1999

A Unified Approach to Difference Sets with gcd(V, N) > 1

James A. Davis
University of Richmond, jdavis@richmond.edu

Jonathan Jedwab

Recommended Citation

Davis, James A., and Jonathan Jedwab. "A Unified Approach to Difference Sets with gcd(V, N) > 1." In *Difference Sets, Sequences and Their Correlation Properties*, edited by A. Pott, V. Kumaran, Tor Helleseth, and Dieter Jungnickel, 85-112. Nato Science Series C. Netherlands: Springer, 1999.

A UNIFIED APPROACH TO DIFFERENCE SETS WITH $\gcd(V, N) > 1$

JAMES A. DAVIS
Department of Mathematics and Computer Science,
University of Richmond, Virginia 23173, U.S.A.
email: `jdavis@richmond.edu`

AND

JONATHAN JEDWAB
Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford, Bristol BS34 8QZ, U.K.
email: `jij@hplb.hpl.hp.com`

Abstract. The five known families of difference sets whose parameters $(v, k, \lambda; n)$ satisfy the condition $\gcd(v, n) > 1$ are the McFarland, Spence, Davis-Jedwab, Hadamard and Chen families. We survey recent work which uses recursive techniques to unify these difference set families, placing particular emphasis on examples. This unified approach has also proved useful for studying semi-regular relative difference sets and for constructing new symmetric designs.

1. Introduction

A k-element subset D of a finite multiplicative group G of order v is called a $(v, k, \lambda; n)$*-difference set in G* provided that the multiset of "differences" $\{d_1 d_2^{-1} : d_1, d_2 \in D, d_1 \neq d_2\}$ contains each nonidentity element of G exactly λ times; we write $n = k - \lambda$. Although the parameter n need not be listed explicitly we have chosen to do so in order to emphasise its importance in the classification and construction of difference sets.

Example 1.1. $D = \{x, x^2, x^4\}$ is a $(7, 3, 1; 2)$-difference set in $\mathbb{Z}_7 = \langle x : x^7 = 1 \rangle$.

Example 1.2. $D = \{y, x, xy, xy^2, x^2y, x^3y^3\}$ is a $(16, 6, 2; 4)$-difference set in $\mathbb{Z}_4^2 = \langle x, y : x^4 = y^4 = 1 \rangle$.

A. Pott et al. (eds.), *Difference Sets, Sequences and their Correlation Properties*, 85–112.

Difference sets arise in a wide variety of theoretical and applied contexts, and for abelian groups correspond to sequences or arrays with favourable periodic autocorrelation properties, see Davis and Jedwab (1997). For a recent survey of difference sets, see Jungnickel (1992) and its updates Jungnickel and Schmidt (1997, 1998) or see Chapter VI of Beth, Jungnickel and Lenz (1999). The reader may also consult Jungnickel and Pott (1999) in this volume.

The central problem is to determine, for each parameter set $(v, k, \lambda; n)$, which groups of order v contain a difference set with these parameters. By a counting argument the parameters $(v, k, \lambda; n)$ of a difference set are related by $k(k-1) = \lambda(v-1)$. We can assume that $k \leq v/2$ because D is a $(v, k, \lambda; n)$-difference set in G if and only if the complement $G \setminus D$ is a $(v, v-k, v-2k+\lambda; n)$-difference set in G. The trivial cases $k = 0$ and $k = 1$ are usually excluded (although trivial examples can be used as the initial case of some recursive constructions). Besides these constraints, difference sets are classified into families according to further relationships between the parameters. In Jungnickel and Schmidt (1997), the known families are grouped into three classes according to their methods of construction:

1. **Singer difference sets.** This class comprises the classical Singer family (known alternatively as the Projective Geometries family) and the Gordon-Mills-Welch family. The difference sets in this class occur in cyclic groups, and are obtained from the action of a cyclic group of linear transformations on the one-dimensional subspaces of a finite field. Generalisations of the Gordon-Mills-Welch construction are considered in Xiang (1999) in this volume.
2. **Cyclotomic difference sets.** This class comprises the Paley family, the families involving residues of higher order than quadratic, and the Twin Prime Power family. The difference sets in this class occur in elementary abelian groups, or the product of two such groups, and are unions of cosets of multiplicative subgroups of a finite field.
3. **Difference sets with $\gcd(v, n) > 1$.** This class comprises the remaining five known families of difference sets, namely McFarland, Spence, Davis-Jedwab, Hadamard and Chen. The difference sets in this class "seem to prefer to live in groups with low exponent and high rank" (Jungnickel and Schmidt (1998)).

This third class, satisfying $\gcd(v, n) > 1$, has attracted a great deal of research interest and is the only one we consider here. We shall be concerned with constructive rather than nonexistence results. This survey draws heavily on the contents of Davis and Jedwab (1997, 1999).

The Hadamard family of difference sets is given by

$$(v, k, \lambda; n) = (4N^2,\ N(2N-1),\ N(N-1);\ N^2)$$

for integer $N \geq 1$ (see Davis and Jedwab (1996) for a survey and Jungnickel and Schmidt (1997, 1998) for updates). The Hadamard family derives its name from the fact that D is a Hadamard difference set if and only if the $(+1, -1)$ incidence matrix of the design corresponding to D is a Hadamard matrix with constant row sum, see Jungnickel (1992) and Turyn (1965).

The McFarland family is given by

$$\begin{aligned}&(v, k, \lambda; n)\\ &\quad = \left(q^{d+1}\left(\frac{q^{d+1}-1}{q-1}+1\right),\, q^{d}\left(\frac{q^{d+1}-1}{q-1}\right),\, q^{d}\left(\frac{q^{d}-1}{q-1}\right);\, q^{2d}\right)\end{aligned}$$

for q a prime power and integer $d \geq 0$ (see Ma and Schmidt (1995) for a summary). The Hadamard and McFarland families coincide in 2-groups: the Hadamard family with $N = 2^d$ corresponds to the McFarland family with $q = 2$.

The Spence family is given by

$$(v, k, \lambda; n) = \left(3^{d+1}\left(\frac{3^{d+1}-1}{2}\right),\, 3^{d}\left(\frac{3^{d+1}+1}{2}\right),\, 3^{d}\left(\frac{3^{d}+1}{2}\right);\, 3^{2d}\right)$$

for integer $d \geq 0$.

The Davis-Jedwab family, introduced in Davis and Jedwab (1997) and named in Beth, Jungnickel and Lenz (1999), is given by $(v, k, \lambda; n) =$

$$\left(2^{2d+4}\left(\frac{2^{2d+2}-1}{3}\right),\, 2^{2d+1}\left(\frac{2^{2d+3}+1}{3}\right),\, 2^{2d+1}\left(\frac{2^{2d+1}+1}{3}\right);\, 2^{4d+2}\right)$$

for integer $d \geq 0$.

The Chen family, introduced in Chen (1997, 1998) and named in Beth, Jungnickel and Lenz (1999), is given by $(v, k, \lambda; n) =$

$$\begin{aligned}&\left(4q^{2d+2}\left(\frac{q^{2d+2}-1}{q^2-1}\right),\, q^{2d+1}\left(\frac{2(q^{2d+2}-1)}{q+1}+1\right),\right.\\ &\qquad\qquad\qquad\qquad \left. q^{2d+1}(q-1)\left(\frac{q^{2d+1}+1}{q+1}\right);\, q^{4d+2}\right)\end{aligned}$$

for integer $d \geq 0$ and q a prime power. The Chen family with $d = 0$ corresponds to the Hadamard family with $N = q$; the Chen family with $q = 2$ corresponds to the Davis-Jedwab family; and the Chen family with $q = 3$ corresponds to the Spence family with d replaced by $2d + 1$. The Davis-Jedwab and Chen families are the first new families of difference sets to be discovered since 1977.

For each of these parameter families, the existence question has been solved for infinitely many values of the parameters, but not necessarily for all possible groups of a given order. The following two results, which give complete solutions to the central problem for certain classes of difference sets, are notable exceptions. (The *exponent* of a group G with identity 1_G, written $\exp(G)$, is the smallest integer α for which $g^\alpha = 1_G$ for all $g \in G$.)

Theorem 1.3. *A Hadamard difference set exists in an abelian group G of order 2^{2d+2} if and only if* $\exp(G) \leq 2^{d+2}$.

Theorem 1.4. *A McFarland difference set with $q = 4$ exists in an abelian group G of order $2^{2d+3}(2^{2d+1}+1)/3$ if and only if the Sylow 2-subgroup of G has exponent at most 4.*

The constructive part of Theorem 1.3 is given in Kraemer (1993) and the nonexistence part is given in Turyn (1965). The constructive part of Theorem 1.4 is given in Davis and Jedwab (1997) and the nonexistence part is given in Ma and Schmidt (1997).

The present authors showed in Davis and Jedwab (1997) that the Hadamard, McFarland, Spence and Davis-Jedwab parameter families can be unified by means of a recursive construction which depends on the existence of certain relative difference sets. The required relative difference sets are themselves constructed by means of a second recursive construction. The present authors showed further in Davis and Jedwab (1999) that by extending these two recursive constructions to use divisible difference sets in place of relative difference sets, the subsequent constructions of Chen difference sets as described in Chen (1997, 1998) can be brought within the unifying framework. This approach deals with all abelian groups known to contain difference sets from the five listed parameter families (although certain initial examples required for the Hadamard family must be constructed separately).

A k-element subset R of a finite multiplicative group G of order $m \cdot u$ containing a normal subgroup U of order u is called a (m, u, k, λ) *relative difference set (RDS) in G relative to U* provided that the multiset $\{r_1 r_2^{-1} : r_1, r_2 \in R, r_1 \neq r_2\}$ contains each element of $G \setminus U$ exactly λ times and contains no element of U. The subgroup U is sometimes called the *forbidden* subgroup. (We have avoided the conventional notation N for the normal subgroup and n for its order so as to avoid confusion with the difference set parameter n.)

Example 1.5. $R = \{1, y, x, x^3 y\}$ is a $(4, 2, 4, 2)$ RDS in $\mathbb{Z}_4 \times \mathbb{Z}_2 = \langle x, y : x^4 = y^2 = 1\rangle$ relative to $\langle x^2 \rangle \cong \mathbb{Z}_2$.

A difference set can be considered as a RDS with $u = 1$. A (m, u, k, λ) RDS in G, relative to some normal subgroup U, is equivalent to a square divisible (m, u, k, λ)-design whose automorphism group G acts regularly on points and blocks (see Pott (1996) for a survey of RDSs and Davis and Jedwab (1997) and Davis, Jedwab and Mowbray (1998) for new constructions). The central problem is to determine, for each parameter set (m, u, k, λ), the groups G of order $m \cdot u$ and the normal subgroups U of order u for which G contains a RDS relative to U with these parameters.

