On New Families of Supplementary Difference Sets over Rings with Short Orbits

Marc Gysin and Jennifer Seberry*

Centre for Computer Security Research,
Department of Computer Science,
The University of Wollongong,
Wollongong, NSW 2500, Australia

Dedicated to Anne Penfold Street.

Abstract

We discuss difference sets (DS) and supplementary difference sets (SDS) over rings. We survey some constructions of SDS over Galois rings where there are no short orbits. From there we move to constructions which involve short orbits. These give rise to new infinite families of SDS over $GF(p) \times GF(q)$, p, q both prime powers. Many of these families have $\lambda = 1$.

We also show some new balanced incomplete block designs and pairwise balanced designs arising from the constructions given here.

1 Introduction

The methods and techniques in this paper have been inspired by many authors including Dokovic [3], Furino [5], Hunt and Wallis [7] and Storer [16]. We use these methods and further generalisations to find many new infinite families of SDS.

Definition 1 (Supplementary Difference Sets) Let $S_1, S_2, \ldots, S_e$ be subsets of Z_v (or any finite abelian group of order v) containing $k_1, k_2, \ldots, k_e$

*Research supported by the Centre for Computer Security Research, ARC Large Grant 223261006 and a University of Wollongong Postgraduate Research Scholarship

elements respectively. Let T_i be the totality of all differences between elements of S_i (with repetitions), and let T be the totality of all the elements of T_i. If T contains each non–zero element of Z_v a fixed number of times, say λ, then the sets will be called e–$\{v; k_1, k_2, \ldots, k_e; \lambda\}$ *supplementary difference sets (SDS).*

The parameters of e–$\{v; k_1, k_2, \ldots, k_e; \lambda\}$ supplementary difference sets satisfy

$$\lambda(v-1) = \sum_{i=1}^{e} k_i(k_i - 1). \tag{1}$$

If $k_1 = k_2 = \ldots = k_e = k$ we shall write e–$\{v; k; \lambda\}$ to denote the e SDS and (1) becomes

$$\lambda(v-1) = ek(k-1).$$

If $e = 1$, then we will denote the SDS as a $\{v; k; \lambda\}$ *difference set (DS)* rather than a $1 - \{v; k; \lambda\}$ SDS.

The rest of this paper is organised as follows. Section 2 gives an introduction to cyclotomy and basic theorems. Section 3 gives some recursive constructions. None of the constructions in Sections 2 and 3 are new. Sections 4, 5 and 6 present new constructions. Section 4 gives a further generalisation of previous results. Section 5 presents a construction yielding supplementary difference sets with short orbits. Section 6 develops further some of the Stanton–Sprott–Whiteman constructions. Finally, in Section 7, we give some new pairwise balanced designs (PBD) and balanced incomplete block designs (BIBD) arising from the previous sections.

2 Cyclotomy

We give a short introduction to cyclotomy. More details are given in [4] and [12]. None of the theorems presented in this section is new.

Definition 2 Let x be a primitive element of $F = GF(q)$, where $q = p^\alpha = ef + 1$ is a prime power. Write $F^* =< x >$. The *cyclotomic classes (or cosets) C_i in F* are:

$$C_i = \{x^{es+i} : s = 0, 1, \ldots, f-1\},\ i = 0, 1, \ldots, e-1.$$

We note that the C_i's are pairwise disjoint and their union is $F^* = F \setminus \{0\}$.

Notation 1 Let $A = \{a_1, a_2, \ldots, a_k\}$ be a k–set; then we will use ΔA for the collection of differences between distinct elements of A, i.e,

$$\Delta A = [a_i - a_j : i \neq j, 1 \leq i, j \leq k].$$

Note that

$$\Delta C_i = C_{i_1} \cup \ldots \cup C_{i_{f-1}},$$

where $0 \leq i_k \leq e-1$ and the i_k's are not necessarily distinct. Also observe that the classes C_i have a multiplicative structure. That is, [1]

$$x^{i_{plus}} \times C_i = C_{i+i_{plus}},$$

and, together with the distributive law,

$$\begin{aligned} \Delta C_{i+i_{plus}} &= x^{i_{plus}} \times C_{i_1} \cup \ldots \cup x^{i_{plus}} \times C_{i_{f-1}} \\ &= C_{i_1+i_{plus}} \cup \ldots \cup C_{i_{f-1}+i_{plus}}. \end{aligned}$$

Now,

$$\begin{aligned} \bigcup_{i=0}^{e-1} \Delta C_i &= \bigcup_{i_{plus}=0}^{e-1} \Delta C_{i+i_{plus}} \\ &= \bigcup_{i_{plus}=0}^{e-1} C_{i_1+i_{plus}} \cup \ldots \cup \bigcup_{i_{plus}=0}^{e-1} C_{i_{f-1}+i_{plus}} \\ &= \bigcup_{i=0}^{e-1} C_i \cup \ldots \cup \bigcup_{i=0}^{e-1} C_i \\ &= (f-1)F^*. \end{aligned}$$

Therefore, we have the following theorem.

Theorem 1 *Let $q = p^\alpha = ef+1$, x, $C_0, \ldots, C_{e-1}$ be defined as above. Then*

$$C_0, \ldots, C_{e-1} \text{ are } e - \{q; f; f-1\} \text{ SDS}.$$

Theorem 1 can be generalised (see, for example, [17]):

Theorem 2 *Let $S_0 = C_{k_1} \cup \ldots \cup C_{k_t}$, $k_i \neq k_j$ for $i \neq j$, $S_m = C_{k_1+m} \cup \ldots \cup C_{k_t+m}$, $t \leq e$. Now*

$$S_0, \ldots, S_{e-1} \text{ are } e - \{q; tf; t(tf-1)\} \text{ SDS}.$$

Proof. Note that

$$\Delta(C_i \cup C_j) = \Delta C_i \cup \Delta(C_i - C_j) \cup \Delta(C_j - C_i) \cup \Delta C_j,$$

[1] If $i + i_{plus} \geq e$, then $i + i_{plus}$ has to be reduced mod e. In the remainder of this paper, we will not indicate when indexes have to be reduced, except for some very special cases which require some further considerations.

where

$$\Delta(C_a - C_b) = [c_a - c_b : c_a \in C_a,\ c_b \in C_b].$$

Similarly to the above we can now write

$$\Delta(C_i \cup C_j) = \bigcup_{s=1}^{f-1} C_{a_s} \cup \bigcup_{s=1}^{f} C_{b_s} \cup \bigcup_{s=1}^{f} C_{c_s} \cup \bigcup_{s=1}^{f-1} C_{d_s};$$

and;

$$\begin{aligned} \bigcup_{m=0}^{e-1} \Delta(C_{i+m} \cup C_{j+m}) &= \ldots \\ \ldots &= (4f-2)F^*. \end{aligned}$$

as above. It can now be easily shown that

$$\bigcup_{m=0}^{e-1} \Delta S_m = \bigcup_{m=0}^{e-1} \Delta(C_{i_1+m} \cup \ldots \cup C_{i_t+m}) = t(tf-1)F^*.$$

□

For q being an odd prime power we define $-1 = x^{\frac{q-1}{2}} = x^{\frac{ef}{2}}$. For odd f, we have $\frac{ef}{2} = e(\frac{f-1}{2}) + \frac{e}{2}$, so $-1 \in C_{\frac{e}{2}}$. Therefore,

$$\begin{aligned} (-1) \times C_k &= (-1) \times \{x^{es+k} : s = 0, \ldots, f-1\} \\ &= \{x^{e(\frac{f-1}{2})+\frac{e}{2}} x^{es+k} : s = 0, \ldots, f-1\} \\ &= \{x^{es+k+\frac{e}{2}} : s = 0, \ldots, f-1\} \\ &= C_{k+\frac{e}{2}}. \end{aligned}$$

Similarly, for $S_m = C_{i_1+m} \cup \ldots \cup C_{i_t+m}$,

$$(-1) \times S_k = S_{k+\frac{e}{2}}.$$

The differences arising from C_k and $(-1) \times C_k$ must be the same, similarly for S_k and $(-1) \times S_k$, Therefore, we get the following theorem.

