois field of order q.

$EA(q)$:= the elementary abelian group of order q, i.e. the additive group of $GF(q)$.

ω := a fixed primitive element of $GF(q)$.

H^d := the group of d-th powers of $GF(q)$.

In particular, $H^1 = H$ is the multiplicative group of $GF(q)$. Note that if $q-1 = d \cdot e$, then H^d can be also regarded as the group of e-th roots of unity in $GF(q)$.

2. A Summary of Known Simple Difference Families from Finite Fields

In this section we review the theorems which lead to the known direct constructions of simple DFs in Galois fields. For the sake of brevity we do not specify the constructions in the statements. On the other hand such constructions will be clear in the light of the theorem in the next section.

THEOREM 2.1 (Bose '39). *If $q = 12t+1$ is a prime power such that $\omega^{4t}-1$ is not a square in $GF(q)$ (equivalently, -3 is not a 4-th power) then there exists an $(EA(q), 4, 1)$-DF.*

THEOREM 2.2 (Bose '39). *If $q = 20t+1$ is a prime power such that $\omega^{4t}+1$ is not a square in $GF(q)$ (equivalently, 5 is not a 4-th power) then there exists an $(EA(q), 5, 1)$-DF.*

We have recently improved (cf. [7]) Theorems 2.1 and 2.2 as follows:

THEOREM 2.3 (Buratti '93). *Let $q = 12t+1$ be a prime power and let 2^n be the highest power of 2 in t. If $\omega^{4t}-1 \notin H^{2^{n+1}}$ (equivalently, -3 is not in $H^{2^{n+2}}$), then there exists an $(EA(q), 4, 1)$-DF.*

THEOREM 2.4 (Buratti '93). *Let $q = 20t+1$ be a prime power and let 2^n be the highest power of 2 in t. If $\omega^{4t}+1 \notin H^{2^{n+1}}$ (equivalently, $(11+5\sqrt{5})/2$ is not in $H^{2^{n+1}}$), then there exists an $(EA(q), 5, 1)$-DF.*

It can be proved (cf. [7]) that Theorem 2.3 always succeds for powers of primes $p \equiv 2 (\mathrm{mod}\, 3)$ and that Theorem 2.4 always succeds for powers of primes $p \equiv \pm 2 (\mathrm{mod}\, 5)$.

Equivalent results to Theorems 2.3, 2.4 are obtained by S. Bitan and T. Etzion (cf. [3], Theorems 5 and 8).

Although it is not indicated in the statements, it should be noted that Theorems 2.3, 2.4 provide necessary and sufficient conditions for the existence of difference families consisting of appropriate cosets of $GF(q)$, while the conditions of Bose's theorems are only sufficient for this.

THEOREM 2.5 (Wilson '72). *Let $q = k(k-1)t + 1$ be a prime power, with k odd. If the set $\{\omega^{i(k-1)t} - 1 \mid 1 \leq i \leq \frac{1}{2}(k-1)\}$ is a complete system of representatives for the cosets of $H^{(k-1)/2}$, then there exists an $(EA(q), k, 1)$-DF.*

THEOREM 2.6 (Wilson '72). *Let $q = k(k-1)t + 1$ be a prime power, with k even. If the set $\{\omega^{ikt} - 1 \mid 1 \leq i \leq \frac{1}{2}k - 1\} \cup \{1\}$ is a complete system of representatives for the cosets of $H^{k/2}$, then there exists an $(EA(q), k, 1)$-DF.*

The above theorems of Wilson provide sufficient conditions for the existence of *radical difference families* (RDFs), i.e. DFs consisting in appropriate cosets of $GF(q)$, and are a generalization of Bose's theorems which correspond to the cases $k = 4$ and $k = 5$. The conditions of the next two theorems are also sufficient for the existence of RDFs but improve those of Wilson because are generally weaker than them. Moreover they are necessary at least for $k \leq 7$ (cf. [9]).

THEOREM 2.7 (Buratti '93). *Let $q = k(k-1)t + 1$ be a prime power, with k odd. Let $d_1 \mid d_2 \mid \ldots \mid d_{2s}$ be a chain of divisors of $\frac{1}{2}(k-1)t$ such that:*

(i) $\Pi_{1 \leq \alpha \leq s} d_{2\alpha}/d_{2\alpha-1} = \frac{1}{2}(k-1)$.

