[48] E. Spence. A family of difference sets. *J. Combin. Theory (A)*, **22**:103–106, 1977.

[49] R.J. Turyn. Character sums and difference sets. *Pacific J. Math.*, **15**:319–346, 1965.

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

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

[52] Q. Xiang and Y.Q. Chen. On Xia's construction of Hadamard difference sets. 1994. Preprint, Ohio State University.

[31] S.L. Ma and A. Pott. Relative difference sets, planar functions and generalized Hadamard matrices. *J. Algebra*, **175**:505–525, 1995.

[32] S.L. Ma and B. Schmidt. Difference sets corresponding to a class of symmetric designs. 1995. Preprint, National University of Singapore.

[33] S.L. Ma and B. Schmidt. On (p^a, p, p^a, p^{a-1})-relative difference sets. *Designs, Codes and Cryptography*, **6**:57–72, 1995.

[34] S.L. Ma and B. Schmidt. A sharp exponent bound for McFarland difference sets with $p = 2$. 1995. Preprint, National University of Singapore.

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

[36] S.J. Martin, M.A. Butler, and C.E. Land. Ferroelectric optical image comparator using PLZT thin films. *Electron. Lett.*, **24**:1486–1487, 1988.

[37] R.L. McFarland. A family of difference sets in non-cyclic groups. *J. Combin. Theory (A)*, **15**:1–10, 1973.

[38] D.B. Meisner. *Menon designs and related difference sets.* PhD thesis, University of London, 1991.

[39] D.B. Meisner. Families of Menon difference sets. *Annals of Discrete Math.*, **52**:365–380, 1992.

[40] D.B. Meisner. New classes of groups containing Menon difference sets. 1993. Preprint.

[41] D.B. Meisner. A difference set construction of Turyn adapted to semi-direct products. In K.T. Arasu et al., editors, *Groups, Difference Sets and the Monster*, pages 169–174. de Gruyter, Berlin-New York, 1996.

[42] A. Pott. On the structure of abelian groups admitting divisible difference sets. *J. Combin. Theory (A)*, **65**:202–213, 1994.

[43] A. Pott. A survey on relative difference sets. In K.T. Arasu et al., editors, *Groups, Difference Sets and the Monster*, pages 195–232. de Gruyter, Berlin-New York, 1996.

[44] B. Schmidt. On (p^a, p^b, p^a, p^{a-b})-relative difference sets. 1994. Preprint, Universität Augsburg.

[45] J. Seberry and M. Yamada. Hadamard matrices, sequences, and block designs. In J.H. Dinitz and D.R. Stinson, editors, *Contemporary Design Theory: a Collection of Surveys*, pages 431–560. Wiley, New York, 1992.

[46] G.K. Skinner. X-ray imaging with coded masks. *Scientific American*, **259**:66–71, August 1988.

[47] K.W. Smith. Non-abelian Hadamard difference sets. *J. Combin. Theory (A)*, **70**:144–156, 1995.

[14] J.F. Dillon. A survey of difference sets in 2-groups. Presented at Marshall Hall Memorial Conference, Vermont, 1990.

[15] J.F. Dillon. *Elementary Hadamard difference sets.* PhD thesis, University of Maryland, 1974.

[16] J.F. Dillon. Variations on a scheme of McFarland for noncyclic difference sets. *J. Combin. Theory (A)*, **40**:9–21, 1985.

[17] J.E.H. Elliott and A.T. Butson. Relative difference sets. *Illinois J. Math.*, **10**:517–531, 1966.

[18] M. van Eupen and V.D. Tonchev. Linear codes and the existence of a reversible Hadamard difference set in $Z_2 \times Z_2 \times Z_5^4$. 1995. Preprint, Michigan Technological University.

[19] E.E. Fenimore and T.M. Cannon. Coded aperture imaging with uniformly redundant arrays. *Applied Optics*, **17**:337–347, 1978.

[20] M.J. Ganley. On a paper of Dembowski and Ostrom. *Arch. Math.*, **27**:93–98, 1976.

[21] J.E. Hershey and R. Yarlagadda. Two-dimensional synchronisation. *Electron. Lett.*, **19**:801–803, 1983.

[22] A.J. Hoffman. Cyclic affine planes. *Canad. J. Math.*, 4:295–301, 1952.

[23] J. Jedwab. Generalized perfect arrays and Menon difference sets. *Designs, Codes and Cryptography*, **2**:19–68, 1992.

[24] D. Jungnickel. On automorphism groups of divisible designs. *Canad. J. Math.*, **34**:257–297, 1982.

[25] D. Jungnickel. Difference sets. In J.H. Dinitz and D.R. Stinson, editors, *Contemporary Design Theory: a Collection of Surveys*, pages 241–324. Wiley, New York, 1992.

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

[27] E.S. Lander. *Symmetric Designs: an Algebraic Approach.* London Mathematical Society Lecture Notes Series 74. Cambridge University Press, Cambridge, 1983.

[28] K.H. Leung and S.L. Ma. Constructions of partial difference sets and relative difference sets on p-groups. *Bull. London Math. Soc.*, **22**:533–539, 1990.

[29] R.A. Liebler. The inversion formula. *J. Combin. Math. and Combin. Computing*, **13**:143–160, 1993.

[30] R.A. Liebler and K.W. Smith. On difference sets in certain 2-groups. In D. Jungnickel and S.A. Vanstone, editors, *Coding Theory, Design Theory, Group Theory*, pages 195–212. Wiley, New York, 1993.

for which M is not a central subgroup. These fall outside the scope of Theorem 9.2 (ii).

Acknowledgement We are grateful to Miranda Mowbray for her careful reading of the manuscript and for many helpful comments.

References

[1] S. Alquaddoomi and R.A. Scholtz. On the nonexistence of Barker arrays and related matters. *IEEE Trans. Information Theory*, **35**:1048–1057, 1989.

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

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

[4] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*. Cambridge University Press, Cambridge, 1986.

[5] Y.Q. Chen, D.K. Ray-Chaudhuri, and Q. Xiang. Constructions of partial difference sets and relative difference sets using Galois rings II. 1995. Preprint, Ohio State University.

[6] J.A. Davis. A note on products of relative difference sets. *Designs, Codes and Cryptography*, **1**:117–119, 1991.

[7] J.A. Davis. A result on Dillon's conjecture in difference sets. *J. Combin. Theory (A)*, **57**:238–242, 1991.

[8] J.A. Davis. Construction of relative difference sets in p-groups. *Discrete Mathematics*, **103**:7–15, 1992.

[9] J.A. Davis. An exponent bound for relative difference sets in p-groups. *Ars Combinatoria*, **34**:318–320, 1992.

[10] J.A. Davis and J. Jedwab. Recursive construction for difference sets. *Bulletin of the Institute of Combinatorics and its Applications*, **13**:128, 1995. Research announcement.

[11] J.A. Davis and J. Jedwab. A survey of Hadamard difference sets. In K.T. Arasu et al., editors, *Groups, Difference Sets and the Monster*, pages 145–156. de Gruyter, Berlin-New York, 1996.

[12] J.A. Davis and S.K. Sehgal. Using the Simplex code to construct relative difference sets in 2-groups. 1994. Preprint, University of Richmond.

[13] J.A. Davis and K.W. Smith. A construction of difference sets in high exponent 2-groups using representation theory. *J. Algebraic Combin.*, **3**, no. 2:137–151, 1994.

group $G_d = \langle x, y \mid x^{2^{d+3}} = y^{2^{d-1}} = 1, yxy^{-1} = x^{2^{d+2}+1} \rangle$ for each $d \geq 2$, and G_d does not contain a normal abelian subgroup of order 2^{d+c} and exponent at most 2^c for any c satisfying $1 \leq c \leq d$. Furthermore the existence of a Hadamard difference set in G_d cannot rely on the existence of a covering EBS on an abelian group contained as a normal subgroup in G_d because Theorem 9.1 (ii) would then give a Hadamard difference set in the abelian group $\langle x, y \mid x^{2^{d+3}} = y^{2^{d-1}} = 1, yx = xy \rangle$ of order 2^{2d+2} and exponent 2^{d+3}, which is ruled out by Turyn's exponent bound [49].