Theorem 3 *Let $q = ef + 1$ be an odd prime power and let f be odd. Now in Theorems 1 and 2:*

$$\begin{aligned} C_0, \ldots, C_{\frac{e}{2}-1} \quad &are \quad \frac{e}{2} - \{q; f; \frac{f-1}{2}\}\ SDS\ ; \\ S_0, \ldots, S_{\frac{e}{2}-1} \quad &are \quad \frac{e}{2} - \{q; tf; \frac{t(tf-1)}{2}\}\ SDS\ . \end{aligned}$$

Note that we could also have chosen any configuration, for example, $C_0, C_{\frac{e}{2}+1}, C_2, \ldots, C_{e-1}$ instead of $C_0, \ldots, C_{\frac{e}{2}-1}$. There are a total of $2^{\frac{e}{2}}$ independent choices of either C_k or $C_{k+\frac{e}{2}}$ for the above $\frac{e}{2} - \{q; f; \frac{f-1}{2}\}$ SDS . Similarly for S_k and $S_{k+\frac{e}{2}}$. Hence, there are many[2] nonisomorphic SDS for either case in Theorem 3.

Another standard construction for SDS is obtained by adding the element $\{0\}$ to each set C_j or S_j in Theorems 1 to 3. Observe that for any set D

$$\Delta(D \cup \{0\}) = \Delta D \cup D \cup (-1) \times D.$$

Theorem 4 *From Theorems 1 to 3 and by adding the element* $\{0\}$ *to each set* C_j *or* S_j*, respectively, we get*

$$\begin{aligned}
&e - \{q; f+1; f+1\}\ SDS\,,\\
&e - \{q; tf+1; t(tf+1)\}\ SDS\,,\\
&\frac{e}{2} - \{q; f+1; \frac{f+1}{2}\}\ SDS\,,\\
&\frac{e}{2} - \{q; t(f+1); \frac{t(tf+1)}{2}\}\ SDS\,.
\end{aligned}$$

3 Supplementary Difference Sets without Short Orbits

In this section we show how we can construct SDS over cross products of Galois fields (also called Galois rings) and over Z_{p^α} by similar constructions as given above. None of the constructions and the SDS in this section are new and they are, for example, covered by a more general construction given in [5] but the approach and (the sketch of) the proof of Theorem 5 here are different from the constructions given in [5]. Other similar constructions are given in [1], [8] and [10].

Definition 3 Let $p_1, \ldots, p_n$ be prime powers and let f be a factor of each $p_i - 1$. Let $e_i = \frac{p_i - 1}{f}$ and x_i be a primitive element of $GF(p_i)$. Let $\ell_i \in \{\Omega\} \cup \{(j, m) : 0 \le j \le \frac{p_i - 1}{f} - 1, 0 \le m \le f-1\}$, $i = 1, \ldots, n$. Then we define *the classes* $C_{\ell_1, \ell_2, \ldots, \ell_n}$ as

$$C_{\ell_1, \ell_2, \ldots, \ell_n} = \{(r_1(s), r_2(s), \ldots, r_n(s)) : s = 0, \ldots, f-1\},$$

[2]This construction gives us $2^{\frac{e}{2}}$ $\frac{e}{2} - \{q; f; \frac{f-1}{2}\}$ SDS . But not all of these SDS are nonisomorphic, for example, if $e = 4$, then C_0, C_2 and C_1, C_3 are isomorphic SDS since one can be obtained from one another by multiplying all the classes with the same fixed element.

where

$$r_i(s) = \begin{cases} 0 & \ell_i = \Omega \\ x_i^{e_i(s+m)+j} & \ell_i = (j,m) \end{cases}$$

$\ell_i \in \{(j,m) : 0 \leq j \leq \frac{p_i-1}{f} - 1, 1 \leq m \leq f-1\}$ will *not be defined* if all $\ell_k = \Omega$, for $k = 0, \ldots, i-1$.

We shall also be concerned with *different types* of class $C_{\ell_1,\ell_2,\ldots,\ell_n}$. We define two classes $C_{\ell_{11},\ell_{21},\ldots,\ell_{n1}}$ and $C_{\ell_{12},\ell_{22},\ldots,\ell_{n2}}$ to be *of a different type*, if there is at least one i such that $\ell_{i1} = \Omega$ and $\ell_{i2} \neq \Omega$ or vice versa; otherwise the classes are to be defined *of the same type.*

Observe that for any n, the totality of all the defined classes $C_{\ell_1,\ldots,\ell_n}$ are a partition of $\{(1,\ldots,1),\ldots,(p_1-1,\ldots,p_n-1)\}$. The total number of different types of class is $2^n - 1$ (if we do not count the class $C_{\Omega,\Omega,\ldots,\Omega} = \{0\}$).

Theorem 5 *Let $p_1, \ldots, p_n$ be prime powers. Let f be a factor of each $p_i - 1$, let $e_i = \frac{p_i-1}{f}$ and x_i be a primitive element of $GF(p_i)$.*

(i)

$$C_{\ell_1,\ldots,\ell_n} \text{ are } \frac{p_1 \times \ldots \times p_n - 1}{f} - \{p_1 \times \ldots \times p_n; f; f-1\} \text{ SDS},$$

for all defined $\ell_1, \ldots, \ell_n$.

(ii) There are $\phi(f)^{n-1}$ nonisomorphic such SDS depending on the initial choices of the primitive elements x_i, $i = 1, \ldots, n$.

(iii) Furthermore, if all p_i's are odd and f is odd, then there are many nonisomorphic $\frac{p_1 \times \ldots \times p_n - 1}{2f} - \{p_1 \times \ldots \times p_n; f; \frac{f-1}{2}\}$ SDS for each of the SDS in (ii).

Proof. We only sketch how to prove (i) to (iii).
(i): It can be shown that the totality of differences arising from one type of class generate this type of class $f-1$ times. That is

$$\bigcup_{\text{same type of class}} \Delta C_{\ell_1,\ldots,\ell_n} = (f-1) \bigcup_{\text{same type of class}} C_{\ell_1,\ldots,\ell_n},$$

and this will complete this part of the proof, since all the classes are a partition of $\{(1,\ldots,1),\ldots,(p_1-1,\ldots,p_n-1)\}$.
(ii): If $n = 1$, then $\phi(f)^{n-1} = 1$. That is, the SDS in this case does not depend on the choice of the primitive element x_1. If, however, $n \geq 2$, then the classes depend on the choice of the primitive elements x_i, $i \geq 2$. For

each p_i, $i \geq 2$ there are $\phi(p_i - 1)$ primitive elements of which $\phi(f)$ will lead to another nonisomorphic set of classes. There are a total of $n-1$ independent such choices, therefore, we have $\phi(f)^{n-1}$ such SDS.
(iii): If all p_i's are odd and f is odd, then $(-1) = (-1, \ldots, -1)$ will not be in $C_{(0,0),\ldots,(0,0)}$. So there are two classes, $C_{(0,0),\ldots,(0,0)}$ and $(-1) \times C_{(0,0),\ldots,(0,0)}$ which generate the same differences. Similarly for all other classes $C_{\ell_1,\ldots,\ell_n}$. Hence, half of the classes must generate all the differences and there are a total of $\frac{p_1 \times \ldots \times p_n - 1}{2f}$ independent choices of either $C_{\ell_1,\ldots,\ell_n}$ or $(-1) \times C_{\ell_1,\ldots,\ell_n}$ to form $\frac{p_1 \times \ldots \times p_n - 1}{2f} - \{p_1 \times \ldots \times p_n; f; \frac{f-1}{2}\}$ SDS. □

Theorems 2 to 4 can now be extended similarly.

Theorem 6 *Let p_i, e_i, x_i, f be as above. Let $t \leq min\{e_i : 1 \leq i \leq n\}$. For each different type of class now define*

$$S_{start} = \bigcup_{i=1}^{t} C_{\ell_{1i},\ldots,\ell_{ni}}$$

such that, for each $\alpha \neq \beta$ and $1 \leq k \leq n$, if $\ell_{k\alpha} = (j_\alpha, m_\alpha)$ and $\ell_{k\beta} = (j_\beta, m_\beta)$, then $j_\alpha \neq j_\beta$.

If we now let all the S_{start}'s "cycle through", then we have

$$\frac{p_1 \times \ldots \times p_n - 1}{f} - \{p_1 \times \ldots \times p_n; tf; t(tf-1)\}\ SDS\,.$$

Theorem 7 *If, in Theorem 6, all p_i's are odd and f is odd, then there are also*

$$\frac{p_1 \times \ldots \times p_n - 1}{2f} - \{p_1 \times \ldots \times p_n; tf; \frac{t(tf-1)}{2}\}\ SDS\,,$$

obtained by taking either $S_{start+k}$ or $(-1) \times S_{start+k}$ for each k and each different type of class.