(ii) For any pair of distinct elements x, y in the set $\{\omega^{i(k-1)t} - 1 \mid 1 \leq i \leq \frac{1}{2}(k-1)\}$ there is a suitable $\alpha \in \{1, \ldots, s\}$ such that x, y are in distinct cosets of $H^{d_{2\alpha-1}}$ modulo $H^{d_{2\alpha}}$, i.e. $x^{-1}y \in H^{d_{2\alpha-1}} \backslash H^{d_{2\alpha}}$.

Then there exists an $(EA(q), k, 1)$-DF.

THEOREM 2.8 (Buratti '93). *Let $q = k(k-1)t + 1$ be a prime power, with k even. Let $d_1 \mid d_2 \mid \ldots \mid d_{2s}$ be a chain of divisors of $\frac{1}{2}k$ such that:*

(i) $\Pi_{1 \leq \alpha \leq s} d_{2\alpha}/d_{2\alpha-1} = \frac{1}{2}k$.

(ii) For any pair of distinct elements x, y in the set $\{\omega^{ikt} - 1 \mid 1 \leq i \leq \frac{1}{2}k - 1\} \cup \{1\}\}$ there is a suitable $\alpha \in \{1, \ldots, s\}$ such that x, y are in distinct cosets of $H^{d_{2\alpha-1}}$ modulo $H^{d_{2\alpha}}$, i.e. $x^{-1}y \in H^{d_{2\alpha-1}} \backslash H^{d_{2\alpha}}$.

Then there exists an $(EA(q), k, 1)$-DF.

The next theorem, besides being very useful for constructing DFs with "small" block size, is worth of attention especially because leads towards *Wilson's asymptotic existence theorem* [28], one of the most important results in design theory.

THEOREM 2.9 (*Wilson's lemma on blocks with evenly distributed differences, '72*). *Let $q = k(k-1)t + 1$ be a prime power and let B be a k-subset of $GF(q)$ such that any coset of $H^{k(k-1)/2}$ contains exactly two elements (additive inverses of each other) of ΔB. Then there exists an $(EA(q), k, 1)$-DF.*

To have an idea of how effective Theorem 2.9 is for low values of k, one can see an application of it in [8] where many DFs with block sizes 4 and 5 are easily obtained. However, as we have already said, the main reason why Theorem 2.9 is interesting is another: Wilson proves that for a fixed arbitrary k, the condition of Theorem 2.9 is asymptotically verified. This, combined with constructions of recursive type, implies that for v sufficiently large the conditions $v - 1 \equiv 0(\bmod k-1)$ and $v(v-1) \equiv 0(\bmod k(k-1))$ are necessary and sufficient for the existence of an $S(2, k, v)$ design (cf. [31]).

R. M. Wilson concludes his cyclotomic paper with the following theorem on simple DFs with block size 6:

THEOREM 2.10 (Wilson '72). *Let $q = 30t + 1$ be a prime power and suppose that there is an element b of $GF(q)$ such that $\{\omega^{10t} - 1, b(\omega^{10t} - 1), b - 1, b - \omega^{10t}, b - \omega^{20t}\}$ is a complete system of representatives for the cosets of the 5th powers. Then there exists an $(EA(q), 6, 1)$-DF.*

3. The Main Construction

In this section, proceeding as indicated by Wilson, we give a very useful theorem for constructing not only difference families but also optimal optical orthogonal codes. Moreover, this theorem has a unifying function because all the theorems stated in the previous section are corollaries of it. We look for families in $GF(q)$ whose members are unions of cosets of a multiplicative subgroup of $GF(q)$ and possibly $\{0\}$. The idea of modifying some known constructions of DFs in Galois fields in order to get OOOCs can be found also in [3].