This provides the motivation for our second (more speculative) approach to nonabelian groups, namely to generalise the definition of building block, BS and covering EBS to allow the group G in Theorem 9.1 to be nonabelian. Liebler [29] has promoted the use of representation theory to study difference sets in nonabelian groups, as a natural generalisation of the use of character theory for abelian groups. A representation ϕ of a group G is a homomorphism from G to the multiplicative group of $s \times s$ matrices, where the degree s of the representation is determined by G. Lemma 1.1 (i) generalises to: the k-element subset D of a group G of order v is a (v, k, λ, n)-difference set in G if and only if $\phi(D)\overline{\phi(D)}' = \sqrt{n} I_s$ for every nontrivial irreducible representation ϕ of G, where $\overline{\phi(D)}'$ is the conjugate transpose of $\phi(D)$ and I_s is the $s \times s$ identity matrix. We might define a building block B in a group G with modulus m to be a subset of G such that for all nontrivial irreducible representations ϕ, the representation sum $\phi(B) = \sum_{g \in B} \phi(g)$ is either 0 or satisfies $\phi(B)\overline{\phi(B)}' = m I_s$. Then a (a, m, t) building set on G relative to U would be a collection of t building blocks in G with modulus m, each containing a elements, such that for every nontrivial irreducible representation ϕ of G exactly one building block has nonzero representation sum if ϕ is nontrivial on U and no building block has nonzero representation sum if ϕ is trivial on U. We could similarly extend the definition of EBS. Although we believe this approach could be fruitful, it will not allow us to replace "central" by "normal" in Theorem 9.1 (i), even when G is still assumed to be abelian. For example, by Theorem 4.2 there is a $(2, 2, 2)$ BS on Z_2^2 relative to Z_2, but there is no $(4, 2, 4, 2)$ RDS in D_8 (the dihedral group of order 8) relative to the central subgroup of order 2 even though D_8 contains a normal subgroup of index 2 isomorphic to Z_2^2. The difficulty appears to arise because the restriction of an irreducible representation to a normal subgroup is not necessarily irreducible.

The following construction of Meisner [39] for Hadamard difference sets (which generalises the result of applying Theorem 2.4 to the case $h = t = 1$ of Theorem 3.2) may be of importance in formulating a general nonabelian approach to the construction of difference sets and semi-regular RDSs involving representation theory.

Theorem 9.3 *Suppose that there exists a $(4N^2, 2, 4N^2, 2N^2)$ semi-regular RDS in a group H of order $8N^2$ relative to a central subgroup $\langle x \rangle$ of order 2. Suppose also that there exists a Hadamard difference set with parameter N in $H/\langle x \rangle$. Then there exists a Hadamard difference set with parameter $2N$ in any group G' containing H as a subgroup of index 2 for which x is a central element of G'.*

Meisner [41], [40], [39] has shown that Theorem 9.3 (together with a partial generalisation of Theorem 4.3) can be used to construct Hadamard difference sets in certain nonabelian groups containing a normal abelian subgroup M, as used in Theorem 9.2 (ii),

the case $d-1$ to be true. By Corollary 7.3 (i) there is a $(2^{d+c-1}m^2, 2^d m, 2^{d-c+1})$ BS on $G_{d,c} \times M$ relative to any subgroup $U_{d,c}$ of order 2, and by the inductive hypothesis there is a $(2^{d+c-2}m^2, 2^{d-1}m, 2^{d-c+1}, -)$ covering EBS on $(G_{d,c}/U_{d,c}) \times M$ (since $c \leq d-1$). The case d then follows from Theorem 3.2.

For (ii), the case $d = 0$ has already been proved in Corollary 6.7 (iv). All other cases are obtained by applying Theorem 9.1 (ii) to the covering EBSs of (i). □

Theorem 9.2 (ii) establishes the existence of Hadamard difference sets in large classes of nonabelian groups. Each value of c in Theorem 9.2 (ii) produces examples which are not found at any other value of c. For larger values of c the required order of the central subgroup becomes larger but the group is allowed to have smaller rank. The case $c = d$ of Theorem 9.2 (i), for which the number of building blocks is 4, was given in Corollary 6.7 (iii) and used to construct Hadamard difference sets in abelian groups in Corollary 6.7 (iv). The cases $c < d$ of Theorem 9.2 (i) do not improve on Corollary 6.7 (iv) for abelian groups but can be used to deal with many nonabelian groups, as described. It would be interesting to know in which 2-groups the existence of a Hadamard difference set (currently an open problem for groups of order at least 256) remains unknown after taking into account Theorem 9.2 (ii) and the two known nonexistence results for nonabelian 2-groups (see [11]). In particular, how many of the 56,092 groups of order 256 remain open?

Theorem 9.1 (i) and (ii) require G to be a central subgroup of G'. The method of Dillon [16] shows that this condition can sometimes be replaced by the weaker condition that G is a normal abelian subgroup of G'. Under this condition the proof of the Theorem is unchanged with respect to the group ring element $\sum_{i \neq j} k_i B_i B_j^{(-1)} k_j^{-1}$, and it suffices to force the group ring element $\sum_i k_i B_i B_i^{(-1)} k_i^{-1} = \sum_i (k_i B_i k_i^{-1})(k_i B_i k_i^{-1})^{(-1)}$ to reduce to $\sum_i B_i B_i^{(-1)}$. This will clearly be the case if the coset representatives k_i can be chosen so that $\{k_i B_i k_i^{-1}\} = \{B_i\}$, in other words so that the map $B_i \mapsto k_i B_i k_i^{-1}$ is a permutation of the building blocks B_i. (When G is contained in the centre of G' the permutation is trivial.) Dillon's conjecture [15] (expressed in the language of this paper) is that the coset representatives can always be chosen to ensure a permutation of the building blocks of a $(2^d, 2^d, 2^{d+1}, -)$ covering EBS on Z_2^{d+1}, which would imply that a Hadamard difference set with $N = 2^d$ exists in any group of order 2^{2d+2} containing a normal subgroup isomorphic to Z_2^{d+1}. Davis [7] gave a scheme for choosing coset representatives for this covering EBS which proves some cases of Dillon's conjecture and Meisner [38] gave further supporting evidence, but the conjecture remains open. (The scheme of [7] can be modified to deal with other covering EBSs, subject to the additional condition that each building block $k_i B_i k_i^{-1}$ is contained in the original collection $\{B_i\}$.)

The case $m = 1$ of Theorem 9.2 (i) constructs a $(2^{d+c-1}, 2^d, 2^{d-c+2}, -)$ covering EBS on any abelian group of order 2^{d+c} and exponent at most 2^c, where $1 \leq c \leq d$. Suppose it were possible to choose coset representatives to ensure a permutation of building blocks for each value of c in this range (the case $c = 1$ being Dillon's conjecture), so that the case $m = 1$ of Theorem 9.2 (ii) would remain true with "central" replaced by "normal abelian". This would still not deal with every 2-group containing a Hadamard difference set, because Davis and Smith [13] have constructed a Hadamard difference set with $N = 2^d$ in the

and therefore normal in G', substitution for $B_i B_j^{(-1)}$ in S gives the sum $\sum_{i \neq j} c_{ij} k_i k_j^{-1} G$. The terms of this sum having $j = 1$ are $\frac{a}{|G|}(a \pm m) \sum_{u \neq 1} k_u G$. Likewise the terms of the sum having $i = 1$ are $\sum_{j \neq 1} c_{1j} 1_{G'} k_j^{-1} G = \frac{a}{|G|}(a \pm m) \sum_{u \neq 1} k_u G$, since $\sum_{j \neq 1} k_j^{-1} G = \sum_{u \neq 1} k_u G$. The remaining terms of the sum are $\frac{a^2}{|G|} \sum_{i \neq j | i,j \neq 1} k_i k_j^{-1} G$. Regarding $k_i k_j^{-1} G$ as a coset of G, we can write $k_i k_j^{-1} G$ as the product of cosets $(k_i G)(k_j G)^{-1}$. Since the cosets $\{k_u G \mid u \neq 1\}$ form a $(h, h-1, h-2, 1)$-difference set in G'/G (the complement of the trivial $(h, 1, 0, 1)$-difference set $\{k_1 G\}$ in G'/G), the remaining terms of the sum are $\frac{a^2}{|G|}(h-2) \sum_{u \neq 1} k_u G = \frac{a^2}{|G|}(h-2)(G'-G)$. Therefore $S = \frac{a}{|G|}(ah \pm 2m)(G'-G) = \lambda(G'-G)$, which holds whether G' is nonabelian or abelian. This completes the proof. □

The constructions of difference sets and semi-regular RDSs in abelian groups given in this paper can be extended to numerous nonabelian groups using Theorem 9.1 (including the special case when G' can be written in the form $G \times K$ for some group K.) In the following discussion we shall concentrate on the construction of difference sets in nonabelian groups using Theorem 9.1 (ii), but equally we can obtain semi-regular RDSs in many nonabelian groups by applying Theorem 9.1 (i) to the BS families constructed in Corollaries 7.3 and 7.7–7.10.