Theorem 8 *In Theorems 5 to 7 we obtain*

$$\frac{p_1 \times \ldots \times p_n - 1}{f} - \{p_1 \times \ldots \times p_n; f+1; f+1\}\ SDS\,,$$

$$\frac{p_1 \times \ldots \times p_n - 1}{f} - \{p_1 \times \ldots \times p_n; tf+1; t(tf+1)\}\ SDS\,,$$

$$\frac{p_1 \times \ldots \times p_n - 1}{2f} - \{p_1 \times \ldots \times p_n; f+1; \frac{f+1}{2}\}\ SDS\,,$$

$$\frac{p_1 \times \ldots \times p_n - 1}{2f} - \{p_1 \times \ldots \times p_n; tf+1; \frac{t(tf+1)}{2}\}\ SDS\,,$$

by adding the element $\{0\}$ to each of the initial sets, in Theorems 5 to 7, respectively.

Clearly, all the above constructions work for $p_1, \ldots, p_n$ being pairwise distinct primes. We then have

$$\begin{aligned} GF(p_1) \times \ldots \times GF(p_n) &\simeq Z_{p_1} \times \ldots \times Z_{p_n} \\ &\simeq Z_{p_1 \times \ldots \times p_n}. \end{aligned}$$

We now turn briefly to SDS over Z_{p^α}. The next theorem corresponds to Lemma 4.3 in [5].

Theorem 9 *Let p be an odd prime and x be an element of Z_{p^α} such that x has multiplicative order $p^\alpha - p^{\alpha-1}$. Let f be a factor of $p-1$. Let*

$$C_{z,\ell_z} = \{p^z x^{\frac{p^{\alpha-z}-p^{\alpha-z-1}}{f}s+\ell_z} : s = 0, \ldots, f-1\},$$

$z = 0, \ldots, \alpha-1$, $\ell_z = 0, \ldots, \frac{p^{\alpha-z}-p^{\alpha-z-1}}{f} - 1$.

(i)

$$C_{z,\ell_z} \text{ are } \frac{p^\alpha - 1}{f} - \{p^\alpha; f; f-1\} \text{ SDS over } Z_{p^\alpha},$$

for z, ℓ_z running through the above ranges.

(ii) The number of nonisomorphic SDS in (i) is one.

(iii) Furthermore, if f is odd, then there are many nonisomorphic $\frac{p^\alpha-1}{2f} - \{p^\alpha; f; \frac{f-1}{2}\}$ SDS.

The constructions in Theorems 2 to 4 can now be applied very similarly. We do not state the theorems here. However, we would like to mention that combinations of SDS over cross products of Galois fields and Z_{p^α} are possible. In Theorems 5 and 9 two classes, say C_j over G_1 and C_k over G_2, could always be expressed as

$$\begin{aligned} C_j &= \{y_1 x_1^{c_1 s+j} : s = 0, \ldots, f-1\}, \\ C_k &= \{y_2 x_2^{c_2 s+k} : s = 0, \ldots, f-1\}. \end{aligned} \tag{2}$$

Any two such classes give immediately rise to f new classes, say $C_{j,k,m}$ over $G_1 \times G_2$, which can be expressed as

$$C_{j,k,m} = \{(y_1 x_1^{c_1 s+j}, y_2 x_2^{c_2(s+m)+k}) : s = 0, \ldots, f-1\}$$

for $m = 0, \ldots, f-1$.

Suppose that the C_j's are a partition of G_1 and the C_k's are a partition of G_2. If now the totality of the C_j's form $\frac{v_1-1}{f} - \{v_1; f; f-1\}$ SDS over G_1, that is,

$$\bigcup_j \Delta C_j = (f-1)\bigcup_j C_j$$

and the totality of the C_k's form $\frac{v_2-1}{f} - \{v_2; f; f-1\}$ SDS over G_2, that is,

$$\bigcup_k \Delta C_k = (f-1)\bigcup_k C_k,$$

then

$$\begin{aligned} C_{j,k,m} &= \{(y_1 x_1^{c_1 s+j}, y_2 x_2^{c_2(s+m)+k}) : s = 0, \ldots, f-1\} \\ D_k &= \{(0, y_2 x_2^{c_2 s+k}) : s = 0, \ldots, f-1\} \\ E_j &= \{(y_1 x_1^{c_1 s+j}, 0) : s = 0, \ldots, f-1\} \end{aligned}$$

are $\frac{v_1 v_2 - 1}{f} - \{v_1 v_2; f; f-1\}$ SDS over $G_1 \times G_2$, since,

$$\begin{aligned} \bigcup_{j,k,m} \Delta C_{j,k,m} &= (f-1) \bigcup_{j,k,m} C_{j,k,m} \\ \bigcup_k \Delta D_k &= (f-1)\bigcup_k D_k \\ \bigcup_j \Delta E_j &= (f-1)\bigcup_j E_j. \end{aligned}$$

Furthermore, the $C_{j,k,m}$'s, D_k's and E_j's are a partition of $G_1 \times G_2$.

It is clear that the above construction can be applied recursively. The constructions from Theorems 2 to 4 may now be applied accordingly.

The theorems given in the above sections produce infinite families of SDS. For a given v the above constructions may lead to different groups. For example, if $v = 25$, then we may consider SDS over

$$\begin{aligned} &GF(25), \text{ or} \\ &Z_5 \times Z_5 \simeq GF(5) \times GF(5), \text{ or} \\ &Z_{25}. \end{aligned}$$

If, in the above constructions, we call $C_{(0,0),\ldots,(0,0)}$, $C_{0,0_0}$ or $C_{0,0,0}$ "the first class", then in Theorems 5 and 9 all the SDS are defined by "second element" in the first class. That is, the whole structure is defined by

$$x = (x_1^{\frac{\phi(|G_1|)}{f}}, \ldots, x_n^{\frac{\phi(|G_n|)}{f}}), \tag{3}$$

where G_i are the different groups involved, x_i is a generator of the units of G_i $(i = 1, \ldots, n)$ and $|G_i|$ is the order of the group G_i.

We also would like to point out that the first class is a[3] subgroup of the units in $G_1 \times \ldots \times G_n$. All the other classes are the orbits of this subgroup. All the orbits and the subgroup have the same order, that is, there are no short orbits. This is due to the construction and (3) which assures that $x^f = (1, 1, \ldots, 1)$ and $x^i = (u_1, \ldots, u_n)$ with $u_k \neq 1$, $(k = 1, \ldots, n)$ for $2 \leq i \leq f - 1$.

4 A More General Construction

The construction in Theorem 10 is similar to Theorem 5. However, the construction here is more general. This generalisation is completely different from the constructions in [5]. A construction using a similar idea for cyclic block designs has been given in [1].

Theorem 10 *Suppose* $C_0, \ldots, C_{e-1}$ *are*

$$e - \{v; f_0, \ldots, f_{e-1}; \lambda\} \text{ SDS over } G;$$

and suppose there is a prime power q *with* $f_i | (q-1)$ *for all* $0 \leq i \leq e-1$. *Furthermore, suppose that* $(\lambda + 1) | (q - 1)$.

Let x *be a primitive element of* $GF(q)$ *and let* $c_{j,s}$ *be the* s*-th element*[4] *in set* C_j. *Let*

$$\begin{aligned} C_{j,\ell} &= \{(c_{j,s}, x^{\frac{q-1}{f_j}s+\ell}) : s = 0, \ldots, f_j - 1\} \\ D_k &= \{(0, x^{\frac{q-1}{\lambda+1}s+k}) : s = 0, \ldots, \lambda\} \\ E_j &= \{(c_{j,s}, 0) : s = 0, \ldots, f_j - 1\}, \end{aligned}$$

where $j = 0, \ldots, e-1$, $k = 0, \ldots, \frac{q-1}{\lambda+1} - 1$, $\ell = 0, \ldots, q-2$.

Now

$C_{j,\ell}, D_k, E_j$ *are* $(eq + \frac{q-1}{\lambda+1})-$
$\{vq; f_0, f_0, \ldots, f_{e-1}, f_{e-1}, \lambda+1, \ldots, \lambda+1, f_0, \ldots, f_{e-1}; \lambda\}$ *SDS over* $G \times GF(q)$,

for j, k, ℓ *running through the above ranges.*

[3]Because there may be more than one way to construct the first class (Theorem 5) we say "a subgroup" and not "the subgroup".