THEOREM 3.1 *Let $k = ef$ or $k = ef + 1$ with e odd in both cases. Let q be a prime power such that the Euclidean division of $q - 1$ by $k(k-1)$ is of type:*

$$q - 1 = k(k-1)t + r,\ 0 \leq r < k(k-1),\ r \text{ divisible by } 2et. \qquad (3.1.a)$$

Set $\varepsilon = \omega^{(q-1)/e}$ and associate with any f-subset $B = \{b_1 = 1, b_2, \ldots, b_f\}$ of H the list L_B defined as follows:

$$L_B := (b_i - b_j \varepsilon^h \mid \left[1 \leq i = j \leq f,\ 1 \leq h \leq \frac{1}{2}(e-1)\right]$$

or

$$[1 \leq i < j \leq f,\ 1 \leq h \leq e]) + L_B^*$$

where L_B^* is the null list for $k = ef$, while is the list $(b_1, b_2, \ldots, b_f)$ of elements of B for $k = ef + 1$.

Let $(H^{d_1} \supset \cdots \supset H^{d_{2s}})$ be a chain of subgroups between H and $H^{(q-1)/(2e)}$—hence $(d_1, \ldots, d_{2s})$ is chain of divisors of $(q-1)/(2e)$—and set $d_0 = 1$, $d_{2s+1} = (q-1)/(2e)$. Suppose that B is an f-subset of H such that:

L_B is a subset of H, i.e. L_B has no repeated element and does not contain zero. *(3.1.b)*

$$\Pi_{0\leq\alpha\leq s} d_{2\alpha+1}/d_{2\alpha} = t. \qquad (3.1.c)$$

$$xy^{-1} \in \cup_{1\leq\alpha\leq s}(H^{d_{2\alpha-1}} \backslash H^{d_{2\alpha}}) \cup \{1\} \qquad \forall x, y \in L_B. \qquad (3.1.d)$$

Then, if we set

$$I := \left\{ \sum_{\alpha=0}^{s} d_{2\alpha} i_\alpha \mid 0 \leq i_\alpha < d_{2\alpha+1}/d_{2\alpha};\, \alpha = 0, 1, \ldots, s \right\},$$

we have that the family $\mathcal{F} := \{\omega^i B \cdot H^{(q-1)/e} \cup B^* \mid i \in I\}$—where $B^* = \varnothing$ or $B^* = \{0\}$ according to which $k = ef$ or $k = ef + 1$ respectively—is an $(EA(q), k, 1)$-OOOC. In particular, if $r = 0$, it is an $(EA(q), k, 1)$-DF.

Proof: Let's prove the theorem in the case $k = ef$.

Firstly, we show that every member of $\mathcal{F}$ is a k-subset of $GF(q)$. Of course, $H^{(q-1)/e}$ and $H^{(q-1)/(2e)}$ are the groups of e-th and $2e$-th roots of unity respectively: $H^{(q-1)/e} = \{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{e-1}\}$ and $H^{(q-1)/(2e)} = \{1, -1\} \cdot H^{(q-1)/e}$.

Now note that any two distinct elements of B represent distinct cosets of $H^{(q-1)/e}$: if $b_i b_j^{-1} \in H^{(q-1)/e}$ with $1 \leq i < j \leq f$, then there exists $h \in \{0, 1, \ldots, e-1\}$ such that $b_i b_j^{-1} = \varepsilon^h$, i.e. $b_i - b_j\varepsilon^h = 0$ which contradicts (3.1.b). From this, we have that any member of $\mathcal{F}$ is a union of f distinct cosets of the group of e-th roots of unity and hence has cardinality $ef = k$.

We need the following identity:

$$\Delta(B \cdot H^{(q-1)/e}) = H^{(q-1)/(2e)} \cdot L_B. \qquad (3.1.e)$$

The inclusion $H^{(q-1)/(2e)} \cdot L_B \subseteq \Delta(B \cdot H^{(q-1)/e})$ is trivial. In order to recognize the inverse inclusion it suffices to express the general element $b_i\varepsilon^h - b_j\varepsilon^{h'}$ of $\Delta(B \cdot H^{(q-1)/e})$ as follows:

$$b_i\varepsilon^h - b_j\varepsilon^{h'} = \begin{cases} \varepsilon^h(b_i - b_j\varepsilon^{h'-h}) \text{ if } i < j \text{ or if } (i = j \text{ and } 1 \leq h' - h \leq (e-1)/2) \\ -\varepsilon^{h'}(b_j - b_i\varepsilon^{h-h'}) \text{ if } i > j \text{ or if } (i = j \text{ and } 1 \leq h - h' \leq (e-1)/2). \end{cases}$$

Now, we must prove that conditions (1.6.a, b, c) hold.