We begin by using the covering EBSs constructed in Theorem 5.2 to obtain difference sets in nonabelian groups with parameters from the McFarland family, Spence family or the new family (4). Applying Theorem 9.1 (ii) to these covering EBSs shows that Corollary 5.3 remains true for nonabelian groups provided each occurrence of "subgroup" is replaced by "central subgroup". For example, Corollary 5.3 (i) becomes: for each $d \geq 0$, there exists a McFarland difference set with $q = p^r$ in any (possibly nonabelian) group of order $q^{d+1}(\frac{q^{d+1}-1}{q-1} + 1)$ containing a central subgroup isomorphic to $Z_p^{(d+1)r}$, where p is prime and $r \geq 1$. This result was given by Dillon [16] and was used in Section 2 to introduce building blocks.

We could similarly apply Theorem 9.1 (ii) to the covering EBSs of Corollary 6.7 (iii) to obtain difference sets in nonabelian groups with Hadamard parameters. But we can obtain more general results than this for Hadamard difference sets by taking advantage of a family of BSs constructed in Section 8:

Theorem 9.2 *Let M be either the trivial group or the group $\prod_i Z_{3^{\alpha_i}}^2 \times \prod_j Z_{p_j}^4$, where $\alpha_i \geq 1$ and where p_j is a prime congruent to 3 modulo 4 or $p_j = 5$, and let $|M| = m^2$. Then the following exist:*

(i) *A $(2^{d+c-1} m^2, 2^d m, 2^{d-c+2}, -)$ covering EBS on $G_{d,c} \times M$, where d and c satisfy $1 \leq c \leq d$ and $G_{d,c}$ is any abelian group of order 2^{d+c} and exponent at most 2^c.*

(ii) *A Hadamard difference set with $N = 2^d m$ in any (possibly nonabelian) group $G_d \times M$ of order $2^{2d+2} m^2$, where either $d = 0$ or G_d contains a central subgroup of order 2^{d+c} and exponent at most 2^c such that d and c satisfy $1 \leq c \leq d$.*

Proof: For (i), the proof is by induction on d. The case $c = d$ has already been proved in Corollary 6.7 (iii), so the case $d = 1$ is true and we can take $c \leq d - 1$. Assume

12. Lemma 1.1 (ii) describes the key property of a semi-regular RDS in G relative to U exploited in this paper: for nonprincipal characters χ of G, the character sum has fixed modulus when χ is nonprincipal on U and is 0 when χ is principal on U. Since the same property holds for semi-regular divisible difference sets [42], can these be dealt with systematically using the methods of this paper? (See the introductory remarks in Section 2 for an example.)

We have seen in Section 1 that the existence pattern for difference sets in nonabelian groups is fundamentally different from that in abelian groups. We now consider how to modify the methods of this paper to deal with nonabelian groups, dropping the implicit assumption that all groups are abelian. Our first approach is based on techniques due to Dillon [16], and generalises Theorems 2.2 and 2.4:

Theorem 9.1 *Let G be an abelian group.*

(i) *Suppose there exists a $(a, \sqrt{at}, t)$ BS on 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 (possibly nonabelian) group containing a central subgroup of index t isomorphic to G.*

(ii) *Suppose there exists a $(a, m, h, \pm)$ covering EBS on G. Then there exists a $(h|G|, ah \pm m, ah \pm m - m^2, m^2)$-difference set in any (possibly nonabelian) group G' containing a central subgroup of index h isomorphic to G.*

Proof: We give the proof of (ii), the proof of (i) being similar. Let $k_1 = 1_{G'}, k_2, \ldots k_h \in G'$ be coset representatives of G in G'. Let $\{B_i\}$ be a $(a, m, h, \pm)$ covering EBS on G, where the building block containing $a \pm m$ elements is B_1, and form the subset $D = \sum_i k_i B_i$ of G'. If G' is abelian then we already know Theorem 2.4 and the proof of Lemma 2.3 that D is a difference set in G' with the stated parameters. By the characterisation of difference sets in the group ring $Z[G']$ this is equivalent to $DD^{(-1)} = m^2 1_{G'} + \lambda G'$, where $\lambda = ah \pm m - m^2 = \frac{a}{|G|}(ah \pm 2m)$ (using the relationship between covering EBS parameters given after Theorem 2.4 for the last equality). We can therefore obtain the result by showing that the same equation for $DD^{(-1)}$ holds when G' is nonabelian as when G is abelian. By the definition of D we can write $DD^{(-1)}$ as the sum of two group ring elements:

$$DD^{(-1)} = \sum_i k_i B_i B_i^{(-1)} k_i^{-1} + \sum_{i \neq j} k_i B_i B_j^{(-1)} k_j^{-1}.$$

Since G is a central subgroup of G', the first group ring element $\sum_i k_i B_i B_i^{(-1)} k_i^{-1}$ is equal to $\sum_i B_i B_i^{(-1)}$ whether G' is nonabelian or abelian, as required.

It remains to consider the second group ring element $S = \sum_{i \neq j} k_i B_i B_j^{(-1)} k_j^{-1}$, taking $i \neq j$. For all nonprincipal characters χ of G we have $\chi(B_i B_j^{(-1)}) = \chi(B_i)\overline{\chi(B_j)} = 0$, where the last equality uses the definition of covering EBS. Therefore $B_i B_j^{(-1)} = c_{ij} G$ for some integer c_{ij}, and by a counting argument $c_{ij} = |B_i||B_j|/|G|$. The definition of covering EBS gives $c_{ij} = a(a \pm m)/|G|$ when i or j is 1 and $c_{ij} = a^2/|G|$ otherwise. Since G is central

1. Can the unifying framework of this paper be extended to encompass all known parameter families of difference sets, including Projective Geometries, the Paley-Hadamard family and the Twin Prime Power family?

2. Can we find suitable BSs and covering EBSs for use in Theorem 3.2 to construct difference sets via Theorem 2.4 whose parameters do not belong to any currently known family?

3. The construction for Hadamard difference sets in Section 6 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 6.6 and their compositions under Theorem 6.5?

4. A construction for McFarland difference sets with $q = 2^r$ in Section 5 relies on the existence of a $(2q^d, q^d, q^d/2)$ BS on a group G of order $2q^{d+1}$ relative to a subgroup of order q. Can we find any examples for $q > 4$ apart from on $G = Z_2^{(d+1)r+1}$ and $Z_4 \times Z_2^{(d+1)r-1}$? In particular, can we find a $(16, 8, 4)$ BS on a group of order 128 and exponent 4 (other than $Z_4 \times Z_2^5$) relative to a subgroup of order 8, or a $(32, 16, 8)$ BS on a group of order 512 and exponent 4 (other than $Z_4 \times Z_2^7$) relative to a subgroup of order 16?

5. Is there a $(320, 88, 24, 64)$-difference set in $Z_4^3 \times Z_5$, the single exceptional group of Corollary 5.3 (iv)? Theorem 3.2 would establish existence for this group if a $(16, 8, 4)$ BS on Z_4^3 relative to either Z_4 or Z_2^2 could be found.