[4]Note that "the order" within the sets C_i may be chosen completely arbitrarily.

Proof.

$$\bigcup_{j=0}^{e-1} \Delta E_j = \lambda \bigcup_{g \in G^*} (g, 0),$$

due to the assumption; and;

$$\bigcup_{k=0}^{\frac{q-1}{\lambda+1}-1} \Delta D_k = \lambda \bigcup_{y \in GF(q)^*} (0, y),$$

due to cyclotomy and the construction. Also

$$\bigcup_{j=0}^{e-1} \Delta C_{j,0} = \bigcup_{k=0}^{\lambda|G^*|-1} (g_k, x^{u_k}),$$

such that $\bigcup_{k=0}^{\lambda|G^*|-1} g_k = \lambda G^*$.

Now

$$\begin{aligned} \bigcup_{j=0}^{e-1} \bigcup_{\ell=0}^{q-2} \Delta C_{j,\ell} &= \bigcup_{k=0}^{\lambda|G^*|-1} \bigcup_{\ell=0}^{q-2} (g_k, x^{u_k+\ell}) \\ &= \lambda \bigcup_{g \in G^*} \bigcup_{y \in GF(q)^*} (g, y), \end{aligned}$$

which completes the proof. □

Corollary 1 *The above construction also works if*

$$\begin{aligned} (\lambda - 1) &\mid (q - 1), \\ (2\lambda + 1) &\mid (q - 1),\ q \textit{ being odd} \\ (2\lambda - 1) &\mid (q - 1),\ q \textit{ being odd.} \end{aligned}$$

Proof. The standard constructions in cyclotomy given above give rise to SDS over $GF(q)$ with $\lambda = f + 1, \frac{f-1}{2}, \frac{f+1}{2}$, where f is the size of the sets. Therefore, for the construction of the D_k's, we have to let $f = \lambda - 1, 2\lambda + 1, 2\lambda - 1$, respectively, and this f must divide $q - 1$. □

Corollary 2 *Suppose there are $\{v; f; \lambda\}$ SDS over G and $\{q; f; \lambda\}$ SDS over $GF(q)$, q a prime power and $f|(q-1)$, then there are $\{vq; f; \lambda\}$ SDS over $G \times GF(q)$.*

Proof. Follows directly from the construction and by embedding the $\{q; f; \lambda\}$ SDS over $GF(q)$ in $G \times GF(q)$ yielding the D_k's. □

Corollary 3 *Suppose* $C_0, \ldots, C_{e-1}$ *are*

$$e - \{v; f; \lambda\} \text{ SDS over } G;$$

and suppose there is a prime power q *with* $f|(q-1)$. *Furthermore, suppose that* $\lambda|(f-1)$.

Let x *be a primitive element of* $GF(q)$ *and let* $c_{j,s}$ *be the* s*-th element in set* C_j. *Let*

$$\begin{aligned} C_{j,\ell} &= \{(c_{j,s}, x^{\frac{q-1}{f}s+\ell}) : s = 0, \ldots, f-1\} \\ D_k &= \{(0, x^{\frac{q-1}{f}s+k}) : s = 0, \ldots, f-1\} \\ E_j &= \{(c_{j,s}, 0) : s = 0, \ldots, f-1\}, \end{aligned}$$

where $j = 0, \ldots, e-1$, $k = 0, \ldots, \frac{q-1}{f} - 1$, $\ell = 0, \ldots, q-2$.

Now

$\frac{f-1}{\lambda}$ *copies of* $C_{j,\ell}, E_j$ *and one copy of* D_k *are* $(eq\frac{f-1}{\lambda} + \frac{q-1}{f})-\{vq; f; f-1\}$ *SDS over* $G \times GF(q)$,

for j, k, ℓ *running through the above ranges.*

Proof. Follows directly from Theorem 10 and the construction. □

Theorem 10 and its corollaries lead to infinite families of SDS. Note that due to Corollary 1 may more than one construction be possible (for example, if $q = 13$ and $\lambda = 3$). Theorem 5 is a special case of Corollary 2.

In the above section constructions of SDS over Z_{p^α} are given. Similarly, we can now extend SDS via Z_{p^α}.

Theorem 11 *Suppose* $C_0, \ldots, C_{e-1}$ *are*

$$e - \{v; f_0, \ldots, f_{e-1}; \lambda\} \text{ SDS over } G;$$

and suppose there is a prime p *with* $f_i|(p-1)$ *for all* $0 \leq i \leq e-1$. *Furthermore, suppose that* $(\lambda+1)|(p-1)$.

Let x be an element of Z_{p^α} such that x has multiplicative order $p^\alpha - p^{\alpha-1}$ and let $c_{j,s}$ be the s-th element in set C_j. Let

$$\begin{aligned} C_{j,z,\ell_z} &= \{(c_{j,s}, p^z x^{\frac{p^{\alpha-z}-p^{\alpha-z-1}}{f_j}s+\ell_z}) : s = 0,\ldots,f_j-1\} \\ D_{z,k_z} &= \{(0, p^z x^{\frac{p^{\alpha-z}-p^{\alpha-z-1}}{\lambda+1}s+k_z}) : s = 0,\ldots,\lambda\} \\ E_j &= \{(c_{j,s}, 0) : s = 0,\ldots,f_j-1\}, \end{aligned}$$

where $j = 0,\ldots,e-1$, $k_z = 0,\ldots,\frac{p^{\alpha-z}-p^{\alpha-z-1}}{\lambda+1} - 1$, $z = 0,\ldots,\alpha-1$, $\ell_z = 0,\ldots,p^{\alpha-z}-p^{\alpha-z-1}-1$.

Now

> *$C_{j,z,\ell_z}, D_{z,k_z}, E_j$ are $(ep^\alpha + \frac{p^\alpha-1}{\lambda+1})-$ $\{vp^\alpha; f_0, f_0, \ldots, f_{e-1}, f_{e-1}, \lambda+1, \ldots, \lambda+1, f_0, \ldots, f_{e-1}; \lambda\}$ SDS over $G \times Z_{p^\alpha}$,*

for j, k_z, z, ℓ_z running through the above ranges.

Proof. Similarly to Theorem 10: The proof follows from Theorem 9 and the construction. □

Remark 1 Similarly to the above, the construction also works if

$$\begin{aligned} (\lambda-1) &\mid (p-1), \\ (2\lambda+1) &\mid (p-1), \\ (2\lambda-1) &\mid (p-1). \end{aligned}$$

The constructions from Corollaries 2 or 3 may be applied.

Example 1 $C_0 = \{1,5,25,8\}$, $C_1 = \{2,10,11,16\}$, $C_2 = \{4,20,22,32\}$, $C_3 = \{13,26\}$ are $4 - \{39; 4,4,4,2; 1\}$ SDS over Z_{39}. The construction in Theorem 10 now yields:

> $22 - \{195; 4,4,4,4,4,4,4,4,4,4,4,4,4,2,2,2,2,2,2,2,4,4,4,2; 1\}$
> SDS over $Z_{39} \times GF(5) \simeq Z_{195}$,
> $40 - \{351; 4,\ldots,\ldots,2,2,2,2,4,4,4,2; 1\}$ SDS over $Z_{39} \times GF(3^2)$,
> $58 - \{507; 4,\ldots,\ldots,2,2,2,2,2,2,4,4,4,2; 1\}$
> SDS over $Z_{39} \times GF(13)$,

and there are many other SDS possible.

Example 2 The sets $\{1,12,8,5\}$, $\{10,3,11,2\}$, $\{4,6,7,9\}$ are $3-\{13;4;3\}$ SDS over $GF(13)$. (Note that "the order" within the sets has been chosen arbitrarily.) We now extend these SDS via $GF(5)$. Let

$$\begin{aligned}
C_{0,0} &= \{(1,1),(12,2),(8,4),(5,3)\} = \{1,12,34,18\},\\
C_{1,0} &= \{(10,1),(3,2),(11,4),(2,3)\} = \{36,42,24,28\},\\
C_{2,0} &= \{(4,1),(6,2),(7,4),(9,3)\} = \{56,32,59,48\},\\
D_0 &= \{(0,1),(0,2),(0,4),(0,3)\} = \{26,52,39,13\},\\
E_0 &= \{(1,0),(12,0),(8,0),(5,0)\} = \{40,25,60,5\},\\
E_1 &= \{(10,0),(3,0),(11,0),(2,0)\} = \{10,55,50,15\},\\
E_2 &= \{(4,0),(6,0),(7,0),(9,0)\} = \{30,45,20,35\},
\end{aligned}$$

and let $C_{j,\ell} = (1,2^\ell) \times C_{j,0}$, for $j = 0,\ldots,2$, $\ell = 0,\ldots,3$. Now $C_{j,\ell}$, D_0, E_0, E_1, E_2 are $16-\{65;4;3\}$ SDS over $GF(13) \times GF(5) \simeq Z_{65}$. These SDS are nonisomorphic to the ones arising from Theorem 5 or given in [5] because the elements in the classes arising from $GF(13)$ have "been shuffled" before the $C_{j,\ell}$ were constructed. There are many other nonisomorphic such SDS, since, for fixed j, there are $\frac{f!}{f} = (f-1)!$ ways to construct the $C_{j,\ell}$'s.