The family $\mathcal{F}$ satisfies condition (1.6.a):

A trivial computation for the cardinality of L_B gives:

$$|L_B| = f(e-1)/2 + ef(f-1)/2 = f(ef-1)/2 = f(k-1)/2.$$

By the assumption (3.1.d), distinct elements of L_B represent distinct cosets of $H^{(q-1)/(2e)}$. Thus, by (3.1.e), $\Delta(B \cdot H^{(q-1)/e})$ is the union of $|L_B|$ distinct cosets of the $2e$-th roots of unity and hence has cardinality $2e \cdot f(k-1)/2 = k(k-1)$.

The family $\mathcal{F}$ satisfies condition (1.6.b):

Let $i = \sum_{\alpha=0}^{s} d_{2\alpha} i_\alpha$ and $j = \sum_{\alpha=0}^{s} d_{2\alpha} j_\alpha$ be elements of I such that $\Delta(\omega^i B \cdot H^{(q-1)/e}) \cap \Delta(\omega^j B \cdot H^{(q-1)/e}) \neq \varnothing$. In such a case by (3.1.e) we have: $\omega^i H^{(q-1)/(2e)} \cdot L_B \cap \omega^j H^{(q-1)/(2e)} \cdot L_B \neq \varnothing$. Thus there exist $x, y \in L_B$ such that $\omega^i H^{(q-1)/2e} x = \omega^j H^{(q-1)/2e} y$, i.e.:

$$\omega^{i-j} \in H^{(q-1)/(2e)} x^{-1} y \text{ with } x, y \in L_B. \tag{3.1.f}$$

Suppose $i \neq j$ and show that such an assumption leads to a contradiction. Let β be the least integer such that $i_\beta \neq j_\beta$; then (3.1.f) can be written as follows:

$$\Pi_{\beta \le \alpha \le s} \omega^{d_{2\alpha}(i_\alpha - j_\alpha)} \in H^{(q-1)/(2e)} x^{-1} y \text{ with } x, y \in L_B. \tag{3.1.g}$$

The group $H^{d_{2\beta}}$ contains both $H^{(q-1)/(2e)}$ and $\omega^{d_{2\alpha}}$ for any $\alpha \ge \beta$. This, together with (3.1.g), gives $x^{-1}y \in H^{d_{2\beta}}$. Then, by (3.1.d), $x^{-1}y$ is also in $H^{d_{2\beta+1}}$ because the intersection between $(H^{d_{2\beta}} \setminus H^{d_{2\beta+1}})$ and $(H^{d_{2\alpha-1}} \setminus H^{d_\alpha})$ is obviously empty for any $\alpha \in \{1, \dots, s\}$. Thus, considering (3.1.g) again, we infer that $\omega^{d_{2\beta}(i_\beta - j_\beta)} \in H^{d_{2\beta+1}}$, i.e. $\omega^{(i_\beta - j_\beta)} \in H^{d_{2\beta+1}/d_{2\beta}}$. Hence $d_{2\beta+1}/d_{2\beta}$ divides $|i_\beta - j_\beta|$ which is smaller than $d_{2\beta+1}/d_{2\beta}$ by definition of I. It follows that $i_\beta = j_\beta$, a contradiction.

The family $\mathcal{F}$ satisfies condition (1.6.c):

The size of $\mathcal{F}$ is equal to the cardinality of I which is t by (3.1.c). On the other hand we have $\left\lfloor \frac{q-1}{k^2-k} \right\rfloor$ by (3.1.a). ■

Remarks 3.2. **(i)** The reason for which in (3.1.a) r is required to be divisible by $2et$ (it seems that only divisibility by $2e$ is necessary to prove Theorem 3.1) is in order that there be compatibility with (3.1.c). In fact if (3.1.c) holds, then solving it for d_{2s+1} we get: $d_{2s+1} = (q-1)/(2e) = t \cdot (\Pi_{1 \le \alpha \le s} d_{2\alpha}/d_{2\alpha-1})$ so that $2et$ is a divisor of $q-1$ and hence of r.