By a counting argument the parameters (m, u, k, λ) of a RDS are related by $k(k-1) = u\lambda(m-1)$. If $k = u\lambda$ then the RDS is called *semi-regular* and the parameters are $(u\lambda, u, u\lambda, \lambda)$. Relative difference sets having semi-regular parameters are of particular interest, especially those occurring in p-groups (in which case the parameters have the form (p^w, p^r, p^w, p^{w-r}) for p prime). Likewise, divisible difference sets having semi-regular parameters have attracted special attention (see Pott (1995) for a definition and discussion of divisible difference sets). And in fact both the relative difference sets used in the recursive constructions of Davis and Jedwab (1997) and the divisible difference sets used in those of Davis and Jedwab (1999) have semi-regular parameters.

Difference sets are usually studied in the context of the group ring $\mathbb{Z}G$ of the group G over the ring of integers $\mathbb{Z}$. The definition of a $(v, k, \lambda; n)$-difference set D in G is equivalent to the equation $DD^{(-1)} = n1_G + \lambda G$ in $\mathbb{Z}G$, where by an abuse of notation we have identified the sets $D, D^{(-1)}, G$ with the respective group ring elements

$$D = \sum_{d \in D} d, \qquad D^{(-1)} = \sum_{d \in D} d^{-1}, \qquad G = \sum_{g \in G} g,$$

and 1_G is the identity of G. Similarly, the definition of a (m, u, k, λ) RDS R in G relative to U is equivalent to the equation $RR^{(-1)} = k1_G + \lambda(G - U)$ in $\mathbb{Z}G$. We shall follow the practice (standard in the difference set literature) of abusing notation by identifying sets with group ring elements, as in the examples above.

An alternative viewpoint for considering difference sets and RDSs, predominant in engineering papers, is via the autocorrelation properties of binary arrays, see Jedwab (1992). The $(1,0)$ binary array A corresponding to a subset D of a group G is $(a_g : g \in G)$ defined by $a_g = 1$ if $g \in D$ and $a_g = 0$ if $g \notin D$. Then $DD^{(-1)} = \sum_{g \in G} R_A(g) g$ in $\mathbb{Z}G$, where $R_A(g) = \sum_{h \in G} a_h a_{gh}$. When G is abelian, $R_A(g)$ is the *periodic autocorrelation* of the binary array A at displacement g, and both A and $(R_A(g) : g \in G)$ can be represented as matrices. The $(+1, -1)$ binary array $B = (b_g : g \in G)$ corresponding to D is given by the linear transformation $b_g = 1 - 2a_g$.

For example, using $+1$ for the symbol $+$ and -1 for $-$, we can represent the $(+1, -1)$ binary array B corresponding to the subset D of Example 1.2

by the matrix

$$\begin{bmatrix} + & - & + & + \\ - & - & - & + \\ + & - & + & + \\ + & + & + & - \end{bmatrix}$$

and its periodic autocorrelation function $(R_B(g) : g \in G)$ by the matrix

$$\begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Similarly the $(+1, -1)$ binary array B corresponding to the subset R in Example 1.5 is

$$\begin{bmatrix} - & - \\ - & + \\ + & + \\ + & - \end{bmatrix}$$

and its periodic autocorrelation function is

$$\begin{bmatrix} 8 & 0 \\ 0 & 0 \\ -8 & 0 \\ 0 & 0 \end{bmatrix}.$$

In the remainder of this paper, all groups mentioned should be understood to be abelian.

We shall require the following definitions and results. A *character* of a group G is a homomorphism from G to the multiplicative group of complex roots of unity. Under pointwise multiplication the set $\widehat{G}$ of characters of G forms a group isomorphic to G. The identity of this group is the *principal character* that maps every element of G to 1. The *character sum* of a character χ over the group ring element C corresponding to a subset of G is $\chi(C) = \sum_{c \in C} \chi(c)$. It is well-known (see Pott (1995), for example) that the character sum $\chi(C)$ is 0 for all non-principal characters χ of G if and only if C is a multiple of G (regarded as a group ring element). If a character χ is non-principal on G and principal on a subgroup U then χ induces a non-principal character ψ on G/U defined by $\psi(gU) = \chi(g)$.

The use of character sums to study difference sets was introduced in the seminal paper Turyn (1965) and subsequently extended to relative difference sets:

Lemma 1.6.

(a) The k-element subset D of a group G of order v is a $(v,k,\lambda;n)$-difference set in G if and only if $|\chi(D)| = \sqrt{n}$ for every non-principal character χ of G.

(b) The k-element subset R of a group G of order $m \cdot u$ containing a subgroup U of order u is a (m,u,k,λ) RDS in G relative to U if and only if for every non-principal character χ of G:

$$|\chi(R)| = \begin{cases} \sqrt{k} & \text{if } \chi \text{ is non-principal on } U, \\ \sqrt{k-u\lambda} & \text{if } \chi \text{ is principal on } U. \end{cases}$$

Lemma 1.6 indicates a general strategy for constructing difference sets and relative difference sets, namely to choose a group subset for which all non-principal character sums have the correct modulus. In the case of a relative difference set whose parameters are semi-regular, note that the required value of the character sum $\chi(R)$, when χ is principal on the subgroup U, is zero. In Section 2 we shall show that the determination of character sums can be greatly facilitated by selecting the group subset to be the union of cosets of "building blocks" whose character properties interact in a simple way.

By way of introduction to this technique, we use Lemma 1.6 to check the validity of Examples 1.2 and 1.5 via character sums. We write the subset D of Example 1.2 as the group ring element $D = y(1+x^2)+x(1+y^2)+xy(1+x^2y^2)$. Let χ be a non-principal character of $\mathbb{Z}_4^2$. Now the image space of χ is $\{1, i, -1, -i\}$ and so $\chi(x^2) = \pm 1$ and $\chi(y^2) = \pm 1$. If $\chi(x^2) = \chi(y^2) = 1$ then $\chi(D) = 2\chi(y+x+xy) = 2\chi(\langle xy \rangle) - 2 = -2$. Otherwise exactly two of $\chi(1+x^2)$, $\chi(1+y^2)$ and $\chi(1+x^2y^2)$ are zero and so $|\chi(D)| = 2$. Therefore by Lemma 1.6 (a), D is a $(16,6,2;4)$-difference set in $\mathbb{Z}_4^2$.

Similarly we write the subset R of Example 1.5 as $R = 1+y+x(1+x^2y)$ and let χ be a non-principal character of $\mathbb{Z}_4 \times \mathbb{Z}_2$. We have $\chi(x^2) = \pm 1$ and $\chi(y) = \pm 1$. If $\chi(x^2) = \chi(y) = 1$ then $\chi(R) = 2\chi(1+x) = 2\chi(\langle x \rangle) = 0$. If $\chi(x^2) = 1$ and $\chi(y) = -1$ then $\chi(R) = 0$. Otherwise $\chi(x^2) = -1$ and exactly one of $\chi(1+y)$ and $\chi(1-y)$ is 0, and so $|\chi(R)| = 2$. Therefore by Lemma 1.6 (b), R is a $(4,2,4,2)$ RDS in $\mathbb{Z}_4 \times \mathbb{Z}_2$ relative to $U = \langle x^2 \rangle$.

We shall return to these two examples after introducing some definitions which allow their essential properties to be described concisely.

2. Building Sets and Extended Building Sets

Definition 2.1. A building block in a group G with modulus m *is a subset of G such that all non-principal character sums over the subset have modulus either* 0 *or* m.

Some examples of building blocks are a coset of a subgroup of G, a semi-regular RDS in G relative to a subgroup U, and a difference set in G.

Definition 2.2. *For integers $a \geq 1$ and $t \geq 1$, a (a, m, t)* building set *(BS) on a group G relative to a subgroup U is a collection of t building blocks in G with modulus m, each containing a elements, such that for every non-principal character χ of G:*

(a) exactly one building block has nonzero character sum if χ is non-principal on U;

(b) each building block has zero character sum if χ is principal on U.

We call the BS *covering* in the case $U = G$, when exactly one building block has nonzero character sum for every non-principal character of G. (The use of "covering" refers not to the intersection or union of the building blocks but to their character properties.)

Definition 2.3. *For integers $a \geq 0$, $m \geq 1$, and $h \geq 1$, a $(a, m, h, +)$* extended building set (EBS) *on a group G with respect to a subgroup U is a collection of h building blocks in G with modulus m, of which $h - 1$ contain a elements and one contains $a + m$ elements, such that for every non-principal character χ of G:*

(a) exactly one building block has nonzero character sum if χ is principal on U;

(b) each building block has zero character sum if χ is non-principal on U.

We define a $(a, m, h, -)$ EBS on G with respect to U in the same way, with $a + m$ replaced by $a - m$. We can treat both cases simultaneously by referring to a $(a, m, h, \pm)$ EBS. Notice that the role of principal and non-principal characters on U in Definition 2.3 is the reverse of that in Definition 2.2! We call the EBS *covering* in the case $U = \{1_G\}$, when exactly one building block has nonzero character sum for every non-principal character of G.

Example 2.4. Let $H_0 = 1 + a$, $H_1 = 1 + b$ and $H_2 = 1 + ab$ be subsets of the group $\mathbb{Z}_2^2 = \langle a, b : a^2 = b^2 = 1 \rangle$. Then $\{\phi, H_0, H_1, H_2\}$ is a $(2, 2, 4, -)$ covering EBS on $\mathbb{Z}_2^2$ and $\{H_1, H_2\}$ is a $(2, 2, 2)$ BS on $\mathbb{Z}_2^2$ relative to H_0.

Example 2.4 is a special case of an important construction which we now describe. Let P be a vector space of dimension 2 over $\mathbb{F}_{p^r}$, where p is prime. The additive group of P is isomorphic to $\mathbb{Z}_p^{2r}$. There are $p^r + 1 = (p^{2r} - 1)/(p^r - 1)$ subspaces $H_0, H_1, \ldots, H_{p^r}$ of P of dimension 1, called hyperplanes, each containing p^r elements. The hyperplanes have the crucial property that any non-principal character of G is principal on exactly one of the hyperplanes (see Davis and Jedwab (1997), for example):

Lemma 2.5. *Let P be a vector space of dimension 2 over $\mathbb{F}_{p^r}$, where p is prime and $r \geq 1$. Any non-principal character of P is principal on exactly one of the $p^r + 1$ hyperplanes of P.*

Corollary 2.6. *Let p be prime and let $r \geq 1$. Then there are subgroups $H_0, H_1, \ldots, H_{p^r}$ of $\mathbb{Z}_p^{2r}$ such that $\{H_1, H_2, \ldots, H_{p^r}\}$ is a (p^r, p^r, p^r) BS on $\mathbb{Z}_p^{2r}$ relative to $H_0 \cong \mathbb{Z}_p^r$ (where H_0 is contained within exactly r direct factors of $\mathbb{Z}_p^{2r}$), and such that $\{\phi, H_0, H_1, H_2, \ldots, H_{p^r}\}$ is a $(p^r, p^r, p^r+2, -)$ covering EBS on $\mathbb{Z}_p^{2r}$.*

Proof. Let $H_0, H_1, \ldots, H_{p^r}$ be the subgroups of $\mathbb{Z}_p^{2r}$ of order p^r corresponding to hyperplanes of P under an isomorphism from $\mathbb{Z}_p^{2r}$ to P. Label the subgroups so that $H_0 \cong \mathbb{Z}_p^r$ is contained in exactly r direct factors of $\mathbb{Z}_p^{2r}$. Then Lemma 2.5 implies the result. □

We next relate the covering EBS and BS of Example 2.4 to the difference set of Example 1.2 and the RDS of Example 1.5 in order to illustrate the motivation for introducing building blocks. The subset D of Example 1.2 can be written as $1 \cdot \phi + yH_0 + xH_1 + xyH_2$ by embedding $\mathbb{Z}_2^2$ in $\mathbb{Z}_4^2$ via $a \mapsto x^2$ and $b \mapsto y^2$. Each of the four building blocks of the $(2, 2, 4, -)$ covering EBS occurs in a different coset of $\mathbb{Z}_2^2$ in $\mathbb{Z}_4^2$. Likewise the subset R of Example 1.5 can be written in the form $1 \cdot H_1 + xH_2$ by embedding $\mathbb{Z}_2^2$ in $\mathbb{Z}_4 \times \mathbb{Z}_2$ via $a \mapsto x^2$ and $b \mapsto y$, and each of the two building blocks of the $(2, 2, 2)$ BS occurs in a different coset of $\mathbb{Z}_2^2$ in $\mathbb{Z}_4 \times \mathbb{Z}_2$. We now show how to formalise this procedure.