Example 3 Section 10.6 in [2] gives $\{v;4;1\}$ SDS for $v = 49,85$. We extend these SDS via $GF(13)$ and let $D = \{(0,0),(0,1),(0,3),(0,9)\}$ (note that $\{0,1,3,9\}$ is a $\{13;4;1\}$ DS, Corollary 2), $C_{j,\ell}$ and E_j as in Theorem 10. We now have $\{r;4;1\}$ SDS for

$$r = 637, 1105,$$

over Z_r.

Example 4 The set $\{0,1,3,9\}$ is a $\{13;4;1\}$ DS over $GF(13)$. We extend these SDS via $\{1,7,24,18\}$, $\{2,14,23,11\}$, $\{4,3,21,22\}$, $\{8,6,17,19\}$, $\{16,12,9,13\}$, $\{5,10,20,15\}$ which are $6-\{25;4;3\}$ SDS over Z_{5^2}. We get

$$\begin{aligned}
C_{0,0,0_0} &= \{(0,1),(1,7),(3,24),(9,18)\} = \{26,157,224,243\},\\
C_{0,0,\ell_0} &= (1,2)^{\ell_0} \times C_{0,0,0_0} = 27^{\ell_0} \times C_{0,0,0_0},\\
C_{0,1,0_1} &= \{(0,5),(1,10),(3,20),(9,15)\} = \{130,235,120,165\},\\
C_{0,1,\ell_1} &= (1,2)^{\ell_1} \times C_{0,1,0_1} = 27^{\ell_1} \times C_{0,1,0_1},\\
D_{0,0_0} &= \{(0,1),(0,24)\} = \{26,299\},\\
D_{0,k_0} &= (2,2)^{k_0} \times D_{0,0_0} = 2^{k_0} \times D_{0,0_0},\\
D_{1,0_1} &= \{(0,5),(0,20)\} = \{130,195\},\\
D_{1,k_1} &= (2,2)^{k_1} \times D_{1,0_1} = 2^{k_1} \times D_{1,0_1},\\
E_0 &= \{(0,0),(1,0),(3,0),(9,0)\} = \{0,300,250,100\}.
\end{aligned}$$

Now for $\ell_0 = 0,\ldots,19$, $\ell_1 = 0,\ldots,3$, $k_0 = 0,\ldots,9$, $k_1 = 0,1$, $C_{0,0,\ell_0}$, $C_{0,1,\ell_1}$, D_{0,k_0}, D_{1,k_1}, E_0 are $37-\{325;4,4,\ldots,\ldots,2,2;1\}$ SDS over $GF(13)\times Z_{5^2} \simeq Z_{325}$.

Corollary 4 *Suppose $n = p^\alpha$ is a prime power and q is an odd prime power. Suppose $(n+1)|(q-1)$. Then we get*

$$(q + \frac{q-1}{2}) - \{q(n^2+n+1); n+1,\ldots,2,n+1;1\} \text{ SDS}$$

over $Z_{n^2+n+1} \times GF(q)$.

Proof. Cyclic projective planes exist for every order $n = p^\alpha$ (Singer), see, for example, [6] or [11]. Therefore, we have a $\{v;k;\lambda\}$ DS with

$$v = n^2+n+1,\ k = n+1,\ \lambda = 1.$$

Theorem 10 gives us the desired SDS. □

Corollary 5 *Suppose $n = p^\alpha$ is a prime power and q is a prime. Suppose $(n+1)|(q-1)$. Then we get*

$$(q^\alpha + \frac{q^\alpha - 1}{2}) - \{q^\alpha(n^2+n+1); n+1,\ldots,2,n+1;1\} \text{ SDS}$$

over $Z_{n^2+n+1} \times Z_{q^\alpha}$, for $\alpha \geq 1$.

Proof. As Corollary 4 but now via Theorem 11. □

5 Supplementary Difference Sets with Short Orbits

Theorem 12 *Let $\ell \geq 1$ be a number such that $\ell+2$ is a prime power. Let q be a prime power with $q \equiv 1 \bmod (\ell+1)^2$. Let x_ℓ and x_q generate $GF(\ell+2)^*$ and $GF(q)^*$, respectively. Let*

$$\begin{aligned} C_j &= \{(x_\ell^s, x_q^{\frac{q-1}{(\ell+1)^2}s+j}) : s = 0,\ldots,(\ell+1)^2-1\} \\ E &= \{(x_\ell^s, 0) : s = 0,\ldots,\ell\} \end{aligned}$$

for $j = 0,\ldots,\frac{q-1}{\ell+1}-1$.

Now the C_j's plus $\ell+1$ copies of E are

$$(\frac{q-1}{\ell+1}+\ell+1)-$$
$$\{(\ell+2)q;(\ell+1)^2,\ldots,(\ell+1)^2,\ell+1,\ldots,\ell+1;\ell(\ell+1)\}\ SDS\,,$$

over $GF(q)\times GF(\ell+2)$, for j running through the above range.

Proof. We define

$$D_k=\{(0,x_q^{\frac{q-1}{(\ell+1)^2}s+k}):s=0,\ldots,(\ell+1)^2-1\},$$

for $k=0,\ldots,\frac{q-1}{(\ell+1)^2}-1$.

We have

$$\begin{aligned}\Delta C_0 &= D_{k_1}\cup\ldots\cup D_{k_\ell}\cup\\ &\quad C_{j_1}\cup\ldots\cup C_{j_{(\ell+1)^2-\ell-1}},\end{aligned}$$

where $0\le k_i\le\frac{q-1}{(\ell+1)^2}-1$, $0\le j_i\le\frac{q-1}{\ell+1}-1$. The classes have a multiplicative structure, so

$$\begin{aligned}(1,x_q^{j_{plus}})\times C_0 &= C_{j_{plus}},\\ \Delta C_{j_{plus}} &= D_{k_1+j_{plus}}\cup\ldots\cup D_{k_\ell+j_{plus}}\cup\\ &\quad C_{j_1+j_{plus}}\cup\ldots\cup C_{j_{(\ell+1)^2-\ell-1}+j_{plus}}.\end{aligned}$$

Therefore,

$$\begin{aligned}\bigcup_{j_{plus}=0}^{\frac{q-1}{\ell+1}-1}\Delta C_{j_{plus}} &= \bigcup_{j_{plus}=0}^{\frac{q-1}{\ell+1}-1}D_{k_1+j_{plus}}\cup\ldots\cup\bigcup_{j_{plus}=0}^{\frac{q-1}{\ell+1}-1}D_{k_\ell+j_{plus}}\cup\\ &\quad\bigcup_{j_{plus}=0}^{\frac{q-1}{\ell+1}-1}C_{j_1+j_{plus}}\cup\ldots\cup\bigcup_{j_{plus}=0}^{\frac{q-1}{\ell+1}-1}C_{j_{(\ell+1)^2-\ell-1}+j_{plus}}\\ &= \ell\bigcup_{k=0}^{\frac{q-1}{\ell+1}-1}D_k\cup((\ell+1)^2-\ell-1)\bigcup_{j=0}^{\frac{q-1}{\ell+1}-1}C_j\\ &= \ell(\ell+1)\bigcup_{k=0}^{\frac{q-1}{(\ell+1)^2}-1}D_k\cup\ell(\ell+1)\bigcup_{j=0}^{\frac{q-1}{\ell+1}-1}C_j.\end{aligned}$$

Also

$$\Delta E=\ell E,$$

so

$$(\ell+1)\Delta E = \ell(\ell+1)E,$$

and the proof is complete. □

Example 5 Let $\ell = 3$ and $q = 17$ (note that $17 \equiv 1 \bmod 16$). Let $(x_\ell, x_q) = (2,5) = 22$. Now

$$\begin{aligned} C_0 &= \{1,22,59,23,81,82,19,78,16,12,9,28,21,37,49,58\}, \\ C_1 &= \{56,42,74,13,31,2,44,33,46,77,79,38,71,32,24,18\}, \\ C_2 &= \{76,57,64,48,36,27,84,63,26,62,4,3,66,7,69,73\}, \\ C_3 &= \{6,47,14,53,61,67,29,43,11,72,54,83,41,52,39,8\}, \\ E &= \{51,17,34,68\}, \end{aligned}$$

and $C_0, C_1, C_2, C_3, E, E, E, E$ are $8 - \{85; 16,16,16,16,4,4,4,4; 12\}$ SDS over $GF(17) \times GF(5) \simeq Z_{85}$.