(ii) Set $m = (q-1)/(2et)$. The most simple way of applying Throrem 3.1, is to look for a f-subset B of H such that:

$$\text{any two elements of } L_B \text{ are in distinct cosets of } H^m. \tag{3.2.a}$$

In fact if (3.2.a) holds, then conditions (3.1.b, c, d) are verified in the case of the trivial chain $H \supseteq H^m$. In this case the description of the difference family is more easy (cf. Section 4).

(iii) With considerations as those made for *radical difference families* in [9, Remark 11], it is possible to show that conditions (3.1.b, c, d) are equivalent to condition (3.2.a) when m and t are coprime.

However, for $GCD(m, t) \neq 1$, conditions (3.1.b, c, d) are actually weaker than (3.2.a). For instance, the radical difference families presented in [7, 9] are all obtainable with (3.1.b, c, d) but not by means of (3.2.a). Another example where (3.2.a) fails while (3.1.b,c,d) succeed is the (577, 9, 1)-DF obtainable as follows: represent $k = 9$ in the form $k = ef$ with

Table 1. $(p, 7, 1)$ difference families with $p < 4000$.

p	B	p	B	p	B	p	B
337	{1}	1303	{1, 6}	2521	{1, 119}	3361	{1, 61}
421	{1}	1429	{1, 168}	2647	{1, 291}	3529	{1, 265}
463	{1}	1723	{1, 138}	2689	{1, 156}	3571	{1, 9}
631	{1, 19}	1933	{1}	2731	{1, 100}	3613	{1, 178}
883	{1}	2017	{1, 29}	2857	{1, 87}	3697	{1, 159}
967	{1, 306}	2143	{1, 139}	3067	{1}	3739	{1, 342}
1009	{1, 69}	2269	{1, 85}	3109	{1, 18}	3823	{1, 41}
1051	{1, 96}	2311	{1, 105}	3319	{1}	3907	{1, 108}
1093	{1, 6}	2437	{1, 39}				

$e = f = 3$. With respect to this representation and using the chain $H \supset H^6 \supset H^{12} \supset H^{24}$, the list $L_{\{1,8,208\}}$ from $GF(577)$ satisfies (3.1.b, c, d).

(iv) Any theorem of Section 2 can be obtained as a corollary of Theorem 3.1. For instance, for $e = 1$ and $r = 0$, condition (3.2.a) coincides with Wilson's lemma on blocks with evenly distributed differences.

(v) By the previous remark and using Wilson's asymptotic existence theorem we have that for any fixed k Theorem 3.1 leads, at least in theory, to an infinite class of $(EA(q), k, 1)$-DFs.

On the contrary, for any fixed k, Theorem 3.1 leads to a finite number of $(EA(q), k, 1)$-OOOCs which are not DFs. In fact (3.1.a) gives: $r \leq k(k-1) - 2(r \neq k(k-1) - 1$ because r is even) and hence when $r \neq 0$, as $2t$ divides $r, t \leq \frac{1}{2}r \leq \frac{1}{2}k(k-1) - 1$. In conclusion: $q < \frac{1}{2}(k^2 - k)^2$.

(vi) Of course, the number of representations of an integer k in the form $k = ef$ or $k = ef + 1$ with e odd, is the sum of the number of odd divisors of k and the number of odd divisors of $k - 1$. This sum is minimum and equal to 3 when k is a Mersenne prime or a power of 2 preceded by a prime. Therefore we meet the greatest difficulty in applying Thm. 3.1 to these values of k.

4. Applying Theorem 3.1

Now, we show the power of Theorem 3.1 by applying it in the simplest way—i.e. checking the possible validity of condition (3.2.a) with the aid of a computer—in order to give some tables of DFs and OOOCs. Each table refers to a fixed value of k; p denotes a prime and B a subset of $GF(p)$; the consequent $(p, k, 1)$-DF or OOOC is

$$\{\omega^{mi} B \cdot H^{(p-1)/e} \cup B^* \mid 0 \leq i < t\} \text{ where :}$$

e is the only odd integer in $\{k/|B|, (k-1)/|B|\}$; $B^* = \emptyset$ or $B^* = \{0\}$ according to which $e = k/|B|$ or $e = (k-1)/|B|$ resp.; t is $\lfloor \frac{(p-1)}{k^2-k} \rfloor$ and m is $(p-1)/(2et)$.