We begin by showing that a BS on a group G relative to a subgroup U can be used to construct a BS on larger groups containing G as a subgroup. In the case when the BS on G has parameters $(a, \sqrt{at}, t)$ this allows the construction of a semi-regular RDS as a single building block on a group containing G..

Lemma 2.7. *Suppose there exists a (a, m, t) BS on a group G relative to a subgroup U and let s be an integer dividing t. Then there exists a $(as, m, t/s)$ BS on G' relative to U, where G' is any group containing G as a subgroup of index s.*

Proof. Let $\{B_1, B_2, \ldots, B_t\}$ be a (a, m, t) BS on G relative to U. For each $j = 1, 2, \ldots, t/s$ we define the subset $R_j = \cup_{i=1}^{s} g_i' B_{i+(j-1)s}$ of G', where $g_1', g_2', \ldots, g_s' \in G'$ are coset representatives of G in G'. (Although the building blocks B_i can have non-empty intersection, by definition no set R_j contains repeated elements.) Let χ be a non-principal character of G' and consider the character sum $\chi(R_j) = \sum_{i=1}^{s} \chi(g_i')\chi(B_{i+(j-1)s})$. We distinguish three cases.

Case 1: χ is principal on G and non-principal on G' (so $s > 1$). We have $\chi(B_{i+(j-1)s}) = |B_{i+(j-1)s}| = a$ for each ordered pair (i, j) and so $\chi(R_j) = a\sum_{i=1}^{s} \chi(g_i') = 0$ for each j. The last equality uses the fact that

χ induces a non-principal character on G'/G, and the associated character sum over this group is 0.

Case 2: χ is principal on U and non-principal on G. By assumption $\chi(B_{i+(j-1)s}) = 0$ for each ordered pair (i, j) and so again $\chi(R_j) = 0$ for each j.

Case 3: χ is non-principal on U. By assumption $|\chi(B_{i+(j-1)s})| = m$ for exactly one ordered pair (i, j) (say (I, J)) and $|\chi(B_{i+(j-1)s})| = 0$ for all other ordered pairs (i, j). Therefore $|\chi(R_J)| = |\chi(g'_I)||\chi(B_{I+(J-1)s})| = m$ and $|\chi(R_j)| = 0$ for each $j \neq J$.

The character sums for the three cases show that $\{R_1, R_2, \ldots, R_{t/s}\}$ is a $(as, m, t/s)$ BS on G' relative to U. □

Theorem 2.8. *Suppose there exists a $(a, \sqrt{at}, t)$ BS on a group G relative to a subgroup U of order u, where $at > 1$. Then there exists a $(at, u, at, at/u)$ semi-regular RDS in G' relative to U, where G' is any group containing G as a subgroup of index t.*

Proof. Apply Lemma 2.7 with $s = t$ to obtain a $(at, \sqrt{at}, 1)$ BS on G' relative to U. For $at > 1$, it follows from Definition 2.2 and Lemma 1.6 (b) that this is equivalent to a $(at, u, at, at/u)$ semi-regular RDS in G' relative to U. □

By following a similar proof to that of Lemma 2.7 and Theorem 2.8 we can show that a covering EBS on a group G can be used to construct a covering EBS on larger groups containing G as a subgroup, and that this allows the construction of a difference set as a single building block on a group containing G.

Lemma 2.9. *Suppose there exists a $(a, m, h, \pm)$ covering EBS on a group G and let s be an integer dividing h. Then there exists a $(as, m, h/s, \pm)$ covering EBS on G', where G' is any group containing G as a subgroup of index s.*

Theorem 2.10. *Suppose there exists a $(a, m, h, \pm)$ covering EBS on a group G. Then there exists a $(h|G|, ah \pm m, ah \pm m - m^2; m^2)$-difference set in any group G' containing G as a subgroup of index h.*

By applying Theorems 2.8 and 2.10 to the BS and covering EBS of Corollary 2.6 we obtain the following result, of which Examples 1.2 and 1.5 are special cases. For q a prime power, we write EA(q) to denote the elementary abelian group of order q.

Example 2.11. Let p be prime and let $r \geq 1$. Then there exists a semi-regular RDS with parameters $(p^{2r}, p^r, p^{2r}, p^r)$ in any group of order p^{3r} containing a subgroup $G \cong \mathbb{Z}_p^{2r}$, relative to some subgroup $U \cong \mathbb{Z}_p^r$ of G, and there exists a McFarland difference set with $q = p^r$ and $d = 1$ in any group of order $q^2(q + 2)$ containing a subgroup isomorphic to EA(q^2).

Further examples of BSs and covering EBSs are given by:

Example 2.12. Let G be any one of the groups $\mathbb{Z}_4^2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2^3$ and $\mathbb{Z}_2^5$. Then there exists a $(8, 4, 2)$ BS on G relative to a subgroup $U \cong \mathbb{Z}_2^2$ contained within two of the largest direct factors of G, and there exists a $(8, 4, 3, -)$ covering EBS on G.

Proof. For $G = \mathbb{Z}_4^2 \times \mathbb{Z}_2 = \langle x, y, z : x^4 = y^4 = z^2 = 1\rangle$ and $U = \langle x^2, y^2\rangle \cong \mathbb{Z}_2^2$ we obtain the desired BS from the work described in Arasu and Seghal (1995) by defining $B_1 = 1 + x + xz + x^2z + x^2yz + xy + xy^3z + y^3$ and $B_2 = 1 + x^3 + x^3y^2z + x^2y^2z + yz + xy^3z + xy^3 + x^2y$ and using direct computation to verify that $\{B_1, B_2\}$ is a $(8, 4, 2)$ BS on G relative to U. For $G = \mathbb{Z}_4 \times \mathbb{Z}_2^3$ or $\mathbb{Z}_2^5$ we use Corollary 2.6 to provide a $(4, 4, 4)$ BS on $\mathbb{Z}_2^4$ relative to $U \cong \mathbb{Z}_2^2$ and then apply Lemma 2.7 with $s = 2$ to construct the desired $(8, 4, 2)$ BS on G relative to U.

For all three groups G we define a third building block $B_3 = U$, and then $\{B_1, B_2, B_3\}$ is a $(8, 4, 3, -)$ covering EBS on G. □

By applying Theorems 2.8 and 2.10 to the BSs and covering EBSs of Example 2.12 we obtain further semi-regular RDSs and difference sets:

Example 2.13. There exists a $(16, 4, 16, 4)$ semi-regular RDS in each of the groups $\mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_4^3$, $\mathbb{Z}_4^2 \times \mathbb{Z}_2^2$, $\mathbb{Z}_8 \times \mathbb{Z}_2^3$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2^4$, $\mathbb{Z}_2^2 \times \mathbb{Z}_4 \times \mathbb{Z}_2^2$ and $\mathbb{Z}_2^6$ relative to a subgroup isomorphic to $\mathbb{Z}_2^2$ contained within the first two direct factors of the group. There exists a $(96, 20, 4, 16)$ McFarland difference set in any group of order 96 whose Sylow 2-subgroup has exponent at most 4.

3. Construction Theorems

In this section we describe two recursive constructions, the first for covering EBSs and the second for BSs. These constructions allow us systematically to generate families of covering EBSs and BSs and then, using Theorems 2.8 and 2.10, to deduce the existence of families of difference sets and semi-regular RDSs. We use the following example to introduce the first recursive construction.

Example 3.1. There exists a $(32, 16, 11, -)$ covering EBS on any group G of order 128 and exponent at most 4.

Proof. Let $U \cong \mathbb{Z}_2^2$ be a subgroup of G contained within two of the largest direct factors of G (so that G/U is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2^3$ or $\mathbb{Z}_2^5$). By Example 2.12 there exists a $(8, 4, 3, -)$ covering EBS on G/U, say $\{B_1', B_2', B_3'\}$. "Lift" this covering EBS by setting $B_j = \{g \in G : gU \in B_j'\}$ for $j = 1, 2, 3$ and let χ be a non-principal character of G. Now each B_j is the union of $|B_j'|$ distinct cosets of U so if χ is non-principal on U then $\chi(B_j) = 0$ whereas if χ is principal on U then $\chi(B_j) = 4\psi(B'_j)$, where ψ is the non-principal character induced by χ on G/U. By Definition 2.3, $\psi(B'_j)$ is nonzero (having modulus 4) for exactly one value of j. Furthermore $|B_1| = |B_2| = 32$ and $|B_3| = 16$. Therefore by Definition 2.3, $\{B_1, B_2, B_3\}$ is a $(32, 16, 3, -)$ EBS on G with respect to U. In addition we shall demonstrate in Example 3.8 that there exists a $(32, 16, 8)$ BS on G relative to U, say $\{B_4, B_5, \ldots, B_{11}\}$. Therefore by Definitions 2.2 and 2.3 the mulitset union $\{B_1, B_2, \ldots, B_{11}\}$ is a $(32, 16, 11, -)$ covering EBS on G: either exactly one of the building blocks B_1, B_2, B_3 has nonzero character sum (with modulus 16) and each of the building blocks $B_4, B_5, \ldots, B_{11}$ has zero character sum, or vice-versa. □

The covering EBS of Example 3.1 gives rise, under Theorem 2.10, to a $(1408, 336, 80, 256)$ McFarland difference set in $G \times \mathbb{Z}_{11}$ having $q = 4$ and $d = 2$. In contrast the $(8, 4, 3, -)$ covering EBS used as an initial object in the proof of Example 3.1 gives rise, under Theorem 2.10, to a $(96, 20, 4, 16)$ McFarland difference set in $G/U \times \mathbb{Z}_3$ having $q = 4$ and $d = 1$. This indicates the pattern of a recursive construction for McFarland difference sets relying on a construction method for covering EBSs which we now prove.