6. Can the exponent bound of Corollary 5.5 for the new family of difference set parameters (4) be improved?

7. Examples of semi-regular RDSs are known for which the forbidden subgroup is not elementary abelian (see the comment following Theorem 8.3). Can Theorem 4.3 be modified to construct BSs relative to a subgroup which is not elementary abelian to bring these RDSs within the framework of this paper?

8. The construction of families of BSs in Section 7 and semi-regular RDSs in Section 8 relies on the existence of initial BSs. Can we find any examples apart from those of Theorem 7.6 and those mentioned after Corollary 7.10? In particular, is the $(8, 4, 2)$ BS of Theorem 7.6 (iv) the case $r = 2$ of an infinite family of BSs relative to a subgroup $U \cong Z_2^r$?

9. The only BSs we have found on groups whose order is not a prime power are those of Corollary 7.3, relative to a subgroup U of order 2. Can we find examples in which U has larger order? If we could do so for $U \cong Z_p^r$ then we would be able to recursively construct families of such BSs (and semi-regular RDSs) using Theorem 7.11.

10. Is there a $(p^{2d+1}, p, p^{2d+1}, p^{2d})$ semi-regular RDS in $Z_{p^{d+1}}^2$ or $U \times Z_{p^{d+1}} \times Z_{p^d}$ relative to a subgroup U of order p, these being the two exceptional cases of Corollary 8.2 (ii)?

11. We have argued in Section 8 that it is more appropriate to consider exponent bounds for a BS than for a RDS. What can be said about a (p^{d+w}, p^d, p^{d-w}) BS relative to a subgroup of order p^r?

Previously it was known that G could be any group of rank at least 9 using (D) with $\alpha = 3$, $d = 2$, or the group $Z_4^2 \times Z_2 \times Z_8^4$ of rank 7 (where U is contained in the first two direct factors) using the RDS product construction on (A) with $\alpha = 3$ and (E) with $\alpha = 2$, $d = 3$. We can now use part (v) of Corollary 8.4 to include three groups of rank 4, namely $Z_{32} \times Z_{16}^3$ for any U, and $Z_{64} \times Z_{16}^2 \times Z_8$ and $Z_{32}^2 \times Z_{16} \times Z_8$ for any U which does not intersect the last direct factor in a nonidentity element, as well as many new groups of rank 5 to 8. Part (v) also shows that G can be any group of exponent at most 16 and U any subgroup.

Finally we apply Theorem 2.2 to the Corollaries of Section 7 for p odd. This also gives substantial improvements over previous results.

Corollary 8.5 *Let p be an odd prime. There exists a $(p^{2dr+j}, p^r, p^{2dr+j}, p^{(2d-1)r+j})$ semi-regular RDS in the following groups G_d of order $p^{(2d+1)r+j}$ relative to any subgroup $U_d \cong Z_p^r$, where j and r satisfy $0 \le j < 2r$:*

(i) When j is even. *For each $d \ge 1$, any group G_d containing a subgroup S_d of index $p^{r+j/2}$ and exponent at most p^d such that, for $d > 1$, S_d/U_d contains a subgroup of index p^r and exponent at most p^{d-1} and such that, for $j > 0$ and $d > 1$, $\mathrm{rank}(S_d/U_d) \ge 2r + j/2$.*

(ii) When j<r. *For each $d \ge 2$, any group G_d containing a subgroup S_d of index p^r and exponent at most p^{d-1} such that, for $d > 2$, S_d/U_d contains a subgroup of index p^r and exponent at most p^{d-2} and such that, for $d > 2$, $\mathrm{rank}(S_d/U_d) \ge 4r + j$.*

(iii) When j≥r. *For each $d \ge 1$, any group G_d containing a subgroup S_d of index p^r and exponent at most p^d such that, for $d > 1$, S_d/U_d contains a subgroup of index p^r and exponent at most p^{d-1} and such that, for $d > 1$, $\mathrm{rank}(S_d/U_d) \ge 2r + j$.*

Proof: The proof is similar to that of Corollary 8.4, using Corollaries 7.7 and 7.8. □

In particular, we can take $j = 0$ and $S_d \cong Z_{p^d}^{2r}$ in Corollary 8.4 (ii) and Corollary 8.5 (i) to show that for each $d \ge 1$ 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 G_d of rank $2r$ relative to any subgroup Z_p^r, including $G_d = Z_{p^{d+1}}^r \times Z_{p^d}^r$ and $G_d = Z_{p^{d+r}} \times Z_{p^d}^{2r-1}$. ($P(r)$ represents the number of partitions of r.)

9 Open problems and nonabelian constructions

In this section, we list some open problems which are suggested by the techniques and results of this paper. We then discuss two possible approaches to generalising the definitions and constructions to deal with nonabelian groups.

It appears from our results that the objects we have called BSs and covering EBSs are fundamental to the construction of difference sets and semi-regular RDSs. We believe that future research could usefully consider the following questions (all groups are still implicitly abelian):

the set of BSs obtained with $c = d$, by applying Lemma 2.1 with $s = 2^r$ (whereas when $i > 0$ this is not the case).

Let $P(i)$ be the number of partitions of the positive integer i. Then we can take $j = r$ and $S_d \cong Z_{2^d}^{2r}$ in Corollary 8.4 (iv) to show that for each $d \geq 2$ there exists a $(2^{(2d+1)r}, 2^r, 2^{(2d+1)r}, 2^{2dr})$ semi-regular RDS in $P(2r)$ nonisomorphic groups G_d of rank $2r$ relative to any subgroup Z_2^r, including $G_d = Z_{2^{d+1}}^{2r}$ and $G_d = Z_{2^{d+2r}} \times Z_{2^d}^{2r-1}$. This shows that although the group rank must be at least $2r$ in order to use the underlying construction of Theorem 4.3, it need not grow any larger.

To illustrate in detail how Corollary 8.4 improves on previous results, take $r = 2$ and $d = 3$ and consider which abelian groups G contain a $(2^{12+j}, 4, 2^{12+j}, 2^{10+j})$ semi-regular RDS relative to a subgroup $U \cong Z_2^2$. We shall refer to the results of Table 1, using $(*)$ to indicate the condition that U is contained in a subgroup of G isomorphic to Z_4^2.

When $j = 0$, the RDS parameters are $(2^{12}, 4, 2^{12}, 2^{10})$ and G has order 2^{14}. Previously it was known that G could be any group of rank at least 8 using (B), any group of rank at least 7 such that $(*)$ is satisfied using (C), or the group $U \times Z_8^4$ of rank 6 using (E) with $\alpha = 2$, $d = 3$. We can now use part (i) of Corollary 8.4 to include five groups G of rank 4, namely $Z_{64} \times Z_8^2 \times Z_4$, $Z_{32} \times Z_{16} \times Z_8 \times Z_4$, $Z_{32} \times Z_8^3$, $Z_{16}^3 \times Z_4$ and $Z_{16}^2 \times Z_8^2$ for any $U \cong Z_2^2$, as well as many new groups of rank 5 and 6 such that $(*)$ is satisfied. Part (ii) of Corollary 8.4 is less powerful than part (i) in terms of large exponent, but it does not require the condition $(*)$ on G. Parts (i) and (ii) together show that G can be any group of exponent at most 16 and U any subgroup, except when $G = Z_2^2 \times Z_{16}^3$ and U intersects one or both of the first two direct factors of G in a nonidentity element.