Firstly note that by Theorem 2.5 the construction of $(p, 3, 1)$-DFs is trivial. For tables of $(p, k, 1)$-DFs with $k \in \{4, 5\}$ cf. [8]. A table of $(p, 6, 1)$-DFs can be found in [28, p. 46].

About Table 2 we point out that it is an abbreviation of a longer one—omitted to save space—where we continue as far as $p < 10^5$. In both these tables the only missing admissible primes are 433, 577 and 1009. Since a $(577, 9, 1)$-DF has been constructed in

Table 2. $(p, 9, 1)$ difference families with $p < 5000$.

p	B	p	B	p	B
73	$\{1\}$	2089	$\{1, 63, 145\}$	3313	$\{1, 16, 210\}$
937	$\{1, 14, 80\}$	2161	$\{1, 28, 968\}$	3457	$\{1, 45, 60\}$
1153	$\{1\}$	2377	$\{1, 129, 275\}$	3529	$\{1, 26, 181\}$
1297	$\{1, 167, 264\}$	2521	$\{1, 2, 265\}$	3673	$\{1, 28, 1372\}$
1657	$\{1, 11, 198\}$	2593	$\{1, 15, 163\}$	3889	$\{1, 33, 377\}$
1801	$\{1, 63, 154\}$	2953	$\{1, 29, 41\}$	4177	$\{1, 17, 1082\}$
1873	$\{1\}$	3169	$\{1, 20, 217\}$	4969	$\{1, 116, 987\}$
2017	$\{1\}$				

Table 3. $(p, 10, 1)$ difference families with $p < 8000$.

p	B	p	B	p	B
1171	$\{1, 31, 409\}$	3691	$\{1, 306\}$	6211	$\{1, 468\}$
1621	$\{1, 68, 704\}$	4051	$\{1, 76, 1397\}$	6301	$\{1, 244\}$
2521	$\{1, 42, 469\}$	4231	$\{1, 683\}$	6571	$\{1, 16, 41\}$
2791	$\{1, 253, 448\}$	4591	$\{1, 43, 2201\}$	6661	$\{1, 223\}$
2971	$\{1, 23, 568\}$	4861	$\{1, 61\}$	6841	$\{1, 644, 1487\}$
3061	$\{1, 178, 1471\}$	5581	$\{1, 125, 930\}$	7561	$\{1, 16, 3552\}$
3331	$\{1, 126, 415\}$	5851	$\{1, 1277\}$	7741	$\{1, 229\}$
3511	$\{1, 687\}$	6121	$\{1, 145\}$		

Table 4. $(p, 11, 1)$ difference families with $p < 30000$.

p	B	p	B	p	B	p	B
10781	$\{1, 1350\}$	14851	$\{1, 783\}$	21011	$\{1, 800\}$	23761	$\{1, 536\}$
12211	$\{1, 2684\}$	15401	$\{1, 2136\}$	21341	$\{1, 205\}$	24091	$\{1, 5742\}$
12541	$\{1, 725\}$	16061	$\{1, 1229\}$	22111	$\{1\}$	24971	$\{1, 1474\}$
14081	$\{1, 961\}$	19031	$\{1, 2422\}$	22441	$\{1, 1869\}$	25411	$\{1, 596\}$
14411	$\{1, 2090\}$	19141	$\{1, 1134\}$	23321	$\{1, 1322\}$	27611	$\{1, 416\}$
14741	$\{1, 452\}$						

Remark 3.2(iii), we may conclude that the existence of a cyclic $S(2, 9, p)$ design of prime order $p < 10^5$ is undecided only for $p \in \{433, 1009\}$.

Recall that the task of constructing at least a non-trivial Steiner 2-design with block size k is easy when k is equal or subsequent to a prime power q. In fact in these cases we have the affine or projective spaces over the field $GF(q)$. The first value of k for which it is rather difficult to construct a non-trivial $S(2, k, v)$ is 15: the only non-trivial $S(2, 15, v)$ that the author knows with $v < 10^5$ was found by Wilson by means of his Theorem 2.5 and has 76231 points. In table 5 several other (cyclic) $S(2, 15, v)$ designs are indirectly exhibited.