Lemma 3.2. *Suppose there exists a $(am, m, h, \pm)$ covering EBS on a group G/U, where U is a subgroup of G of order u. Then there exists an EBS on G with respect to U with parameters $(uam, um, h, \pm)$.*

Proof. Let $\{B'_1, B'_2, \ldots, B'_h\}$ be a $(am, m, h, \pm)$ covering EBS on G/U. For each j let $B_j = \{g \in G : gU \in B'_j\}$ be the pre-image of B'_j under the quotient mapping from G to G/U. Since B_j is the union of $|B'_j|$ distinct cosets of U, it follows both that $|B_j| = u|B'_j|$ and that for every non-principal character χ of G:

$$\chi(B_j) = \begin{cases} 0 & \text{if } \chi \text{ is non-principal on } U, \\ u\psi(B'_j) & \text{if } \chi \text{ is principal on } U, \end{cases}$$

where ψ is the non-principal character induced by χ on G/U. By the definition of covering EBS, $\psi(B'_j)$ is nonzero (having modulus m) for exactly one value of j. Therefore $\{B_1, B_2, \ldots, B_h\}$ is a $(uam, um, h, \pm)$ EBS on G with respect to U. □

Theorem 3.3. *Let G be a group containing a subgroup U of order u. Suppose there exists a $(am, m, h, \pm)$ covering EBS on G/U and there exists a (uam, um, t) BS on G relative to U. Then there exists a $(uam, um, h+t, \pm)$ covering EBS on G.*

Proof. By Lemma 3.2 the existence of a $(am, m, h, \pm)$ covering EBS on G/U implies the existence of a $(uam, um, h, \pm)$ EBS, say $\{B_1, B_2, \ldots, B_h\}$, on G with respect to U. So by Definition 2.3, a non-principal character χ of

G gives a nonzero character sum on exactly one of the building blocks $B_1, B_2, \ldots, B_h$ if χ is principal on U, and gives a zero character sum on all these building blocks otherwise. By assumption there exists a (uam, um, t) BS, say $\{B_{h+1}, B_{h+2}, \ldots, B_{h+t}\}$, on G relative to U. So by Definition 2.2, a non-principal character χ of G gives a nonzero character sum on exactly one of the building blocks $B_{h+1}, B_{h+2}, \ldots, B_{h+t}$ if χ is non-principal on U, and gives a zero character sum on all these building blocks otherwise. Combining the character properties, we see that the multiset union of the building blocks $\{B_1, B_2, \ldots, B_{h+t}\}$ is a $(uam, um, h+t, \pm)$ covering EBS on G. □

The proof of Theorem 3.3 demonstrates the power of the notion of building sets and extended building sets. The crucial property, that at most one of the building blocks has a nonzero character sum, allows us to combine their favourable character properties simply by taking the multiset union of the constituent building blocks. In contrast the binary array viewpoint would require a much more complicated analysis involving the crosscorrelation of pairs of arrays.

Example 3.4. There exists a $(16, 8, 5, +)$ covering EBS on each of the groups $\mathbb{Z}_4^2 \times \mathbb{Z}_2^2$, $\mathbb{Z}_4 \times \mathbb{Z}_2^4$ and $\mathbb{Z}_2^6$.

Proof. Let G be any one of the listed groups and let $U \cong \mathbb{Z}_2^2$ be a subgroup of G such that $G/U \cong \mathbb{Z}_2^4$. Now by Corollary 2.6 with $p = 2$ and $r = 1$ there exists a $(2, 2, 4, -)$ covering EBS on $\mathbb{Z}_2^2$. Therefore by Theorem 2.10, $\mathbb{Z}_2^4$ contains a $(16, 6, 2; 4)$-difference set, which can be viewed as a $(4, 2, 1, +)$ covering EBS on $\mathbb{Z}_2^4$. Also Section 4 of Davis and Jedwab (1997) demonstrates that there exists a $(16, 8, 4)$ BS on G relative to U. Combining these under Theorem 3.3 we obtain a $(16, 8, 5, +)$ covering EBS on G. □

We remark that whereas the covering EBS of Example 3.1 comprises ten blocks of equal cardinality and an eleventh which is *smaller*, the covering EBS of Example 3.4 comprises four blocks of equal cardinality and a fifth which is *larger*. Under Theorem 2.10 the covering EBS of Example 3.4 gives rise to a $(320, 88, 24, 64)$ Davis-Jedwab difference set in $G \times \mathbb{Z}_5$ having $d = 1$. This indicates the pattern of a recursive construction for Davis-Jedwab difference sets, since the initial $(16, 6, 2; 4)$-difference set used in the proof of Example 3.4 can be regarded as a Davis-Jedwab difference set with $d = 0$.

However both Examples 3.1 and 3.4 rely on the existence of certain BSs. In general the recursive construction of covering EBSs using Theorem 3.3, and therefore of difference sets using Theorem 2.10, relies on the existence of families of suitable BSs. This motivates the second recursive construction of this section, for BSs.

The idea of the construction is to exploit the hyperplane structure of Lemma 2.5 to obtain a more general result than Corollary 2.6. Begin with a group G containing a subgroup Q isomorphic to $\mathbb{Z}_p^{2r}$ and consider those subgroups H_i of G which correspond to hyperplanes when viewed as subgroups of Q. We now show that if there exists a BS on G/H_i relative to Q/H_i for $i = 1, 2, \ldots, p^r$ then each BS can be "lifted" from the quotient group G/H_i to G to collectively form a BS on G relative to H_0.

Theorem 3.5. *Let G be a group containing a subgroup $Q \cong \mathbb{Z}_p^{2r}$, where p is prime and $r \geq 1$ (the case $Q = G$ being allowed). Let $H_0, H_1, \ldots, H_{p^r}$ be the subgroups of G of order p^r corresponding to hyperplanes when viewed as subgroups of Q. Suppose there exists a (a, m, t) BS on G/H_i relative to Q/H_i for each $i = 1, 2, \ldots, p^r$. Then there exists a $(p^r a, p^r m, p^r t)$ BS on G relative to H_0.*

Proof. For each $i \geq 1$, let $\{B'_{i1}, B'_{i2}, \ldots, B'_{it}\}$ be a (a, m, t) BS on G/H_i relative to Q/H_i. Following the proof of Lemma 3.2, for each $i \geq 1$ and for each j let $B_{ij} = \{g \in G : gH_i \in B'_{ij}\}$. Since B_{ij} is the union of $|B'_{ij}| = a$ distinct cosets of H_i, $|B_{ij}| = p^r a$, and for every non-principal character χ of G and for each $i \geq 1$ and for each j:

$$\chi(B_{ij}) = \begin{cases} 0 & \text{if } \chi \text{ is non-principal on } H_i, \\ p^r \psi(B'_{ij}) & \text{if } \chi \text{ is principal on } H_i, \end{cases} \tag{$\star$}$$

where $\psi(B'_{ij})$ is the non-principal character induced by χ on G/H_i. By the definition of BSs, for each $i \geq 1$, $\psi(B'_{ij})$ is nonzero (having modulus m) for exactly one value of j if ψ is non-principal on Q/H_i, and is zero for each value of j if ψ is principal on Q/H_i.

We claim that $\{B_{ij} : 1 \leq i \leq p^r, 1 \leq j \leq t\}$, comprising $p^r t$ subsets B_{ij} of G, is a $(p^r a, p^r m, p^r t)$ BS on G relative to H_0. To establish this, let χ be a non-principal character of G and distinguish three cases.

Case 1: χ is non-principal on Q and on H_0. By Lemma 2.5, χ is principal on H_I for some $I \neq 0$ and non-principal on H_i for each $i \neq I$. Therefore $\chi(B_{ij}) = 0$ for each $i \neq I$ and $\chi(B_{Ij}) = p^r \psi(B'_{Ij})$, from ($\star$). Since χ is non-principal on Q, ψ is non-principal on Q/H_I and so $\psi(B'_{Ij})$ is nonzero (having modulus m) for exactly one value of j. Therefore $\chi(B_{ij})$ is nonzero (having modulus $p^r m$) for exactly one ordered pair (i, j).

Case 2: χ is non-principal on Q and principal on H_0. By Lemma 2.5, χ is non-principal on H_i for each $i \neq 0$. Therefore $\chi(B_{ij}) = 0$ for each ordered pair (i, j), from ($\star$).

Case 3: χ is principal on Q (note this cannot arise if $Q = G$). In this case χ is principal on H_i for each $i \geq 0$. Therefore $\chi(B_{ij}) = p^r \psi(B'_{ij})$ for each $i \geq 1$, from ($\star$). Since ψ is principal on Q/H_i, $\psi(B'_{ij}) = 0$ for each ordered pair (i, j).

The results for the three cases establish the claim. □

Given a group G and a subgroup $H_0 \cong \mathbb{Z}_p^r$ on which we wish to construct a BS using Theorem 3.5, we are free to choose Q to be any subgroup of G isomorphic to $\mathbb{Z}_p^{2r}$ containing H_0. This choice will determine the subgroups $H_i \neq H_0$ of G corresponding to hyperplanes. By suitable choice of generators of G we can assume that Q is contained in $2r$ direct factors of G and that any one particular hyperplane H_i is contained in r of these direct factors. Then the proof of Theorem 3.5 describes a procedure for constructing the BS explicitly. Given a (a, m, t) BS on each of the p^r quotient groups G/H_i relative to Q/H_i, we lift each BS from G/H_i to G by taking $B_{ij} = \{g \in G : gH_i \in B'_{ij}\}$. This produces the $p^r t$ building blocks of a $(p^r a, p^r m, p^r t)$ BS on G relative to H_0. We now illustrate this procedure in detail.

Example 3.6. There exists a $(32, 16, 8)$ BS on $G = \mathbb{Z}_4^3 \times \mathbb{Z}_2 = \langle x, y, z, w : x^4 = y^4 = z^4 = w^2 = 1\rangle$ relative to $H_0 = \langle x^2, y^2\rangle \cong \mathbb{Z}_2^2$.