Note that ℓ odd implies $\ell + 2$ and q odd. That is, -1 exists. Now $-1 = (-1,-1) = (x_\ell^{\frac{\ell+1}{2}}, x_q^{\frac{q-1}{2}})$ is not in C_0 which can be easily shown. That is, $(-1) \times C_0 \neq C_0$. But the differences generated from ΔC_0 and $\Delta(-C_0)$ must be the same. Since this applies for every class C_j, we can take only half of the classes in Theorem 12 to get SDS. We have the following corollary.

Corollary 6 *If, in Theorem 12, ℓ is odd, then there are also*

$$\left(\frac{q-1}{2(\ell+1)} + \frac{\ell+1}{2}\right) - \{(\ell+2)q; (\ell+1)^2, \ldots, (\ell+1)^2, \ell+1, \ldots, \ell+1; \ell\frac{\ell+1}{2}\} \text{ SDS},$$

over $GF(q) \times GF(\ell+2)$.

Example 6 In Example 5, C_0, C_1, E, E are

$$4 - \{85; 16,16,4,4; 6\} \text{ SDS}$$

over Z_{85}.

Example 7 Let $\ell = 1$ and $q = 5$ (note that $5 \equiv 1 \bmod 4$). In this case the constructions in Theorem 12 *and* Corollary 6 work and the SDS in Corollary 6 are given by

$$\begin{aligned} C_0 &= \{(1,1),(2,2),(1,4),(2,3)\} = \{1,2,4,8\} \\ E &= \{(1,0),(2,0)\} = \{10,5\}. \end{aligned}$$

Now C_0, E are $2-\{15;4,2;1\}$ SDS over $GF(5)\times GF(3)\simeq Z_{15}$.

Let $\ell=1$ and $q=13$ (note that $13\equiv 1 \bmod 4$). In this case the constructions in Theorem 12 *and* Corollary 6 work and the SDS in Corollary 6 are given by

$$\begin{aligned} C_0 &= \{(1,1),(2,8),(1,12),(2,5)\} = \{1,8,25,5\} \\ C_1 &= \{(1,2),(2,3),(1,11),(2,10)\} = \{28,29,37,23\} \\ C_2 &= \{(1,4),(2,6),(1,9),(2,7)\} = \{4,32,22,20\} \\ E &= \{(1,0),(2,0)\} = \{13,26\}. \end{aligned}$$

Now C_0, C_1, C_2, E are $4-\{39;4,4,4,2;1\}$ SDS over $GF(13)\times GF(3)\simeq Z_{39}$.

Let $\ell=1$ and $q=17$ (note that $17\equiv 1 \bmod 4$). In this case the constructions in Theorem 12 *and* Corollary 6 work and the SDS in Corollary 6 are given by

$$\begin{aligned} C_0 &= \{(1,1),(2,13),(1,16),(2,4)\} = \{1,47,16,38\} \\ C_1 &= \{(1,5),(2,14),(1,12),(2,3)\} = \{22,14,46,20\} \\ C_2 &= \{(1,8),(2,2),(1,9),(2,15)\} = \{25,2,43,32\} \\ C_3 &= \{(1,6),(2,10),(1,11),(2,7)\} = \{40,44,28,41\} \\ E &= \{(1,0),(2,0)\} = \{34,17\}. \end{aligned}$$

Now C_0, C_1, C_2, C_3, E are $5-\{51;4,4,4,4,2;1\}$ SDS over $GF(17)\times GF(3)\simeq Z_{51}$.

Note that C_0 is again a subgroup of the units of $GF(\ell+2)\times GF(q)$. The other classes are all orbits of this subgroup. But this time we have one short orbit, that is, one class with less elements than C_0, which is E.

6 Twin Prime Power Constructions

Stanton, Sprott, Storer and Whiteman, see, for example, [15], [16] or [18], showed constructions of DS over $GF(p)\times GF(p+2)$, with p, $p+2$ both prime powers. We give very similar constructions here which give new families of SDS.

Theorem 13 *Let p, $p+2$ be two prime powers $p>2$. Let x, y generate $GF(p)^*$, $GF(p+2)^*$, respectively. Let $f=\frac{p^2-1}{2}=lcm(p-1,p+1)$. Let*

$$\begin{aligned} C_i &= \{(x^s, y^{s+i}) : s=0,\ldots,f-1\} \\ E_k &= \{(x^{\frac{p-1}{2}s+k}, 0) : s=0,1\}, \end{aligned}$$

where $i = 0, 1$, $k = 0, \ldots, \frac{p-1}{2} - 1$. *Then* C_0, $E_0, \ldots, E_{\frac{p-1}{2}-1}$ *are*

$$\frac{p+1}{2} - \{p(p+2); \frac{p^2-1}{2}, 2, \ldots, 2; \frac{(p-1)^2}{4}\} \text{ SDS}$$

over $GF(p) \times GF(p+2)$.

Proof. Define $E = \{(x^s, 0) : s = 0, \ldots, p-2\}$, $D = \{(0, y^s) : s = 0, \ldots, p\}$. Note that C_0, C_1, D, E are a partition of $(GF(p) \times GF(p+2)) \setminus \{0\}$. ΔC_0 generates $\frac{(p-1)^2}{2}$ classes C_{i_k}, $i_k = 0, 1$, $\frac{(p-1)^2}{4}$ times D and $\frac{(p-1)^2}{4} - 1$ times E, which follows directly from the construction (by counting "the number of hits from ΔC_0" in each of the classes C_0, C_1, D, E and taking into account the length, that is, the number of elements in each class). Observe that

$$\bigcup_{k=0}^{\frac{p-1}{2}-1} \Delta E_k = E.$$

It now only remains to prove that half of the i_k's are 0 (and the other half therefore 1). Note that

$$-1 \times C_0 = (-1, -1) \times C_0 = (x^{\frac{p-1}{2}}, y^{\frac{p+1}{2}}) \times C_0 = C_1,$$

since $(x^{\frac{p-1}{2}}, y^{\frac{p+1}{2}}) = (x^{\frac{p-1}{2}}, y^{\frac{p-1}{2}+1}) \in C_1$. But

$$\Delta C_0 = \Delta(-C_0) = \Delta C_1.$$

Hence, half of the C_{i_k}'s generated by ΔC_0 are C_0's and the other half are C_1's. □

Remark 2 The only reason why the E_k's in Theorem 13 are needed is because ΔC_0 does not generate enough E's (namely $\frac{(p-1)^2}{4} - 1$ instead of $\frac{(p-1)^2}{4}$). Therefore, the class E has to be generated once more via the ΔE_k's.

Remark 3 The SDS in Corollary 6 and Theorem 13 for the case $GF(3) \times GF(5) \simeq Z_{15}$ are the same.

We restate the theorem of Stanton, Sprott [15] and Whiteman [18] and reprove it by simply counting the differences generated by $\Delta\{C_0 \cup E \cup \{0\}\}$.

Theorem 14 (Stanton–Sprott–Whiteman restated) *Let* C_0, E *be defined as above, then* $\{C_0 \cup E \cup \{0\}\}$ *is a*

$$\{p(p+2); \frac{p^2-1}{2} + p; \frac{(p+1)^2}{4} - 1\} \text{ DS}$$

over $GF(p) \times GF(p+2)$.