When $j = 1$, the RDS parameters are $(2^{13}, 4, 2^{13}, 2^{11})$ and G has order 2^{15}. Assume that G and U mentioned in this paragraph satisfy $(*)$, which is necessary by Lemma 7.4. Previously it was known that G could be any group of rank at least 10 and exponent at most 4 using (F), or any group of rank at least 8 having the form $Z_4^2 \times Z_2 \times G'$ (where U is contained in the first two direct factors) using the RDS product construction on (B) with $\alpha = 5$ and (A) with $\alpha = 3$. We can now use part (iii) of Corollary 8.4 to include six groups of rank 5, namely $Z_{32} \times Z_8^3 \times Z_2$, $Z_{16}^2 \times Z_8^2 \times Z_2$, $Z_{16} \times Z_8^3 \times Z_4$ and Z_8^5 for any U, and $Z_{32} \times Z_8^2 \times Z_4^2$ and $Z_{16}^2 \times Z_8 \times Z_4^2$ for any U which is not contained in the last two direct factors, as well as many new groups of rank 6 and higher. Part (iii) also shows that G can be any group of exponent at most 8 and U any subgroup

When $j = 2$, the RDS parameters are $(2^{14}, 4, 2^{14}, 2^{12})$ and G has order 2^{16}. Previously it was known that G could be any group of rank at least 9 using (B), any group of rank at least 8 such that $(*)$ is satisfied using (C), or the group $Z_4^2 \times Z_8^4$ of rank 6 where U is contained in the first two direct factors using the RDS product construction on (A) with $\alpha = 2$ and (E) with $\alpha = 2$, $d = 3$. We can now use part (iv) of Corollary 8.4 to include five groups of rank 4 (five being the number of partitions of $2r = 4$), namely $Z_{128} \times Z_8^3$, $Z_{64} \times Z_{16} \times Z_8^2$, $Z_{32}^2 \times Z_8^2$, $Z_{32} \times Z_{16}^2 \times Z_8$ and Z_{16}^4 for any U, as well as many new groups of rank 5, 6 and 7 such that $(*)$ is satisfied. We can also use part (ii) of Corollary 8.4 to include examples not satisfying $(*)$ for which G has low rank, for example $G = Z_{64} \times Z_2 \times Z_8^2 \times Z_4 \times Z_2$ where U is contained in the first two direct factors of G.

When $j = 3$, the RDS parameters are $(2^{15}, 4, 2^{15}, 2^{13})$ and G has order 2^{17}. Assume that all G and U mentioned in this paragraph satisfy $(*)$, which is necessary by Lemma 7.4.

(Leung and Ma [28] and Chen, Ray-Chaudhuri and Xiang [5] have also given constructions for semi-regular RDSs in certain p-groups relative to an arbitrary subgroup of order p^r, and Schmidt [44] has exhibited a $(16, 4, 16, 4)$ RDS in $U \times Z_4 \times Z_2^2$ with $U \cong Z_4$.) To our knowledge no abelian groups other than those described have been previously shown to contain semi-regular RDSs.

We now show how these results can be improved for $U \cong Z_p^r$ by applying Theorem 2.2 to the Corollaries of Section 7, firstly taking $p = 2$.

Corollary 8.4 *There exists a* $(2^{2dr+j}, 2^r, 2^{2dr+j}, 2^{(2d-1)r+j})$ *semi-regular RDS in the following groups* G_d *of order* $2^{(2d+1)r+j}$ *relative to any subgroup* $U_d \cong Z_2^r$, *where* j *and* r *satisfy* $0 \leq j < 2r$*:*

(i) When j=0 and r=2. *For each* $d \geq 2$, *any group* G_d *containing a subgroup* S_d *of index* 8 *and exponent at most* 2^d *such that* U_d *is contained in a subgroup of* S_d *isomorphic to* Z_4^2 *and such that, for* $d > 2$, S_d/U_d *contains a subgroup of index* 4 *and exponent at most* 2^{d-1}.

(ii) When j is even. *For each* $d \geq 1$, *any group* G_d *containing a subgroup* S_d *of index* $2^{r+j/2}$ *and exponent at most* 2^d *such that, for* $d > 1$, S_d/U_d *contains a subgroup of index* 2^r *and exponent at most* 2^{d-1} *and such that, for* $j > 0$ *and* $d > 1$, $\mathrm{rank}(S_d/U_d) \geq 2r + j/2$.

(iii) When j<r. *For each* $d \geq 2$, *any group* G_d *containing a subgroup* S_d *of index* 2^r *and exponent at most* 2^d *such that* U_d *is contained in a subgroup of* S_d *isomorphic to* Z_4^r *and such that* S_d/U_d *contains a subgroup of index* 2^r *and exponent at most* 2^{d-1} *and such that, for* $j > 0$, $\mathrm{rank}(S_d/U_d) \geq 2r + j$.

(iv) When j=r. *For each* $d \geq 2$, *any group* G_d *containing a subgroup* S_d *of index* 2^{2r} *and exponent at most* 2^d *such that* U_d *is contained in a subgroup of* S_d *isomorphic to* Z_4^r *and such that* S_d/U_d *contains a subgroup of index* 2^r *and exponent at most* 2^{d-1}.

(v) When j>r. *For each* $d \geq 1$, *any group* G_d *containing a subgroup* S_d *of index* 2^r *and exponent at most* 2^{d+1} *such that* U_d *is contained in a subgroup of* S_d *isomorphic to* Z_4^r *and such that* S_d/U_d *contains a subgroup of index* 2^{j-r} *and exponent at most* 2^d.

Proof: We apply Theorem 2.2 to certain of the families of BSs constructed in Corollaries 7.7, 7.9 and 7.10, putting $p = 2$ and ignoring the initial BSs.

For (i), use the BSs from Corollary 7.10 with $c = d$. For (ii), use the BSs from Corollary 7.7 with $c = d$ and set $2i = j$. For (iii), use the BSs from Corollary 7.9 with $c = d$ and set $i = j + r$. For (iv), use the BSs from Corollary 7.9 with $c = d - 1$ and $d \geq 3$, set $i = j - r = 0$ and then replace d by $d+1$ throughout. For (v), use the BSs from Corollary 7.9 with $c = d$ and $d \geq 2$, set $i = j - r$ and then replace d by $d+1$ throughout. □

The case $j = r$ is dealt with separately from the case $j > r$ in Corollary 8.4 because, when $i = 0$, the set of BSs obtained from Corollary 7.9 with $c = d - 1$ strictly contains

then the following exponent bounds apply: $\exp(G) \leq p^{\alpha+1}$ for $w = 2\alpha$ [9]; $\exp(G) \leq p^{\alpha+1}$ for p odd and $w = 2\alpha+1$ [31]; and $\exp(G) \leq 2^{\alpha+2}$ for $p = 2$ and $w = 2\alpha+1$ [42]. The first exponent bound is attained for $\alpha \geq r$ and any p by $G = Z_{p^{\alpha+1}} \times Z_p^{r+\alpha-1}$ and any $U \cong Z_p^r$. To show this, apply Theorem 2.2 to the BSs of Corollary 4.2 followed by Lemma 4.5. The first bound is also attained for $\alpha \geq 1$ and $p = r = 2$ by $G = Z_{2^{\alpha+1}} \times Z_4 \times G_\alpha$, where $U \cong Z_2^2$ is contained in the first two direct factors of G and where G_α is any group of order $2^{\alpha-1}$ and exponent at most 4, except possibly $G_3 = Z_4$. To show this for $\alpha \geq 2$, apply Theorem 2.2 to the BSs of Theorem 5.1 (ii) and (iii). (These examples can also be obtained by taking the minimum value of c in certain of the Corollaries of Section 7.) As already discussed, we believe that the RDS group is not the natural place to determine an exponent bound.

On the existence side, the previous state of knowledge for $r > 1$ is summarised in Table 1. In stating these results we have applied the method of contraction of RDSs (the case $t = 1$ of Lemma 4.5) as appropriate. The construction of Leung and Ma [28] applies to many groups, of which we have included only those of rank less than $5r$. This is the only previous construction for which the rank of G does not necessarily grow with the order of the group. The RDSs in Table 1 can also be combined using the "product" construction, due to Davis [6] and Pott [43]. The product construction carries over to BSs and we now state it in this form without proof, but we shall only require the RDS part, namely the case $t = t' = 1$. The principal disadvantage of the product construction is that under repeated application the rank of G is forced to grow.