Proof. We firstly choose the subgroup $Q \cong \mathbb{Z}_2^4$ of G to be $\langle x^2, y^2, z^2, w\rangle$, which contains H_0. We next determine the subgroups of G corresponding to hyperplanes, by reference to the multiplicative structure of $\mathbb{F}_4$. Since x^2+x+1 is an irreducible polynomial of degree 2 over $\mathbb{F}_4$ we can regard $\mathbb{F}_4$ as having multiplicative generator δ, where $\delta^2 = \delta + 1$. Then the hyperplanes of $\mathbb{F}_4^2$ are $\langle(1,0)\rangle$, $\langle(0,1)\rangle$, $\langle(1,1)\rangle$, $\langle(\delta,1)\rangle$ and $\langle(\delta+1,1)\rangle$. Define an isomorphism from $\mathbb{F}_4^2$ to Q by $(1,0) \mapsto x^2$, $(\delta, 0) \mapsto y^2$, $(0,1) \mapsto z^2$ and $(0,\delta) \mapsto w$. The subgroups of G corresponding to the hyperplanes are then respectively $H_0 = \langle x^2, y^2\rangle$, $H_1 = \langle z^2, w\rangle$, $H_2 = \langle x^2z^2, y^2w\rangle$, $H_3 = \langle y^2z^2, x^2y^2w\rangle$ and $H_4 = \langle x^2y^2z^2, x^2w\rangle$. For each $i \neq 0$ we now form the quotient group G/H_i and its associated subgroup Q/H_i. In this case we find that $G/H_i \cong \mathbb{Z}_4^2 \times \mathbb{Z}_2$, and $Q/H_i \cong \mathbb{Z}_2^2$ is contained within $\mathbb{Z}_4^2$, for each $i \neq 0$. We therefore require a $(8, 4, 2)$ BS on $\langle a, b, c : a^4 = b^4 = c^2\rangle$ relative to $\langle a^2, b^2\rangle$. Using Example 2.12, such a BS is given by the group ring elements

$$\begin{aligned} B'_1(a,b,c) &= 1 + a + ac + a^2c + a^2bc + ab + ab^3c + b^3, \\ B'_2(a,b,c) &= 1 + a^3 + a^3b^2c + a^2b^2c + bc + ab^3c + ab^3 + a^2b. \end{aligned}$$

In order to construct the BS on G we write each quotient group G/H_i explicitly in terms of its generators. We find

$$G/H_1 = \langle xH_1, yH_1, zH_1\rangle, \qquad G/H_2 = \langle xH_2, yH_2, xzH_2\rangle,$$

$$G/H_3 = \langle xH_3, yH_3, yzH_3\rangle \quad \text{and} \quad G/H_4 = \langle xH_4, yH_4, xyzH_4\rangle,$$

the first two generators having order 4 and the third generator having order 2 in each case. We also find $Q/H_i \cong \langle x^2H_i, y^2H_i\rangle$ for each $i \neq 0$. Therefore a

$(8,4,2)$ BS in G/H_i relative to Q/H_i is given by the building blocks B'_{i1} and B'_{i2} where for $j=1,2$ we have $B'_{1j} = B'_j(x,y,z)H_1$, $B'_{2j} = B'_j(x,y,xz)H_2$, $B'_{3j} = B'_j(x,y,yz)H_3$ and $B'_{4j} = B'_j(x,y,xyz)H_4$. For example, B'_{21} is given by

$$H_2 + xH_2 + x^2zH_2 + x^3zH_2 + x^3yzH_2 + xyH_2 + x^2y^3zH_2 + y^3H_2.$$

Each of the expressions B'_{ij} is a group ring element in $\mathbb{Z}[G/H_i]$ comprising 8 elements of the quotient group G/H_i. We finally obtain $B_{ij} = \{g \in G : gH_i \in B'_{ij}\}$ by regarding the formal expression for B'_{ij} as a group ring element in $\mathbb{Z}G$ comprising 32 elements of G. The 8 building blocks $\{B_{ij} : 1 \le i \le 4, 1 \le j \le 2\}$ then form a $(32,16,8)$ BS on G relative to H_0. □

For the group G of Example 3.6 we see that all the quotient groups G/H_i having $i \neq 0$ are isomorphic but in general this need not be the case. For example, let $r = 3$ and consider the group

$$\begin{aligned} G &= \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \\ &= \langle x,y,z,u,v,w : x^2 = y^4 = z^8 = u^8 = v^4 = w^4 = 1\rangle. \end{aligned}$$

Follow the procedure given in the proof of Example 3.6 to label the hyperplanes of $\mathbb{F}_8^2$ and define an isomorphism from $\mathbb{F}_8^2$ to $Q = \langle x = y^2 = z^4 = u^4 = v^2 = w^2 = 1\rangle \cong \mathbb{Z}_2^6$, taking the irreducible polynomial of degree 3 over $\mathbb{F}_2$ to be x^3+x+1. Then the subgroups of G corresponding to the hyperplanes $\langle(1,1)\rangle$, $\langle(\delta^2,1)\rangle$ and $\langle(\delta^4,1)\rangle$ are $H_2 = \langle xu^4, y^2v^2, z^4w^2\rangle$, $H_4 = \langle z^4u^4, xy^2v^2, y^2z^4w^2\rangle$ and $H_6 = \langle y^2z^4u^4, xy^2z^4v^2, xz^4w^2\rangle$ respectively. The factor groups G/H_2 and G/H_6 are not isomorphic to G/H_4: we have

$$\begin{aligned} G/H_2 &= \langle H_2, yH_2, zH_2, uH_2, yvH_2, wz^2H_2\rangle \\ &\cong (\mathbb{Z}_1\times)\mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \\ G/H_4 &= \langle H_4, yH_4, zH_4, zuH_4, vH_4, yz^2wH_4\rangle \\ &\cong (\mathbb{Z}_1\times)\mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2, \\ G/H_6 &= \langle H_6, yz^2u^2H_6, zH_6, uH_6, wyvH_6, wH_6\rangle \\ &\cong (\mathbb{Z}_1\times)\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_4. \end{aligned}$$

Furthermore, although each of the factor groups Q/H_2, Q/H_4 and Q/H_6 is isomorphic to $\mathbb{Z}_2^3$, the direct factors of G/H_i which contain Q/H_i are different in each case: we have $Q/H_2 = \langle y^2H_2, z^4H_2, u^4H_2\rangle$ (contained within the second, third and fourth direct factors of G/H_2), $Q/H_4 = \langle y^2H_4, z^4H_4, v^2H_4\rangle$ (contained within the second, third and fifth direct factors of G/H_4) and $Q/H_6 = \langle z^4H_6, u^4H_6, w^2H_6\rangle$ (contained within the third, fourth and sixth direct factors of G/H_6).

The above discussion illustrates that to apply Theorem 3.5 effectively we need information about the form of G/H_i and Q/H_i. In fact we have shown in Davis and Jedwab (1997) that by appropriate choice of generators, exactly r direct factors of G retain the same exponent in G/H_i (these being the direct factors that contain Q/H_i) and r are reduced by a factor of p:

Lemma 3.7. *Let G be the group $\prod_{u=1}^{2r} \mathbb{Z}_{p^{1+\alpha_u}}$ containing a subgroup $Q \cong \mathbb{Z}_p^{2r}$, where p is prime and $\alpha_u \geq 0$. Let $H_0, H_1, \ldots, H_{p^r}$ be the subgroups of G of order p^r corresponding to hyperplanes when viewed as subgroups of Q. Then for each H_i there exists a r-element subset S of $\{1, 2, \ldots, 2r\}$ such that $G/H_i \cong \prod_{u \notin S} \mathbb{Z}_{p^{1+\alpha_u}} \times \prod_{u \in S} \mathbb{Z}_{p^{\alpha_u}}$. Moreover, for each H_i a suitable choice of generators of G ensures that $Q/H_i \cong \mathbb{Z}_p^r$ is contained in the first r direct factors of G/H_i as specified.*

Lemma 3.7 allows us readily to generalise Example 3.6:

Example 3.8. There exists a $(32, 16, 8)$ BS on any group G of order 128 and exponent at most 4 relative to a subgroup $U \cong \mathbb{Z}_2^2$ contained within two of the largest direct factors of G.

Proof. Let $Q \cong \mathbb{Z}_2^4$ be a subgroup of G containing $H_0 = U$. For each subgroup $H_i \neq H_0$ of G of order 4, corresponding to a hyperplane when viewed as a subgroup of Q, Lemma 3.7 shows that G/H_i has order 32 and exponent at most 4 and that $Q/H_i \cong \mathbb{Z}_2^2$ is contained in two of the largest direct factors of G/H_i. By Example 2.12 there is a $(8, 4, 2)$ BS on G/H_i relative to Q/H_i and so by Theorem 3.5 we obtain the desired BS on G. □

Just as Theorem 3.3 can be applied recursively to construct covering EBSs, subject to the existence of families of suitable BSs, so Theorem 3.5 can be applied recursively to construct BSs — but without relying on the existence of other objects! (When Theorem 3.5 is applied in this way it is important to keep track of the position of the subgroup H_0 in relation to the group G at each stage.) The pattern of a recursive construction for a family of such BSs is indicated by comparing the BSs of Example 2.12 with those of Example 3.8. This family will be described explicitly in Section 4 and used in the construction of McFarland difference sets (see also the proof of Example 3.1 and subsequent remarks).

Figure 1 is a schematic representation of the recursive construction of BSs and covering EBSs described in this section. On the right side of the figure Theorem 3.5 is used to obtain a BS on a group G by lifting a BS on each of the factor groups G/H_i for $i \neq 0$. On the left side of the figure Theorem 3.3 is used to obtain a covering EBS on a group G by lifting a covering EBS on G/H_0 and combining with a BS on G relative to H_0 (see Theorems 3.3 and 4.6 of Davis and Jedwab (1997) for details).

4. The McFarland, Spence, Davis-Jedwab, Hadamard and Chen Families

In this section we summarise the recursive construction of difference sets in the McFarland, Spence, Davis-Jedwab and Hadamard families from covering EBSs using Theorems 3.3 and 3.5 (see Davis and Jedwab (1997) for details). We also summarise the recursive construction of difference sets in the Chen families, for which a modification to Theorem 3.5 is required (see Davis and Jedwab (1999) for details). These results deal with all (abelian) groups known to contain such difference sets, although certain initial examples required for the Hadamard family must be constructed separately.

Recursive application of Theorem 3.5 yields the following families of BSs. All of the initial BSs needed to begin the recursions are given by (or can be derived from) Corollary 2.6, Example 2.12 and the example of a $(4,4,4,1)$ RDS in $\mathbb{Z}_4^2$ relative to $\mathbb{Z}_2^2$ given in Jungnickel (1982).

Theorem 4.1. *For each $d \geq 1$, the following exist:*

(a) A (p^{dr}, p^{dr}, p^{dr}) BS on $\mathbb{Z}_p^{(d+1)r}$ relative to $\mathbb{Z}_p^r$, where p is prime and $r \geq 1$.

(b) A $(2^{2d+1}, 2^{2d}, 2^{2d-1})$ BS on any group G_d of order 2^{2d+3} and exponent at most 4 relative to a subgroup $U_d \cong \mathbb{Z}_2^2$ contained within two of the largest direct factors of G_d.

(c) A $(2^{2d+2}, 2^{2d+1}, 2^{2d})$ BS on any group G_d of order 2^{2d+4} and exponent at most 4 relative to a subgroup $U_d \cong \mathbb{Z}_2^2$ contained within two of the largest direct factors of G_d, except possibly $G_1 = \mathbb{Z}_4^3$.

Using Theorem 3.3 and the BSs of Theorem 4.1 we can recursively construct the following families of covering EBSs. The only non-trivial initial covering EBSs required, for case (d), can be derived from the covering EBS of Corollary 2.6 (which itself is given by putting $d = 1$ in case (a) below).