Proof. We know that

$$\Delta\{C_0 \cup E \cup \{0\}\} =$$
$$\Delta C_0 \cup \Delta E \cup \Delta(C_0 - E) \cup \Delta(E - C_0) \cup C_0 \cup -C_0 \cup E \cup -E =$$
$$\frac{(p-1)^2}{4}(C_0 \cup C_1) \cup \frac{(p-1)^2}{4} D \cup (\frac{(p-1)^2}{4} - 1)E$$
$$\cup (p-2)E \cup \Delta(C_0 - E) \cup \Delta(E - C_0) \cup C_0 \cup C_1 \cup 2E.$$

We have to examine $\Delta(C_0 - E)$ and $\Delta(E - C_0)$. Again by counting "the number of hits from $\Delta(C_0 - E)$" we find that $\Delta(C_0 - E)$ generates $\frac{p-1}{2}$ D's and $(p-2)$ C_{i_k}'s. Similarly, $\Delta(E - C_0)$ generates $\frac{p-1}{2}$ D's and $(p-2)$ $(-C_{i_k})$'s.

Therefore, $(C_0 \cup C_1)$ is generated

$$\frac{(p-1)^2}{4} + p - 2 + 1 = \frac{(p+1)^2}{4} - 1$$

times. The class D is generated

$$\frac{(p-1)^2}{4} + p - 1 = \frac{(p+1)^2}{4} - 1$$

times. And, finally, the class E is generated

$$\frac{(p-1)^2}{4} - 1 + p - 2 + 2 = \frac{(p+1)^2}{4} - 1$$

times. □

Corollary 7 *Let C_0, D be defined as above, then $\{C_0 \cup D\}$ is a*

$$\{p(p+2); \frac{(p+1)^2}{2}; \frac{(p+1)^2}{4}\}\ DS$$

over $GF(p) \times GF(p+2)$.

Proof. The complement of $\{C_0 \cup E \cup \{0\}\}$ is $\{C_1 \cup D\}$ which is a DS. But $\Delta\{C_1 \cup D\} = \Delta - \{C_1 \cup D\} = \Delta\{C_0 \cup D\}$. Hence, $\{C_0 \cup D\}$ is a DS with the above parameters. □

Example 8 Let $p = 5$, $p + 2 = 7$, $(x, y) = (2, 3) = 17$. Now

$$\begin{aligned} C_0 &= \{1, 17, 9, 13, 11, 12, 29, 3, 16, 27, 4, 33\} \\ D &= \{15, 10, 30, 20, 25, 5\} \\ E &= \{21, 7, 14, 28\} \\ E_0 &= \{21, 14\} \\ E_1 &= \{7, 28\}, \end{aligned}$$

and C_0, E_0, E_1 are $3 - \{35; 12, 2, 2; 4\}$ SDS. Furthermore,

$$\{C_0 \cup E \cup \{0\}\} = \{1, 17, 9, 13, 11, 12, 29, 3, 16, 27, 4, 33, 21, 7, 14, 28, 0\},$$

which is a $\{35; 17; 8\}$ DS; and;

$$\{C_0 \cup D\} = \{1, 17, 9, 13, 11, 12, 29, 3, 16, 27, 4, 33, 15, 10, 30, 20, 25, 5\},$$

which is a $\{35; 18; 9\}$ DS. All the SDS and DS are over $GF(5) \times GF(7) \simeq Z_{35}$.

The above theorems motivate us to find other pairs of prime powers p, $p+a$ (a now greater than 2) with $gcd(p-1, p+a-1) = 2$ to construct DS and SDS in a similar manner. However, some calculations show that DS and SDS as in the above theorems are only possible for $a = 2$. If $a > 2$, then the set D (the zeroes in p) will be generated too many times.

A more successful approach is to drop the condition $gcd(p-1, p+a-1) = 2$. That is, we let $g = gcd(p-1, p+a-1)$ and try to find appropriate conditions about a and g.

Theorem 15 *Let p, $q = (g-1)p + 2$ be two prime powers $p > 2$, where $g = gcd(p-1, q-1)$. Let x, y generate $GF(p)^*$ and $GF(q)^*$, respectively. Let $f = \frac{(p-1)(q-1)}{g} = lcm(p-1, q-1)$. Let*

$$\begin{aligned} C_i &= \{(x^s, y^{s+i}) : s = 0, \ldots, f-1\} \\ E &= \{(x^s, 0) : s = 0, \ldots, p-2\}, \end{aligned}$$

where $i = 0, \ldots, g-1$. Then $\{C_0 \cup E \cup \{0\}\}, \ldots, \{C_{\frac{g}{2}-1} \cup E \cup \{0\}\}$ are

$$\frac{g}{2} - \{pq; \frac{(p-1)(q-1)}{g} + p; \lambda\} \text{ SDS}$$

over $GF(p) \times GF(q)$, where

$$\lambda = \frac{pq - 1 - g}{2g}.$$

Proof. Similarly to the proof above (Theorem 14). The construction also involves the fact that $-1 = (-1, -1) = (x^{\frac{p-1}{2}}, y^{\frac{q-1}{2}}) \in C_{\frac{g}{2}}$. Therefore, we only need the classes $\{C_0 \cup E \cup \{0\}\}$ to $\{C_{\frac{g}{2}-1} \cup E \cup \{0\}\}$ to generate the SDS. But $-1 \in C_{\frac{g}{2}}$ can be easily proven by showing that $\frac{q-1-(p-1)}{2} \equiv \frac{g}{2} \bmod g$. □

The above theorem and construction are very similar to Theorem II.1 in Storer [16]. This theorem was originally due to Whiteman [18]. However, in Storer DS are constructed, while Theorem 15 gives SDS. The case $g = 2$ is of course Theorem 14.

Example 9 Let $p = 5$, $g = 4$. Now $q = 3p + 2 = 17$ is a prime power. Also $gcd(4, 16) = 4 = g$. Let $x = 2$ and $y = 5$. Now

$$\begin{aligned}\{C_0 \cup E \cup \{0\}\} &= \{1, 22, 59, 23, 81, 82, 19, 78, 16, 12, 9, 28, 21, 37, 49, 58, \\ &\quad 0, 51, 17, 34, 68\} \\ \{C_1 \cup E \cup \{0\}\} &= \{56, 42, 74, 13, 31, 2, 44, 33, 46, 77, 79, 38, 71, 32, 24, 18, \\ &\quad 0, 51, 17, 34, 68\},\end{aligned}$$

and $\{C_0 \cup E \cup \{0\}\}$, $\{C_1 \cup E \cup \{0\}\}$ are $2 - \{85; 21; 10\}$ SDS.

We close the section by pointing out the similarity of Theorem 12 to Theorem 15 for $q = (\ell+1)^2 + 1$. If we denote the other prime in Theorem 12 by p, then $p = \ell + 2$. Now $g = gcd(p-1, q-1) = \ell + 1$ and $q = (g-1)p + 2$. The classes C_0 in either theorems are now the same (if we take the same generators of $GF(p)^*$ and $GF(q)^*$). The whole construction is now very similar. Taking only half of the classes (Theorem 15) corresponds of course to Corollary 6.

7 Balanced Incomplete Block Designs and Pairwise Balanced Designs

Definition 4 Let B be a collection of b blocks (or sets) of size k over a finite set V with v elements. If B satisfies the following conditions

(i) each element v_i occurs exactly r times;

(ii) each unordered pair (v_i, v_j) occurs in exactly λ of the b blocks;

then B is called a *balanced incomplete block design (BIBD).*

The parameters of a BIBD satisfy

$$\begin{aligned} bk &= vr, \\ \lambda(v-1) &= r(k-1). \end{aligned}$$

Since 2 of the parameters v, b, r, k, λ are redundant, we will refer to a BIBD as BIBD(v, k, λ).

If $S_0, \ldots, S_{t-1}$ are $t - \{v; f; \lambda\}$ SDS, then we may obtain $v \times t$ blocks $B_{i,j}$, where $B_{i,j}$ is obtained from S_i by adding the element j to each of the elements in S_i. It can be easily shown that the $B_{i,j}$'s are a BIBD. Therefore, we have the following theorem.