In the introduction it has already been remarked that any simple difference family is also an optimal optical ortogonal code; tables 6–11 refer to OOOCs which are not DFs with at least two codeword-sets and are obtainable with Theorem 3.1.

Two wide classes of OOOCs with Hamming-weight 4 and 5 and which are not DFs have recently been constructed using finite fields by S. Bitan and T. Etzion (cfr. [3], Thm 6 and Thm 9).

Table 5. $(p, 15, 1)$ difference families with $p < 10^5$.

p	B	p	B	p	B
13441	{1, 214, 837}	72661	{1, 2431}	89671	{1, 4397}
45361	{1, 632, 8778}	76231	{1}	93871	{1, 2305}
66571	{1, 120, 6355}	80221	{1, 14398}	97231	{1, 11176}
71821	{1, 488, 1100}				

Table 6. $(p, 4, 1)$ OOOCs which are not DFs.

p	B	p	B	p	B
29	{1, 2, 4, 12}	43	{1, 2, 4, 12}	71	{1, 2, 4, 28}

Table 7. $(p, 5, 1)$ OOOCs which are not DFs.

p	B	p	B	p	B
53	{1, 2, 4, 10, 14}	79	{1, 2, 4, 10, 29}	97	{1, 2, 5, 12, 25}
67	{1, 2, 4, 12, 54}	89	{1, 2, 4, 10, 42}	199	{1, 2, 4, 8, 83}
73	{1, 2, 4, 8, 30}				

Table 8. $(p, 6, 1)$ OOOCs which are not DFs.

p	B	p	B
73	{1, 2}	193	{1, 2, 4, 12, 19, 46}
89	{1, 2, 4, 8, 13, 32}	239	{1, 2, 4, 9, 37, 138}
97	{1, 2, 4, 8, 25, 67}	257	{1, 2, 7, 16, 51, 110}
103	{1, 2, 4, 8, 32, 44}	353	{1, 2, 4, 8, 47, 103}
109	{1, 2, 4, 8, 22, 78}	449	{1, 2, 4, 10, 242, 395}
137	{1, 2, 4, 9, 37, 48}		

Table 9. $(p, 7, 1)$ OOOCs which are not DFs.

p	B	p	B
97	{1, 2, 4, 8, 21, 29, 62}	157	{1, 2, 4, 8, 19, 35, 105}
101	{1, 2, 4, 8, 25, 54, 91}	163	{1, 10}
109	{1, 2, 4, 8, 23, 64, 81}	193	{1, 57}
113	{1}	277	{1, 2, 4, 8, 56, 83, 100}
139	{1, 2, 10, 55, 70, 113, 117}	661	{1, 2, 10, 69, 221, 613, 659}
151	{1, 2, 30, 51, 65, 111, 124}		

Table 10. $(p, 9, 1)$ OOOCs which are not DFs.

p	B	p	B	p	B
181	{1}	337	{1, 9, 25}	547	{1, 25, 147}
193	{1, 10, 64}	421	{1, 19, 204}	859	{1, 6, 369}
271	{1, 2, 6}				

Table 11. $(p, 10, 1)$ OOOCs which are not DFs.

p	B	p	B	p	B
241	{1, 9}	401	{1, 37}	601	{1, 42}
307	{1, 3, 7}	433	{1}	769	{1, 8, 176}
331	{1, 3}				

Acknowledgements

The author wishes to thank Sara Bitan and Tuvi Etzion for having brought to his attention their results on OOOCs, and Marilisa Carosi for her valuable computing work.

Added in Proof

Note that Theorem 3.1, in the case $r = 0$, can be found in a slightly different form in M. Greig, Some Balanced Incomplete Block Design Constructions, *Congressus Numerantium*, vol. 77 (1990) pp. 121–134.