Theorem 4.2. *For each $d \geq 0$, the following exist:*

(a) A $(p^{dr}, p^{dr}, \frac{p^{(d+1)r}-1}{p^r-1}+1, -)$ covering EBS on $\mathbb{Z}_p^{(d+1)r}$, where p is prime and $r \geq 1$.

(b) A $(2^{2d+1}, 2^{2d}, \frac{2^{2d+1}+1}{3}, -)$ covering EBS on any group of order 2^{2d+3} and exponent at most 4.

(c) A $(3^d, 3^d, \frac{3^{d+1}-1}{2}, +)$ covering EBS on $\mathbb{Z}_3^{d+1}$.

(d) A $(2^{2d+2}, 2^{2d+1}, \frac{2^{2d+2}-1}{3}, +)$ covering EBS on any group of order 2^{2d+4} and exponent at most 4, except possibly $\mathbb{Z}_4^3$ in the case $d = 1$.

By applying Theorem 2.10 to the covering EBSs of Theorem 4.2 we deduce the existence of the following families of difference sets.

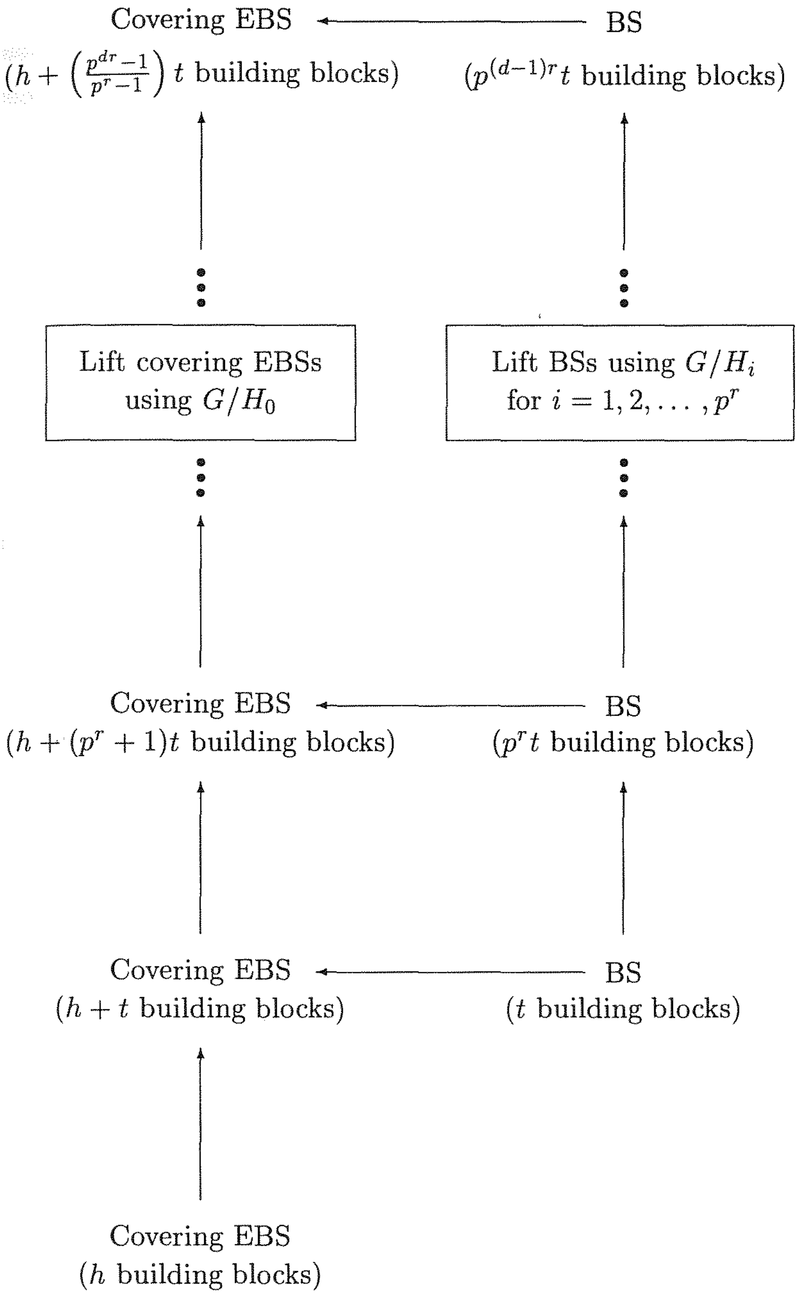
Covering EBS
$(h + \left(\frac{p^{dr}-1}{p^r-1}\right) t$ building blocks)
BS
$(p^{(d-1)r}t$ building blocks)
Lift covering EBSs using G/H_0
Lift BSs using G/H_i for $i = 1, 2, \ldots, p^r$
Covering EBS
$(h + (p^r + 1)t$ building blocks)
BS
$(p^r t$ building blocks)
Covering EBS
$(h + t$ building blocks)
BS
$(t$ building blocks)
Covering EBS
$(h$ building blocks)

Figure 1. Recursive construction of covering EBSs and BSs using Theorems 3.3 and 3.5

Corollary 4.3. *For each $d \geq 0$, the following exist:*

(a) A McFarland difference set in any group of order $q^{d+1}(\frac{q^{d+1}-1}{q-1}+1)$ with $q = p^r$ containing a subgroup isomorphic to $\mathrm{EA}(q^{d+1})$, where p is prime and $r \geq 1$.

(b) A McFarland difference set in any group of order $2^{2d+3}(\frac{2^{2d+1}+1}{3})$ with $q = 4$ containing a subgroup of order 2^{2d+3} and exponent at most 4.

(c) A Spence difference set in any group of order $3^{d+1}(\frac{3^{d+1}-1}{2})$ containing a subgroup isomorphic to $\mathbb{Z}_3^{d+1}$.

(d) A Davis-Jedwab difference set in any group of order $2^{2d+4}(\frac{2^{2d+2}-1}{3})$ containing a subgroup of order 2^{2d+4} and exponent at most 4, except possibly when the subgroup is $\mathbb{Z}_4^3$ in the case $d = 1$.

This completes the summary of known results for the McFarland, Spence and Davis-Jedwab parameter families.

We consider next the Hadamard parameter family. The key initial object required for the recursive construction of Hadamard difference sets is a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on a group of odd order m^2. The following basic examples are currently known.

Theorem 4.4. *There exists a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on the following groups M of order m^2:*

(a) M is the trivial group.

(b) $M = \mathbb{Z}_{3^\alpha}^2$, where $\alpha \geq 1$.

(c) $M = \mathbb{Z}_p^4$, where p is an odd prime.

While case (a) of Theorem 4.4 is trivial, the other two cases are definitely not! Case (b) is given in Arasu, Davis, Jedwab and Seghal (1993). Case (c) is given in Chen (1997), which built on a succession of papers: Xia (1992), Xiang and Chen (1996), van Eupen and Tonchev (1997), and Wilson and Xiang (1997).

The following result, based on a construction in Turyn (1984), allows us to compose the $(m(\frac{m-1}{2}), m, 4, +)$ covering EBSs of Theorem 4.4 to produce examples in more general groups.

Theorem 4.5. *Suppose there exists a $(m_i(\frac{m_i-1}{2}), m_i, 4, +)$ covering EBS on a group M_i of odd order m_i^2 for $i = 1, 2$. Then there exists a covering EBS on $M_1 \times M_2$ with parameters $(m_1 m_2(\frac{m_1 m_2-1}{2}), m_1 m_2, 4, +)$.*

We can use the covering EBSs given by composition, as described above, to derive appropriate initial BSs and covering EBSs for constructing the Hadamard family. Recursive application of Theorems 3.3 and 3.5, followed by Theorem 2.10, leads to the following conclusion. We write $\prod_i \mathbb{Z}_{a_i}$ to denote the direct product of finitely many groups $\mathbb{Z}_{a_1}, \mathbb{Z}_{a_2}, \ldots, \mathbb{Z}_{a_r}$ for some $r \geq 0$, with the convention that in the case $r = 0$ this represents the trivial group.

Corollary 4.6. *Let M be the group $\prod_i \mathbb{Z}_{3^{\alpha_i}}^2 \times \prod_j \mathbb{Z}_{p_j}^4$, where each $\alpha_i \geq 1$ and where each p_j is an odd prime, and let $|M| = m^2$. Then the following exist:*

(a) A $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on M.
(b) A $(2^{2d-1}m^2, 2^d m, 2)$ BS on $G_d \times M$ relative to any subgroup of order 2, where $d \geq 1$ and G_d is any group of order 2^{2d} and exponent at most 2^d.
(c) A $(2^{2d-1}m^2, 2^d m, 4, -)$ covering EBS on $G_d \times M$, where $d \geq 1$ and G_d is any group of order 2^{2d} and exponent at most 2^d.
(d) A Hadamard difference set with $N = 2^d m$ in $G_d \times M$, where $d \geq 0$ and G_d is any group of order 2^{2d+2} and exponent at most 2^{d+2}.

This completes the summary of known results for the Hadamard parameter family.

We turn now to the Chen parameter family. In the recursive construction of the McFarland, Spence, Davis-Jedwab and Hadamard families summarised above, the BSs used in Theorems 3.3 and 3.5 all have parameters of the form $(a, \sqrt{at}, t)$ (and so give rise under Theorem 2.8 to semi-regular relative difference sets). In contrast the recursive construction of the Chen family uses (a, m, t) BSs for which $m \neq \sqrt{at}$ (which give rise to semi-regular divisible difference sets with $\lambda_1 \neq 0$, see Davis and Jedwab (1999)).

The key step, both in the original constructions given in Chen (1997, 1998), and in our recursive formulation (given in full in Davis and Jedwab (1999)), occurs in the derivation of suitable initial BSs from the restriction of Corollary 4.6 to elementary abelian groups. In the case leading to Chen difference sets with odd q, this key step involves replacing one of four building blocks by its complement. In the case leading to Chen difference sets with even q, the key step involves modifying Theorem 3.5 to allow lifting with respect to "contracted" hyperplanes. Once these initial BSs have been derived we can recursively construct the following families of BSs using Theorem 3.5 (without modification).

Theorem 4.7.

(a) For each $d \geq 0$ there exists a $(q^{2d+1}(\frac{q-1}{2}), q^{2d+1}, 4q^{2d})$ BS on $\mathrm{EA}(q^{2d+2})$ relative to $\mathrm{EA}(q^2)$, where $q = 3^r$ or $q = p^{2r}$ for p an odd prime, and $r \geq 1$.
(b) For each $d \geq 1$ there exists a $(q^{2d+1}(q-1), q^{2d+1}, 2q^{2d})$ BS on $\mathrm{EA}(2q^{2d+2})$ relative to $\mathrm{EA}(q^2)$, where $q = 2^r$ and $r \geq 1$.