Source	w	Min rank(G)	Conditions
(A) Jungnickel [24]	α	α	$p = 2$ $(*)$
		$r + \alpha$	p odd
(B) Davis [8]	2α	$r + \alpha$	$\alpha \geq r$
(C) Davis and Sehgal [12]	2α	$\alpha + 1$	$p = 2$, $r = 2$, $\alpha \geq 2$ $(*)$
		$\alpha + 2$	$p = 2$, $r = 3$, $\alpha \geq 5$ $(*)$
(D) Pott [42]	$(2d+1)\alpha$	$(d+1)\alpha$	$p = 2$, $\alpha \geq r$, $d \geq 1$ $(*)$
		$r + (d+1)\alpha$	p odd, $\alpha \geq r$
(E) Leung and Ma [28]	$2d\alpha$	$r + 2\alpha$	$\alpha \geq r$, $d \geq 1$, $G = U \times Z_{p^d}^{2\alpha}$
(F) Chen, Ray-Chaudhuri and Xiang [5]	$2\alpha - 1$	$(3\alpha - 1)/2$	$p = 2$, $\alpha \geq r$, α odd, $\exp(G) = 4$ $(*)$

Table 1: A (p^w, p^r, p^w, p^{w-r}) semi-regular RDS exists in any abelian group G relative to any subgroup U isomorphic to Z_p^r provided G has the specified minimum rank and $w \geq r \geq 1$ and the stated conditions are satisfied, where p is prime. $(*)$ indicates the additional condition that G contains a subgroup isomorphic to Z_4^r containing U.

Theorem 8.3 *Let G be a group of order uaa' containing a subgroup U of order u, and let H and H' be subgroups of G of order ua and ua' respectively, where $H \cap H' = U$. Suppose there exists a $(a, \sqrt{at}, t)$ BS on H relative to U and there exists a $(a', \sqrt{a't'}, t')$ BS on H' relative to U. Then there exists a $(aa', \sqrt{aa'tt'}, tt')$ BS on G relative to U.*

For (ii), put $r = 1$ and $i = 0$ and consider the initial BS of Corollary 7.8 on Z_p^{2r+i} together with the case $d = 1$ of Corollary 7.8. This gives a $(p^2, p^{1/2}, 1)$ BS on Z_p^2 relative to Z_p and a $(p^2, p^{3/2}, p)$ BS on Z_p^3 relative to Z_p. This gives the result for $d = 0$ and $d = 1$. For $d > 1$, we have excluded the cases $G_d = Z_{p^{d+1}}^2$ and $G_d = U_d \times Z_{p^{d+1}} \times Z_{p^d}$. Therefore G_d contains a subgroup S (containing U_d) of index p and exponent at most p^d for which $S \ncong U_d \times Z_{p^d}^2$. The case $r = 1$, $i = 0$, $c = d$ of Corollary 7.8 shows that there exists a $(p^{2d}, p^{(2d+1)/2}, p)$ BS on any group S_d of order p^{2d+1} and exponent at most p^d relative to any subgroup U_d of order p except possibly when $d > 1$ and $S_d/U_d \cong Z_{p^d}^2$, which is equivalent to $S_d \cong U_d \times Z_{p^d}^2$. □

Corollary 8.2 (i) and many of the cases of Corollary 8.2 (ii) were proved by Ma and Schmidt [33]. Davis [9] showed that the exponent bound of p^{d+1} in Corollary 8.2 (i) is necessary, and Ma and Pott [31] established the corresponding bound for Corollary 8.2 (ii). It follows from this and from our earlier discussion of the case $p^r = 2$ that for p prime, the only abelian groups G of order p^{w+1} in which the existence of a (p^w, p, p^w, p^{w-1}) RDS relative to a subgroup U of order p remains unknown have p odd, $w = 2d + 1$, and either $G = Z_{p^{d+1}}^2$ or $G = U \times Z_{p^{d+1}} \times Z_{p^d}$. We have chosen to express the existence condition in Corollary 8.2 (ii) for $d > 1$ in terms of G_d/U_d in order to emphasise the importance of the position of U_d within G_d.

For $r = 1$, all the RDSs arising from the BS families of Section 7 via Theorem 2.2 can be obtained by taking $c = d$. However for $r > 1$, each value of c gives rise to different RDSs. For example, take $d = 4$, $r = 2$ and $i = 0$ in Corollary 7.9. Using Theorem 2.2 we obtain a $(2^{18}, 4, 2^{18}, 2^{16})$ semi-regular RDS in certain groups G_c containing a subgroup S_c of order 2^{8+2c} and exponent at most 2^c relative to a subgroup $U_c \cong Z_2^2$. In the case $c = 2$, the maximum exponent of G_c is 2^{10} and the minimum rank is 6, both of which are attained by $G_2 = Z_{2^{10}} \times Z_4^5$ and any U_2. In the case $c = 3$, the maximum exponent of G_c is reduced to 2^9 but the minimum rank is now 5, attained by $G_3 = Z_{2^9} \times Z_8^3 \times Z_4$ and any U_3. In the case $c = 4$, the maximum exponent of G_c is further reduced to 2^8 but the minimum rank becomes 4, attained by $G_4 = Z_{2^8} \times Z_{16}^3$ and any U_4.

This shows that for the group G containing the RDS, a small rank is associated with a small exponent. But for the subgroup S on which the underlying BS is defined, we have the usual correspondence between small rank and large exponent. (In the above example, minimum rank 6 and maximum exponent 4, minimum rank 5 and maximum exponent 8, and minimum rank 4 and maximum exponent 16.) For this reason we believe that the natural place to consider exponent bounds is the BS group S rather than the RDS group G. In our opinion the most interesting RDS examples are those for which the underlying BS group has small rank and large exponent. We shall therefore mostly concentrate on the RDSs arising from Corollaries 7.7–7.10 for the value $c = d$. Further RDSs can be obtained for $c < d$ by direct reference to the Corollaries. To highlight the central results we shall also omit RDSs arising from the initial BSs of the Corollaries, which would require a separate statement of conditions.

Henceforth we take $r > 1$. We now review the previous state of knowledge for a (p^w, p^r, p^w, p^{w-r}) semi-regular RDS in an abelian group G relative to $U \cong Z_p^r$, where p is prime and $w \geq r > 1$. The best known nonexistence results are that if such RDSs exist

(i) *A* $(2^{2d}m^2, 2, 2^{2d}m^2, 2^{2d-1}m^2)$ *semi-regular RDS in* $G_d \times M$ *relative to any subgroup* U_d *of order* 2*, where* G_d *is any group of order* 2^{2d+1} *and exponent at most* 2^{d+1}*.*

(ii) *A* $(2^{2d+1}m^2, 2, 2^{2d+1}m^2, 2^{2d}m^2)$ *semi-regular RDS in* $G_d \times M$ *relative to any subgroup* U_d *of order* 2 *contained in a subgroup of* G_d *isomorphic to* Z_4*, where* G_d *is any group of order* 2^{2d+2} *and exponent at most* 2^{d+2}*.*

Proof: For (i), G_d contains a subgroup of index 2 and exponent at most 2^d containing U_d. Apply Theorem 2.2 to the case $c = d$ of Corollary 7.3 (i).

For (ii), G_d contains a subgroup S of index 2 and exponent at most 2^{d+1} such that U_d is contained in a subgroup of S isomorphic to Z_4. Put $c = d$ in Corollary 7.3 (ii), replace d by $d + 1$ throughout and then apply Theorem 2.2. □

Corollary 8.1 was proved for trivial M by Ma and Schmidt [33] and for all appropriate groups M (as described in Section 6) by Jedwab [23] via lengthy computations on binary arrays. (Jungnickel [24] earlier noted that a Hadamard difference set with parameter $N = 2^{d-1}m$ in a group W_d of order $2^{2d}m^2$ can be used to construct a RDS with the parameters of Corollary 8.1 (i) in the subset of groups having the "splitting" form $U_d \times W_d$.) Davis [9] used techniques introduced by Turyn [49] to show that the exponent bound of 2^{d+1} on G_d in Corollary 8.1 (i) is necessary as well as sufficient for trivial M, and Pott [42] proved the corresponding result for the exponent bound 2^{d+2} in Corollary 8.1 (ii). Exponent bounds on G_d when M is nontrivial can be obtained for both parts of the Corollary by similar methods, subject to number theoretic conditions. As already noted, the condition in Corollary 8.1 (ii), that U_d is contained in a subgroup of G_d isomorphic to Z_4, is necessary by Lemma 7.4. Jungnickel [24] has shown that the existence of a $(2m, 2, 2m, m)$ semi-regular RDS (not necessarily in an abelian group) implies the existence of a Hadamard matrix of order $2m$, which in turn implies that $m = 1$ or m is even (see Seberry and Yamada [45] for a recent survey of Hadamard matrices). Therefore we cannot substitute the value $d = 0$ in Corollary 8.1 (ii) when M is nontrivial (although we can when M is trivial).