References

1. Beth, T., Jungnickel, D., and Lenz, H. 1993. *Design Theory*. Cambridge University Press, Cambridge.
2. Bitan, S., and Etzion, T. 1993. The last packing number of quadruples and cyclic SQS. *Designs, Codes and Cryptography* 3(4):283–313.
3. Bitan, S., and Etzion, T. 1993. Constructions for optimal constant weight cyclically permutable codes and difference families. Submitted to *IEEE Transactions of Information Theory*.
4. Bose, R. C. 1939. On the construction of balanced incomplete block designs. *Ann. Eugenics* 9:353–399.
5. Brickell, E. F., and Wei, V. K. 1987. Optical orthogonal codes and cyclic block designs. *Congressus Numerantium* 58:175–192.
6. Buratti, M. 1993a. Problemi e risultati sulle famiglie differenza. *Sem. Geom. Comb. Dip. Mat. Universitá di Roma "La Sapienza"*, Quaderno n. 108.
7. Buratti, M. 1993b. Improving two theorems of Bose on difference families. To appear in *Journal of Combinatorial Designs*.
8. Buratti, M. 1993c. Constructions of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$. To appear in the *Proceedings of the 14th British Combinatorial Conference*.
9. Buratti, M. 1993d. On simple radical difference families. To appear in the *Journal of Combinatorial Designs*.
10. Cameron, P. J., and Lint van, J. H. 1980. *Graphs, Codes and Designs*. London Math. Soc. Lecture Notes 43. Cambridge University Press, Cambridge.
11. Chung, H., and Kumar, P. V. 1990. Optical orthogonal codes—new bounds and an optimal construction. *IEEE Transactions of Information Theory* 36(4):866–872.
12. Chung, F. R. K., Salehi, J. A., and Wei, V. K. 1989. Optical orthogonal codes: design, analysis and applications. *IEEE Transactions of Information Theory* 35(3):595–604.
13. Colbourn, C. J., and Colbourn, M. J. 1984. Recursive constructions for cyclic block designs. *J. Statist. Plann. Infer.* 10:97–103.
14. Colbourn, M. J., and Mathon, R. 1980. On cyclic Steiner 2-designs. *Ann. Discrete Math.* 7:215–253.
15. Dembowski, P. 1968. *Finite Geometries*. Springer, Berlin-Heidelberg-New York.
16. Furino, S. 1991. Difference families from rings. *Discrete Math.* 97:177–190.
17. Grannell, M. J., and Griggs, T. S. 1984. Product constructions for cyclic block designs I. Steiner quadruple systems. *J. Combin. Theory Ser. A* 36:56–65.
18. Grannell, M. J., and Griggs, T. S. 1986. Product constructions for cyclic block designs II. Steiner 2-designs. *J. Combin. Theory Ser. A* 42:179–183.
19. Hall, M., Jr. 1986. *Combinatorial Theory*, 2nd ed. J. Wiley & Sons, New York.
20. Hanani, H. 1975. Balanced incomplete block designs and related designs. *Discrete Math.* 11:255–369.
21. Hughes, D. R., and Piper, F. C. 1988. *Design Theory*. Cambridge University Press, Cambridge.
22. Jimbo, M., and Kuriki, S. 1983. On a composition of cyclic 2-designs. *Discrete Math.* 46:249–255.
23. Jungnickel, D. 1978. Composition theorems for difference families and regular planes. *Discrete Math.* 23:151–158.
24. Lehmer, E. 1953. On residue difference sets. *Canad. J. Math.* 5:425–432.

25. Mathon, R. 1987. Constructions for cyclic Steiner 2-designs. *Ann. Discrete Math.* 34:353–362.

26. Phelps, K. T. 1987. Isomorphism problems for cyclic block designs. *Ann. Discrete Math.* 34:385–392.

27. Tallini, G. 1993. Composizioni di disegni. *Sem. Geom. Comb. Dip. Mat. Universitá di Roma "La Sapienza"*, Quaderno n. 109.

28. Wilson, R. M. 1972a. Cyclotomy and difference families in elementary abelian groups. *J. Number Theory* 4:17–42.

29. Wilson, R. M. 1972b. An existence theory for pairwise balanced designs I. Composition theorems and morphisms. *J. Combin. Theory Ser. A* 13:220–245.

30. Wilson, R. M. 1972c. An existence theory for pairwise balanced designs II. The structure of PBD-closed sets and the existence conjectures. *J. Combin. Theory Ser. A* 13:246–273.

31. Wilson, R. M. 1975. An existence theory for pairwise balanced designs, III. Proof of the existence conjectures. *J. Combin. Theory Ser. A* 18:71–79.