We next use Theorem 3.3 and the BSs of Theorem 4.7 to construct recursively an infinite family of covering EBSs. The initial covering EBSs are again provided by the restriction of Corollary 4.6 to elementary abelian groups.

Theorem 4.8. *For each $d \geq 0$ the following exist:*

(a) *A* $(q^{2d+1}(\frac{q-1}{2}), q^{2d+1}, 4(\frac{q^{2d+2}-1}{q^2-1}), +)$ *covering EBS on* $\mathrm{EA}(q^{2d+2})$, *where* $q = 3^r$ *or* $q = p^{2r}$ *for* p *an odd prime, and* $r \geq 1$.

(b) *A* $(q^{2d+1}(q-1), q^{2d+1}, 2(\frac{q^{2d+2}-1}{q^2-1}), +)$ *covering EBS on* $\mathrm{EA}(2q^{2d+2})$, *where* $q = 2^r$ *and* $r \geq 1$.

By applying Theorem 2.10 to the covering EBSs of Theorem 4.8 we obtain the following families of Chen difference sets.

Corollary 4.9. *For each* $d \geq 0$ *the following exist:*

(a) *A Chen difference set with* $q = 3^r$ *or* $q = p^{2r}$ *in any group of order* $4q^{2d+2}(\frac{q^{2d+2}-1}{q^2-1})$ *containing a subgroup isomorphic to* $\mathrm{EA}(q^{2d+2})$, *where* p *is an odd prime and* $r \geq 1$.

(b) *A Chen difference set with* $q = 2^r$ *in any group of order* $4q^{2d+2}(\frac{q^{2d+2}-1}{q^2-1})$ *containing a subgroup isomorphic to* $\mathrm{EA}(2q^{2d+2})$, *where* $r \geq 1$.

5. Recursive Construction of Building Sets

Whereas in Section 4 we used Theorem 3.5 only as required to provide suitable families of BSs for the recursive construction of difference sets, in this section we shall demonstrate that Theorem 3.5 is a powerful construction method in its own right for generating families of BSs. These BSs in turn yield families of semi-regular relative difference sets (under Theorem 2.8, when the parameters have the form $(a, \sqrt{at}, t)$) or families of semi-regular divisible difference sets, see Davis and Jedwab (1999).

For an extended example we consider the (p^r, p^r, p^r) BS on $\mathbb{Z}_p^{2r}$ relative to $\mathbb{Z}_p^r$ of Corollary 2.6. We noted in Theorem 4.1 (a) that recursive application of Theorem 3.5 to this BS yields:

Theorem 5.1. *Let* p *be prime and* $r \geq 1$. *For each* $d \geq 1$ *there exists a* (p^{dr}, p^{dr}, p^{dr}) *BS on* $\mathbb{Z}_p^{(d+1)r}$ *relative to* $\mathbb{Z}_p^r$.

We now show that we can also derive from this initial (p^r, p^r, p^r) BS a family of BSs whose building blocks again have modulus p^{dr} but which are defined on groups of lower rank than $\mathbb{Z}_p^{(d+1)r}$.

Example 5.2. Let p be prime and $r \geq 1$. There exists a (p^{3r}, p^{2r}, p^r) BS on any group G_2 of order p^{4r} and exponent at most p^2 relative to any subgroup $U_2 \cong \mathbb{Z}_p^r$, where G_2/U_2 contains a subgroup of index p^r and exponent p.

Proof. By Corollary 2.6 there exists a (p^r, p^r, p^r) BS on $\mathbb{Z}_p^{2r}$ relative to $\mathbb{Z}_p^r$. Put $s = p^r$ in Lemma 2.7 to obtain a $(p^{2r}, p^r, 1)$ BS on any group G of order p^{3r}, relative to any subgroup $U \cong \mathbb{Z}_p^r$, subject to the condition: G contains a subgroup S (containing U) of index p^r and exponent p.

We now wish to apply Theorem 3.5 to obtain a (p^{3r}, p^{2r}, p^r) BS on G_2 relative to U_2. We can do this provided there exists a subgroup $Q_2 \cong \mathbb{Z}_p^{2r}$

of G_2 whose hyperplanes $H_0, H_1, \dots, H_p^r$, when viewed as subgroups of G_2, satisfy the conditions: $H_0 = U_2$ and, for each $i \neq 0$, G_2/H_i contains a subgroup S_2/H_i (containing Q_2/H_i) of index p^r and exponent p. The case $d = 2$ of the group theoretic result stated as Lemma 5.5 shows that this condition on each of the factor groups G_2/H_i is implied by the single condition that G_2/U_2 contains a subgroup of index p^r and exponent p, completing the proof. □

For example, if $G_2 = \mathbb{Z}_p^{2r-2} \times \mathbb{Z}_{p^2}^{r+1}$ (where $r > 1$) and we write the subgroup $U_2 \cong \mathbb{Z}_p^r$ as being contained within r direct factors of G_2 then all choices of U_2 are allowed, except possibly U_2 being contained within the subgroup $\mathbb{Z}_p^{2r-2}$. This demonstrates that the position of the subgroup U_2 within G_2 is important. In particular, in the case $r = 2$, Example 5.2 deals with all groups G_2 of order p^8 and exponent at most p^2 and all subgroups $U_2 \cong \mathbb{Z}_p^2$, except possibly $G_2 \cong U_2 \times \mathbb{Z}_{p^2}^3$. We now repeat the above procedure.

Example 5.3. Let p be prime and $r \geq 1$. There exists a (p^{5r}, p^{3r}, p^r) BS on any group G_3 of order p^{6r} and exponent at most p^3 relative to any subgroup $U_3 \cong \mathbb{Z}_p^r$, where G_3/U_3 contains a subgroup of index p^r and exponent at most p^2 and contains a subgroup of index p^{3r} and exponent p.

Proof. Put $s = p^r$ in Lemma 2.7 to obtain from Example 5.2 a $(p^{4r}, p^{2r}, 1)$ BS on any group G of order p^{5r}, relative to any subgroup $U \cong \mathbb{Z}_p^r$, subject to the following condition: G contains a subgroup S (containing U) of index p^r and exponent at most p^2 such that S/U contains a subgroup of index p^r and exponent p.

We next wish to apply Theorem 3.5 to obtain a (p^{5r}, p^{3r}, p^r) BS on G_3 relative to U_3. This can be done provided there exists a subgroup $Q_3 \cong \mathbb{Z}_p^{2r}$ of G_3 whose hyperplanes $H_0, H_1, \dots, H_p^r$, when viewed as subgroups of G_3, satisfy the conditions: $H_0 = U_3$ and, for each $i \neq 0$, G_3/H_i contains a subgroup S_3/H_i (containing Q_3/H_i) of index p^r and exponent at most p^2 such that $(S_3/H_i)/(Q_3/H_i)$ contains a subgroup of index p^r and exponent p. The case $d = 3$ of Lemma 5.5 shows that this condition on each of the G_3/H_i is implied by the condition that G_3/U_3 contains a subgroup of index p^r and exponent at most p^2 and contains a subgroup of index p^{3r} and exponent p, completing the proof. □

By repeating this procedure we obtain a BS on a group G_d of order p^{2dr} and exponent at most p^d relative to a subgroup $U_d \cong \mathbb{Z}_p^r$, with the following accumulation of conditions on the factor group G_d/U_d (see Davis and Jedwab (1997) for a formal proof):

Theorem 5.4. *Let p be prime and $r \geq 1$. For each $d \geq 1$ there exists a $(p^{(2d-1)r}, p^{dr}, p^r)$ BS on any group G_d of order p^{2dr} and exponent at most*

p^d relative to any subgroup $U_d \cong \mathbb{Z}_p^r$, where, for $d > 1$, G_d/U_d contains a subgroup of index $p^{(2d-2j-1)r}$ and exponent at most p^j for $j = 1, 2, \ldots, d-1$.

The group theoretic lemma which allows conditions on the factor groups G_d/H_i to be replaced by conditions on G_d/U_d (see Theorem 7.5 of Davis and Jedwab (1997) for a proof) is:

Lemma 5.5. *Let p be prime and $d > 1$, and let G be a group of order p^{2dr} and exponent at most p^d containing a subgroup $U \cong \mathbb{Z}_p^r$. Suppose that G/U contains a subgroup of index $p^{(2d-2j-1)r}$ and exponent at most p^j for $j = 1, 2, \ldots, d-1$. Then G contains a subgroup $Q \cong \mathbb{Z}_p^{2r}$ whose hyperplanes $H_0, H_1, \ldots, H_{p^r}$, when viewed as subgroups of G, satisfy the following:*

(a) $H_0 = U$.
(b) For each $i \neq 0$, G/H_i contains a subgroup S/H_i (containing Q/H_i) of index p^r and exponent at most p^{d-1} such that $(S/H_i)/(Q/H_i)$ contains a subgroup of index $p^{(2d-2j-3)r}$ and exponent at most p^j for $j = 1, 2, \ldots, d-2$.

Beginning with an initial example such as the (p^r, p^r, p^r) BS considered above, repeated application of Theorem 3.5 and Lemma 5.5 gives a result of the form of Theorem 5.4, involving multiple conditions on the factor group G_d/U_d. For a particular example some of the conditions may be redundant. In the case of Theorem 5.4 it is straightforward to see by inspection that the conditions for $j = 1, 2, \ldots, d-2$ are all implied by the condition for $j = d-1$. Therefore Theorem 5.4 can be rewritten as:

Corollary 5.6. *Let p be prime and $r \geq 1$. For each $d \geq 1$ there exists a $(p^{(2d-1)r}, p^{dr}, p^r)$ BS on any group G_d of order p^{2dr} and exponent at most p^d relative to any subgroup $U_d \cong \mathbb{Z}_p^r$, where, for $d > 1$, G_d/U_d contains a subgroup of index p^r and exponent at most p^{d-1}.*

For example, take $G_d = \mathbb{Z}_{p^d}^{2r}$ in Corollary 5.6 (so that the condition on G_d/U_d is always satisfied) and let $P(r)$ be the number of partitions of the positive integer r. Then Theorem 2.8 shows that for each $d \geq 1$ and for any prime p there exists a $(p^{2dr}, p^r, p^{2dr}, p^{(2d-1)r})$ semi-regular RDS in $P(r)$ nonisomorphic groups of rank $2r$ relative to any subgroup $\mathbb{Z}_p^r$. Two such groups are $\mathbb{Z}_{p^{d+1}}^r \times \mathbb{Z}_{p^d}^r$ and $\mathbb{Z}_{p^{d+r}} \times \mathbb{Z}_{p^d}^{2r-1}$. This shows that the group rank of the underlying BS, and also of the resulting RDSs, can remain fixed at $2r$ as the group order grows without bound.