In the remainder of this section, the groups G containing RDSs will be p-groups. The most extensive previous results for RDSs are for $r = 1$, so we next take the order of U to be an odd prime p.

Corollary 8.2 *Let* p *be an odd prime.*

(i) *For each* $d \geq 1$*, there exists a* $(p^{2d}, p, p^{2d}, p^{2d-1})$ *semi-regular RDS in any group of order* p^{2d+1} *and exponent at most* p^{d+1} *relative to any subgroup* U_d *of order* p*.*

(ii) *For each* $d \geq 0$*, there exists a* $(p^{2d+1}, p, p^{2d+1}, p^{2d})$ *semi-regular RDS in any group* G_d *of order* p^{2d+2} *and exponent at most* p^{d+1} *relative to any subgroup* U_d *of order* p*, except possibly when* $G_1 \cong Z_{p^2}^2$ *or when* $G_d/U_d \cong Z_{p^{d+1}} \times Z_{p^d}$ *for* $d > 1$*.*

Proof: The proof is by application of Theorem 2.2 to the following BSs.

For (i), G_d contains a subgroup of index p and exponent at most p^d containing U_d. The case $r = 1$, $i = 0$, $c = d$ of Corollary 7.7 shows that there exists a (p^{2d-1}, p^d, p) BS on any group of order p^{2d} and exponent at most p^d relative to any subgroup of order p.

can be shown that the resulting BSs have parameters in the same families as those of Corollary 7.9 and that (apart from initial examples) the BSs are defined on substantially the same set of groups. Nonetheless this method allows a relaxation of condition (iii) of Corollary 7.9, involving $\mathrm{rank}(G_{d,c}/U_{d,c})$ for $i > r$, for certain values of i when $r \geq 5$. For example, the minimum rank of $G_{d,c}$ when $r = 5$ and $i = 8$ can be reduced from 13 to 12 in this way.

We conclude this section by modifying Theorem 7.5 to deal with groups whose order is not a prime power.

Theorem 7.11 *Let W be a group of order $w \geq 1$, let p be a prime not dividing w and let $r \geq 1$. Suppose there exists a $(p^r aw, p^r\sqrt{awt}, p^r t)$ BS on any group $G_{\bar{c},\bar{c}} \times W$, whose Sylow p-subgroup $G_{\bar{c},\bar{c}}$ has order $p^{2r}a$ and exponent at most $p^{\bar{c}}$, relative to any subgroup $U_{\bar{c},\bar{c}} \cong Z_p^r$, where $a > p^{\bar{c}(2r-1)-2r-1}$ and $\bar{c} \geq 1$. Then for each d and c satisfying $\bar{c} \leq c \leq d$, there exists a $(p^{(d+c-2\bar{c}+1)r}aw, p^{(d-\bar{c}+1)r}\sqrt{awt}, p^{(d-c+1)r}t)$ BS on any group $G_{d,c} \times W$, whose Sylow p-subgroup $G_{d,c}$ has order $p^{(d+c-2\bar{c}+2)r}a$ and exponent at most p^c, relative to any subgroup $U_{d,c} \cong Z_p^r$, provided that, for each j in the range $\bar{c} \leq j \leq c-1$, $G_{d,c}/U_{d,c}$ contains a subgroup of index $p^{(d+c-2j-1)r}$ and exponent at most p^j.*

Furthermore the theorem remains true for $\bar{c} \geq 2$ if $U_{\bar{c},\bar{c}}$ is additionally constrained to be contained within a subgroup of $G_{\bar{c},\bar{c}}$ isomorphic to $Z_{p^2}^r$, provided that each $U_{d,c}$ is likewise contained within a subgroup of $G_{d,c}$ isomorphic to $Z_{p^2}^r$.

Theorem 7.11 can be proved from Theorem 7.1 in a similar manner to Theorem 7.5: the important calculations involve only the Sylow p-subgroup $G_{d,c}$ and not the group W. We did not give this more general form earlier in order to avoid the introduction of several new parameters at the same time. In particular cases, the conditions on subgroups of $G_{d,c}/U_{d,c}$ in Theorem 7.11 can be replaced by a smaller set of conditions, as in Corollaries 7.7–7.10. Theorem 7.11 could have been used in this way to prove the results of Corollary 7.3. Moreover Theorem 7.11 has potential use in determining the existence of new families of BSs, subject to finding appropriate initial BSs on groups whose order is not a prime power.

8 Application to semi-regular relative difference sets

In this section we use Theorem 2.2 to deduce the existence of families of semi-regular RDSs in groups G relative to subgroups $U \cong Z_p^r$ from the BSs constructed in Section 7. In particular we show that the order of G can grow without bound for fixed rank $2r$. We are not aware of any abelian groups G known to contain semi-regular RDSs relative to an elementary abelian subgroup which are not covered by these results.

We begin with the special case of a subgroup U of order $p^r = 2$. This is a rich source of RDSs in groups G whose order has distinct prime factors, deriving from the $(m(\frac{m-1}{2}), m, 4, +)$ covering EBSs on groups M constructed in Corollary 6.7 (i).

Corollary 8.1 *Let M be either the trivial group or the group $\prod_i Z_{3^{\alpha_i}}^2 \times \prod_j Z_{p_j}^4$, where $\alpha_i \geq 1$ and where p_j is a prime congruent to 3 modulo 4 or $p_j = 5$, and let $|M| = m^2$. For each $d \geq 1$ the following exist:*

$w_j - (d+c-2j-2)r - i \leq \frac{jr}{c}(c - \frac{(d-2)r+i}{r}) \leq 0$. When $c > \frac{(d-2)r+i}{r}$ (which implies that $c = d-1$ or $c = d$), we assume the condition on $j = c-1$ holds and consider j in the range $1 \leq j \leq c-2$. Following the same argument as previously, $w_j \leq (c-j)\alpha_c + \frac{c-1-j}{c-1}\sum_{u=j+1}^{c-1} u\alpha_u \leq (c-j)\alpha_c + \frac{c-1-j}{c-1}((d+c-2)r+i-c\alpha_c)$. In the case $c = d-1$ we obtain $w_j - (2d-2j-3)r - i \leq \frac{j}{d-2}(\alpha_{d-1} - (r+i))$ and the assumed condition on $j = d-2$ implies $\alpha_{d-1} \leq r+i$, whereas in the case $c = d$ we obtain $w_j - (2d-2j-2)r - i \leq \frac{j}{d-1}(\alpha_d - i)$ and the assumed condition on $j = d-1$ implies $\alpha_d \leq i$. □

The condition in Corollary 7.9 that $U_{d,c} \cong Z_2^r$ is contained in a subgroup of $G_{d,c}$ isomorphic to Z_4^r is necessary when $r+i$ is odd, by Lemma 7.4.