Theorem 16 *If there are $t - \{v; f; \lambda\}$ SDS, then there is a BIBD(v, f, λ).*

v	V	K	How
15	$GF(3) \times GF(5) \simeq Z_{15}$	$\{4,2\}$	Corollary 6 with $\ell = 1$
39	$GF(3) \times GF(13) \simeq Z_{39}$	$\{4,2\}$	Corollary 6 with $\ell = 1$
51	$GF(3) \times GF(17) \simeq Z_{51}$	$\{4,2\}$	Corollary 6 with $\ell = 1$
65	$GF(13) \times GF(5) \simeq Z_{65}$	$\{4,2\}$	$\{0,1,3,9\}$ and Theorem 10
75	$GF(3) \times GF(5^2)$	$\{4,2\}$	Corollary 6 with $\ell = 1$
87	$GF(3) \times GF(29) \simeq Z_{87}$	$\{4,2\}$	Corollary 6 with $\ell = 1$
111	$GF(3) \times GF(37) \simeq Z_{111}$	$\{4,2\}$	Corollary 6 with $\ell = 1$
123	$GF(3) \times GF(41) \simeq Z_{123}$	$\{4,2\}$	Corollary 6 with $\ell = 1$
147	$GF(3) \times GF(7^2)$	$\{4,2\}$	Corollary 6 with $\ell = 1$
159	$GF(3) \times GF(53) \simeq Z_{159}$	$\{4,2\}$	Corollary 6 with $\ell = 1$
183	$GF(3) \times GF(61) \simeq Z_{183}$	$\{4,2\}$	Corollary 6 with $\ell = 1$
195	$Z_{15} \times GF(13) \simeq Z_{195}$	$\{4,2\}$	Corollary 6 and Theorem 10
195	$Z_{39} \times GF(5) \simeq Z_{195}$	$\{4,2\}$	Corollary 6 and Theorem 10
217	$Z_{31} \times GF(7) \simeq Z_{217}$	$\{6,2\}$	Corollary 4 with $n = 5$
219	$GF(3) \times GF(73) \simeq Z_{219}$	$\{4,2\}$	Corollary 6 with $\ell = 1$
221	$GF(13) \times GF(17) \simeq Z_{221}$	$\{4,2\}$	$\{0,1,3,9\}$ and Theorem 10
231	$Z_{21} \times GF(11) \simeq Z_{231}$	$\{5,2\}$	Corollary 4 with $n = 4$
243	$GF(3) \times GF(3^4)$	$\{4,2\}$	Corollary 6 with $\ell = 1$
247	$GF(19) \times GF(13) \simeq Z_{247}$	$\{3,2\}$	$\{4,9,6\}, \{5,16,17\}, \{8,18,12\}$ and Theorem 10
255	$Z_{15} \times GF(17) \simeq Z_{255}$	$\{4,2\}$	Corollary 6 and Theorem 10
255	$Z_{51} \times GF(5) \simeq Z_{255}$	$\{4,2\}$	Corollary 6 and Theorem 10
325	$GF(13) \times Z_{5^2} \simeq Z_{325}$	$\{4,2\}$	$\{0,1,3,9\}$ and Theorem 11
351	$Z_{39} \times GF(3^2)$	$\{4,2\}$	Corollary 6 and Theorem 10
377	$GF(13) \times GF(29) \simeq Z_{377}$	$\{4,2\}$	$\{0,1,3,9\}$ and Theorem 10
403	$Z_{31} \times GF(13) \simeq Z_{403}$	$\{6,2\}$	Corollary 4 with $n = 5$
435	$Z_{15} \times GF(29) \simeq Z_{435}$	$\{4,2\}$	Corollary 6 and Theorem 10
481	$GF(13) \times GF(37) \simeq Z_{481}$	$\{4,2\}$	$\{0,1,3,9\}$ and Theorem 10
507	$Z_{39} \times GF(13)$	$\{4,2\}$	Corollary 6 and Theorem 10
513	$Z_{57} \times GF(3^2)$	$\{8,2\}$	Corollary 4 with $n = 7$
555	$Z_{15} \times GF(37) \simeq Z_{555}$	$\{4,2\}$	Corollary 6 and Theorem 10
615	$Z_{15} \times GF(41) \simeq Z_{615}$	$\{4,2\}$	Corollary 6 and Theorem 10
651	$Z_{21} \times GF(31) \simeq Z_{651}$	$\{5,2\}$	Corollary 4 with $n = 4$
795	$Z_{15} \times GF(53) \simeq Z_{795}$	$\{4,2\}$	Corollary 6 and Theorem 10
915	$Z_{15} \times GF(61) \simeq Z_{915}$	$\{4,2\}$	Corollary 6 and Theorem 10
1001	$Z_{91} \times GF(11) \simeq Z_{1001}$	$\{10,2\}$	Corollary 4 with $n = 9$

Table 1: Some PBD with $\lambda = 1$.

A more sophisticated construction is given in [12], Theorem 23:

Theorem 17 (Theorem 23 from [12]) *If there are* $n - \{v; f; \lambda\}$ *SDS, then there are* $BIBD(v+1, f, \alpha f(f-1))$, *for* $\alpha \geq 1$.

If there are e–$\{v; f; \lambda\}$ SDS, then there are also e–$\{v; v-f; ev - 2ef + \lambda\}$ complementary SDS. Therefore, all the above constructions also produce many complementary SDS and BIBD.

Definition 5 Let B be a collection of blocks (or sets) of sizes $k_i \in K$ over a finite set V with v elements. If each unordered pair (v_i, v_j) of elements of V occurs in exactly λ blocks, then B is called a *pairwise balanced design,* $PBD(v, K, \lambda)$.

The parameters of a PBD satisfy

$$\sum_{B_i \in B} k_i(k_i - 1) = \lambda v(v-1),$$

where k_i is the size of block B_i. A $BIBD(v, k, \lambda)$ is a $PBD(v, \{k\}, \lambda)$. Therefore, by Theorem 16, if there are $t - \{v; f; \lambda\}$ SDS, then there is a $PBD(v, \{f\}, \lambda)$.

In Table 1 we present some PBD with $\lambda = 1$ which are obtained by the above constructions. There are many other PBD possible.

8 Conclusion

Many theorems which produce infinite families of SDS (and therefore BIBD and PBD) have been given. Many of these theorems can be applied recursively without multiplying the parameter λ. Some of the constructions are very similar for certain parameters which indicates that there might be some further generalisations. The authors feel that there are many other theorems possible which shall be investigated in another paper.

References

[1] M.J. Colbourn and C.J. Colbourn, Recursive constructions for cyclic block designs, *J. Statist. Plann. Inf.*, **10** (1984), 97–103.

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

[3] D. Dokovic, Some new D-optimal designs, *Australasian J. Comb.*, to be published.

[4] A.V. Geramita and J. Seberry, Orthogonal Designs, Quadratic Forms and Hadamard Matrices (Marcel Dekker, New York–Basel, 1979).

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

[6] M. Hall Jr, Combinatorial Theory (Blaisdell Publishing Company, USA, 1967).

[7] D. Hunt and J.S. Wallis, Cyclotomy, Hadamard arrays and supplementary difference sets, *Proceedings of the Second Manitoba Conference on Numerical Mathematics*, Congressus Numerantium VII (Manitoba, 1972), 351–381.

[8] D. Jungnickel, Composition theorems for difference families and regular planes, *Discrete Mathematics*, **23** (1978), 151–158.

[9] R. Lidl and G. Pilz, *Applied Abstract Algebra*, Undergraduate Texts in Mathematics (Springer Verlag, New York, 1984).

[10] K.T. Phelps, Isomorphism problems for cyclic block designs, *Ann. Discrete Math.*, **34** (1987), 385–392.

[11] H.J. Ryser, *Combinatorial Mathematics*, Carus Mathematical Monographs, MAA, **14** (John Wiley and Sons, 1963).

[12] J. Seberry Wallis, Some remarks on supplementary difference sets, *Colloq. Math. Soc. J. Bolyai*, Hungary, **10** (1973), 1503–1526.

[13] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, *Contemporary Design Theory - a Collection of Surveys*, eds. J.Dinitz and D.R. Stinson (John Wiley and Sons, New York, 1992), 431–560.

[14] D.A. Sprott, A note on balanced incomplete block designs, *Canad. J. Math.* **6** (1965), 341–346.

[15] R.G. Stanton and D.A. Sprott, A family of difference sets, *Canad. J. Math.* **10** (1958), 73–77.

[16] T. Storer, *Cyclotomy and Difference Sets* Lectures in Advanced Mathematics **2** (Markham Publishing Company, Chicago, 1967).

[17] J. Wallis, A note on BIBD's, *J. Austral. Math. Soc.* **16**(1973), 257–261.

[18] A.L. Whiteman, A family of difference sets, *Illinois Journal of Mathematics*, **6** (1962), 107–121.

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