Compare Theorems 5.1 and 5.4 as two possible outcomes of applying Theorem 3.5 to the (p^r, p^r, p^r) BS of Corollary 2.6. To derive Theorem 5.1 we constrained the group exponent at each stage to be p whereas for Theorem 5.4 we allowed the group exponent to grow by a factor of p at each stage. One consequence is that after applying Theorem 2.8 to these BSs, the minimum group rank for the semi-regular RDSs arising from Theorem 5.4 can be as small as $2r$ but for those arising from Theorem 5.1 must be at least $(d+1)r$. On the other hand the group exponent for the RDSs arising from Theorem 5.1 can be as much as p^{dr+1} but for those arising from Theorem 5.4 must be at most p^{d+r}. This illustrates a trade-off between a small rank and a high maximum exponent for the resulting RDSs. It is possible to derive other BSs representing intermediate points between the extremes of Theorems 5.1 and 5.4 by constraining the exponent of the group on which the BS is defined to be at most p^c for a fixed value of c in the range $1 \leq c \leq d$ (see Corollary 7.7 of Davis and Jedwab (1997)).

In general, given a single initial example of a BS (which could comprise just one building block) we can obtain an infinite family of BSs using Theorem 3.5. In some cases we can also produce further families of BSs by "contracting" the initial BS prior to recursive application of Theorem 3.5 (as described in Davis and Jedwab (1997) and Davis, Jedwab and Mowbray (1998)). Apart from the (p^r, p^r, p^r) BS of Corollary 2.6 discussed as an extended example in this section, we have the following initial examples of BSs:

Example 5.7. The following BSs exist:

(a) A $(p^r, p^{r/2}, 1)$ BS on $\mathbb{Z}_p^{2r}$ relative to $\mathbb{Z}_p^r$, where p is an odd prime and $r \geq 1$.

(b) A $(2^r, 2^{r/2}, 1)$ BS on $\mathbb{Z}_4^r$ relative to $\mathbb{Z}_2^r$, where $r \geq 1$.

(c) A $(2^{2r-1}, 2^{(2r-1)/2}, 1)$ BS on $\mathbb{Z}_4^r \times G$ relative to the subgroup $\mathbb{Z}_2^r$ of $\mathbb{Z}_4^r$, where $r \geq 1$ is odd and G is any group of order 2^{r-1} and exponent at most 4.

(d) A $(8, 4, 2)$ BS on $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ relative to the subgroup $\mathbb{Z}_2^2$ of $\mathbb{Z}_4^2$.

(e) A $(8, 4, 2)$ BS on $\mathbb{Z}_2 \times \mathbb{Z}_4^2 \times \mathbb{Z}_2$ relative to the subgroup $\mathbb{Z}_2^3$ of $\mathbb{Z}_2 \times \mathbb{Z}_4^2$.

(f) A $(2^p(2^p-1)^2, 2^{p/2}(2^p-1), 1)$ BS on $\mathbb{Z}_4^p \times \mathbb{Z}_{2^p-1}^2$ relative to the subgroup $\mathbb{Z}_2^p$ of $\mathbb{Z}_4^p$, where $2^p - 1$ is prime.

(g) A $(2^{2r}3, 2^r\sqrt{3}, 1)$ BS on $\mathbb{Z}_{2^r}^2 \times \mathbb{Z}_3^2$ relative to the subgroup $\mathbb{Z}_3$ of $\mathbb{Z}_3^2$, where $r \geq 1$.

Cases (a) and (b) are equivalent to semi-regular RDSs constructed in Jungnickel (1982), case (c) is equivalent to semi-regular RDSs constructed in Chen, Ray-Chaudhuri and Xiang (1996), and cases (f) and (g) are equivalent to semi-regular RDSs constructed in Davis, Jedwab and Mowbray (1998). Case (d) is contained in Example 2.12 and case (e) is given in Davis and Jedwab (1999a). Further initial examples of BSs on groups whose order is not a prime power are described in Davis, Jedwab and Mowbray (1998).

The families of BSs arising from these examples under recursive application of Theorem 3.5, and the semi-regular RDSs then arising under Theorem 2.8, are described in Davis and Jedwab (1997) for cases (a), (b), (c) and (d), in Davis and Jedwab (1999a) for case (e), and in Davis, Jedwab and Mowbray (1998) for cases (f) and (g). Certain extensions to Lemmas 3.7 and 5.5 are required to handle some of these examples. In particular, cases (b), (c), (d), (e) and (f) involve a BS on a group G relative to a subgroup $U \cong \mathbb{Z}_p^r$ such that U is contained in a subgroup of G not isomorphic to $\mathbb{Z}_p^r$, and this must be taken into consideration when Theorem 3.5 is applied recursively. We note that for cases (f) and (g) we can obtain additional families of semi-regular RDSs by means of a product construction, see Davis, Jedwab and Mowbray (1998).

Finally we remark that when the subgroup U has order 2 the pattern of existence for semi-regular RDSs is very rich. We have already seen examples in Corollary 4.6 (b) of BSs which give rise to such RDSs under Theorem 2.8 and Davis and Jedwab (1997) gives recursive constructions for further families originating with the covering EBSs of Corollary 4.6 (a).

6. Open Questions

- The construction of Hadamard difference sets described in Section 4 relies on the existence of a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on a group of odd order m^2. Can we find any examples apart from those of Theorem 4.4 and their compositions under Theorem 4.5?
- The construction of Hadamard difference sets described in Section 4 for which $n = N^2$ is not a prime power depends on Theorem 4.5. Is there an analogous composition theorem for McFarland difference sets or for Chen difference sets?
- The construction of Chen difference sets with $q = 2^r$ summarised in Corollary 4.9 (b), when applied to the case $q = 2$, does not deal with all the groups covered by Corollary 4.3 (d) even though the parameters then coincide. Does this point to the construction of Chen difference sets in new groups with $q = 2^r > 2$?
- The construction of McFarland difference sets described in Section 4 includes results specific to the case $q = 4$ (which are summarised in Corollary 4.3 (b) and contribute the existence part of Theorem 1.4). Can we find comparable results for McFarland difference sets with $q = 2^r > 4$?
- Chen (1999) gives necessary conditions on the parameters of certain covering EBSs. Can we find difference sets in new parameter families by constructing covering EBSs satisfying these conditions?
- Ionin (1998) gives a recursive construction for symmetric designs relying on building sets and covering EBSs and as a consequence produces seven new infinite families of symmetric designs. Can we apply this method to find further new symmetric designs?

References

Arasu, K.T., Davis, J.A., Jedwab, J. and Sehgal, S.K. (1993) New constructions of Menon difference sets. *J. Combin. Theory (A)* **64**, 329–336.

Arasu, K.T. and Sehgal, S.K. (1995) Some new difference sets, *J. Combin. Theory (A)* **69**, 170–172.

Beth, T, Jungnickel, D. and Lenz, H. (1999) *Design Theory*, Cambridge University Press, Cambridge, 2nd edition, to appear.

Chen, Y.Q. (1997) On the existence of abelian Hadamard difference sets and a new family of difference sets, *Finite Fields Appl.* **3**, 234–256.

Chen, Y.Q. (1998) A construction of difference sets, *Designs, Codes and Cryptography* **13**, 247–250.

Chen, Y.Q. (1999) On a family of covering extended building sets, *Designs, Codes and Cryptography*, to appear.

Chen, Y.Q., Ray-Chaudhuri, D.K. and Xiang, Q. (1996) Constructions of partial difference sets and relative difference sets using Galois rings II, *J. Combin. Theory (A)* **76**, 179–196.

Davis, J.A. and Jedwab, J. (1996) A survey of Hadamard difference sets, in K.T. Arasu et al. (eds.), *Groups, Difference Sets and the Monster*, de Gruyter, Berlin-New York, pp. 145–156.

Davis, J.A. and Jedwab, J. (1997) A unifying construction for difference sets, *J. Combin. Theory (A)* **80**, 13–78.

Davis, J.A. and Jedwab, J. (1999) Some recent developments in difference sets, in F.C. Holroyd et al. (eds.), *Combinatorial Designs and their Applications*, Chapman & Hall/CRC Press Research Notes in Mathematics, CRC Press, Boca Raton, pp. 83–102.

Davis, J.A. and Jedwab, J. (1999a) A new family of relative difference sets in 2-groups, *Designs, Codes and Cryptography*, to appear.

Davis, J.A., Jedwab, J. and Mowbray, M. (1998) New families of semi-regular relative difference sets, *Designs, Codes and Cryptography* **13**, 131–146.

van Eupen, M. and Tonchev, V.D. (1997) Linear codes and the existence of a reversible Hadamard difference set in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5^4$, *J. Combin. Theory (A)* **79**, 161–167.

Ionin, Y.J. (1998) Building symmetric designs with building sets, preprint, Central Michigan University.

Jedwab, J. (1992) Generalized perfect arrays and Menon difference sets, *Designs, Codes and Cryptography* **2**, 19–68.

Jungnickel, D. (1982) On automorphism groups of divisible designs, *Canad. J. Math.* **34**, 257–297.

Jungnickel, D. (1992) Difference sets, in J.H. Dinitz and D.R. Stinson (eds.), *Contemporary Design Theory: a Collection of Surveys*, Wiley, New York, pp. 241–324.

Jungnickel, D. and Pott, A. (1999) Difference sets: an introduction, this volume.

Jungnickel, D. and Schmidt, B. (1997) Difference sets: an update, in J.W.P. Hirschfeld, S.S. Magliveras and M.J. de Resmini (eds.), *Geometry, Combinatorial Designs and Related Structures*, Cambridge University Press, Cambridge, pp. 89–112.

Jungnickel, D. and Schmidt, B. (1998) Difference sets: a second update, *Rend. Circ. Mat. Palermo (2) Suppl.* **53**, 89–118.

Kraemer, R.G. (1993) Proof of a conjecture on Hadamard 2-groups, *J. Combin. Theory (A)* **63**, 1–10.

Ma, S.L. and Schmidt, B. (1995) The structure of the abelian groups containing McFarland difference sets, *J. Combin. Theory (A)* **70**, 313–322.

Ma, S.L. and Schmidt, B. (1997) A sharp exponent bound for McFarland difference sets with $p = 2$, *J. Combin. Theory (A)* **80**, 347–352.

Pott, A. (1995) *Finite Geometry and Character Theory*, Lecture Notes in Mathematics **1601**, Springer, Berlin.

Pott, A. (1996) A survey on relative difference sets, in K.T. Arasu et al. (eds.), *Groups,* *Difference Sets and the Monster*, de Gruyter, Berlin-New York, pp. 195–232.

Turyn, R.J. (1965) Character sums and difference sets, *Pacific J. Math.* **15**, 319–346.

Turyn, R.J. (1984) A special class of Williamson matrices and difference sets, *J. Combin. Theory (A)* **36**, 111–115.

Wilson, R.M. and Xiang, Q. (1997) Constructions of Hadamard difference sets, *J. Combin. Theory (A)* **77**, 148–160.

Xia, M.-Y. (1992) Some infinite classes of special Williamson matrices and difference sets, *J. Combin. Theory (A)* **61**, 230–242.

Xiang, Q. (1999) Recent results on difference sets with classical parameters, this volume.

Xiang, Q. and Chen, Y.Q. (1996) On Xia's construction of Hadamard difference sets, *Finite Fields Appl.* **2**, 87–95.