Corollary 7.10 *There exists a $(8,4,2)$ BS on $Z_4^2 \times Z_2$ relative to the subgroup Z_2^2 of Z_4^2. For each d and c satisfying $2 \leq c \leq d$, there exists a $(2^{2d+2c-3}, 2^{2d}, 2^{2d-2c+3})$ BS on any group $G_{d,c}$ of order $2^{2d+2c-1}$ and exponent at most 2^c relative to any subgroup $U_{d,c} \cong Z_2^2$, where $U_{d,c}$ is contained in a subgroup of $G_{d,c}$ isomorphic to Z_4^2 and where, for $d > 2$ and $c = d$, $G_{d,c}/U_{d,c}$ contains a subgroup of index 4 and exponent at most 2^{d-1}.*

Proof: The $(8,4,2)$ BS is given in Theorem 7.6 (iv). By Theorem 4.3 and Lemma 4.4 there exists a $(32,16,8)$ BS on any group G of order 128 and exponent 4 relative to $U \cong Z_2^2$, where U is contained within a subgroup of G isomorphic to Z_4^2. This provides the initial BS on $G_{\bar{c},\bar{c}}$ relative to $U_{\bar{c},\bar{c}}$ in Theorem 7.5, taking $p = r = 2$, $a = 8$ and $t = \bar{c} = 2$. By making use of the additional constraint that $U_{\bar{c},\bar{c}}$ is contained within a subgroup isomorphic to $Z_{p^2}^r$ we then obtain the required BS on $G_{d,c}$ relative to $U_{d,c}$ provided that, for each c in the range $2 \leq c \leq d$, the following condition on j is satisfied for each j in the range $2 \leq j \leq c-1$: $G_{d,c}/U_{d,c}$ contains a subgroup of index $2^{2(d+c-2j-1)}$ and exponent at most 2^j. The remainder of the proof is similar to that of the first and third cases in the proof of Corollary 7.7. As in the proof of Corollary 7.9, the constraint that $U_{d,c}$ is contained within a subgroup of $G_{d,c}$ isomorphic to Z_4^2 does not affect the analysis of $G_{d,c}/U_{d,c}$.

When $c \leq d-1$ we do not assume any condition on j and consider j in the range $2 \leq j \leq c-1$. By similar reasoning to that used previously we show that $w_j - 2(d+c-2j-1) \leq \frac{2j}{c}(c+1-d) + (j-c)/c \leq 0$. When $c = d$ we assume the condition on $j = d-1$ to hold, so that $\alpha_d \leq 2$, and consider j in the range $2 \leq j \leq d-2$. We obtain $w_j - 2(2d-2j-1) \leq \frac{1}{d-1}(j(\alpha_d - 2) + j + 1 - d) \leq 0$. □

Further examples of BSs can be constructed from those in Corollaries 7.7–7.10 using Lemma 2.1. We believe the set of BSs so produced to be complete in the sense that no other examples could be obtained from the four sources of initial BSs of Theorem 7.6 using the underlying construction of Theorem 4.3. In Section 8 we discuss further some implications of Corollaries 7.7–7.10.

A fifth source of initial BSs is given by Chen, Ray-Chaudhuri and Xiang's construction [5] of a $(2^{2r-1}, 2^r, 2^{2r-1}, 2^{r-1})$ semi-regular RDS in any group G of order 2^{3r-1} and exponent 4 relative to $U \cong Z_2^r$, where U is contained within a subgroup of G isomorphic to Z_4^r and $r \geq 1$ is odd. We can regard this as a $(2^{2r-1}, 2^{(2r-1)/2}, 1)$ BS on the stated group and subgroup and use the above procedure to obtain an additional corollary. It

proof of Corollary 7.7 and can likewise be replaced by a smaller set of conditions. The only difference is that here $G_{d,c}/U_{d,c}$ has order $p^{(d+c-1)r+(r+i)}$ rather than $p^{(d+c-1)r+i}$. Since the replacement of conditions on j in the proof of Corollary 7.7 does not rely on the inequality $i < r$, this part of the proof carries over completely with $r+i$ used instead of each occurrence of i. $\square$

Corollary 7.9 *Let i and r satisfy $0 \leq i < 2r$. There exists a $(2^{r+i}, 2^{(r+i)/2}, 1)$ BS on $Z_4^r \times Z_2^i$ relative to the subgroup Z_2^r of Z_4^r. For each d and c satisfying $2 \leq c \leq d$, there exists a $(2^{(d+c-2)r+i}, 2^{((2d-1)r+i)/2}, 2^{(d-c+1)r})$ BS on any group $G_{d,c}$ of order $2^{(d+c-1)r+i}$ and exponent at most 2^c relative to any subgroup $U_{d,c} \cong Z_2^r$, where $U_{d,c}$ is contained in a subgroup of $G_{d,c}$ isomorphic to Z_4^r and where all of the following hold:*

(i) *For $c = d$, $G_{d,c}/U_{d,c}$ contains a subgroup of index $2^{\min\{r,i\}}$ and exponent at most 2^{d-1}.*

(ii) *For $i < r$ and $d > 2$ and $c = d-1$, $G_{d,c}/U_{d,c}$ contains a subgroup of index 2^{r+i} and exponent at most 2^{d-2}.*

(iii) *For $i > r$ and c in the range $\max\{1, \frac{(d-2)r+i}{i}\} < c \leq d$, $\mathrm{rank}(G_{d,c}/U_{d,c}) \geq r+i$.*

Proof: By Theorem 7.6 (iii) and Lemma 4.5 there exists a $(2^{r+i}, 2^{(r+i)/2}, 1)$ BS on $Z_4^r \times Z_2^i$ relative to the subgroup Z_2^r of Z_4^r. Then by Theorem 4.3 and Lemma 4.4 there exists a $(2^{2r+i}, 2^{(3r+i)/2}, 2^r)$ BS on $Z_4^{r+u} \times Z_2^{r+i-2u}$ relative to the subgroup Z_2^r of Z_4^r for each u in the range $0 \leq u \leq \min\{r, i\}$. Equivalently, there exists a $(2^{2r+i}, 2^{(3r+i)/2}, 2^r)$ BS on any group $G_{2,2}$ of order 2^{3r+i} and exponent at most 4 relative to any subgroup $U_{2,2} \cong Z_2^r$, where $U_{2,2}$ is contained in a subgroup of $G_{2,2}$ isomorphic to Z_4^r and where $G_{2,2}/U_{2,2}$ contains a subgroup of index $2^{\min\{r,i\}}$ and exponent 2. This is the case $d = c = 2$ of the Corollary. We claim that this implies the existence of the required BS on $G_{d,c}$ relative to $U_{d,c}$ provided that, for each c in the range $2 \leq c \leq d$, the following condition on j is satisfied for each j in the range $1 \leq j \leq c-1$: $G_{d,c}/U_{d,c}$ contains a subgroup of index $2^{(d+c-2j-2)r+\min\{r,i\}}$ and exponent at most 2^j. This claim does not follow directly from Theorem 7.5 with $\bar{c} = 2$ because of the presence of a subgroup condition on $G_{2,2}/U_{2,2}$. However the proof of Theorem 7.5 can be modified to establish the claim. The constraint that $U_{d,c}$ is contained within a subgroup of $G_{d,c}$ isomorphic to Z_4^r (which derives from the corresponding constraint on $U_{\bar{c},\bar{c}}$) is equivalent to $\mathrm{rank}(G_{d,c}/U_{d,c}) = \mathrm{rank}(G_{d,c})$ and so can be regarded as a constraint on $G_{d,c}$ which does not affect the analysis of $G_{d,c}/U_{d,c}$ which follows.

For $i \geq r$ the conditions on j are identical to those in the proof of Corollary 7.7 with $p = 2$, the only difference being that here $G_{d,c}/U_{d,c}$ has order $2^{(d+c-1)r+(i-r)}$ for i in the range $r \leq i < 2r$ rather than $2^{(d+c-1)r+i}$ for i in the range $0 \leq i < r$. Therefore the replacement of conditions on j in the proof of Corollary 7.7 carries over completely with $i-r$ used instead of each occurrence of i.

For $i < r$, the remainder of the proof is similar to that of the first and third cases of Corollary 7.7, with the equation $\sum_{u=1}^{c} u\alpha_u = (d+c-2)r+i$ replacing (10). When $c \leq \frac{(d-2)r+i}{r}$, we do not assume any condition on j and consider j in the range $1 \leq j \leq c-1$. The inequality $w_j \leq \frac{c-j}{c} \sum_{u=j+1}^{c} u\alpha_u$ previously found now implies that

implies that $w_j \leq \frac{c-j}{c}((d+c-1)r+i)$. Rearrangement gives $w_j - (d+c-2j-1)r \leq \frac{j(r+i)}{c}(c - \frac{(d-1)r+i}{r+i}) - i(j-1)$. Since $c \leq \frac{(d-1)r+i}{r+i}$, we obtain $w_j - (d+c-2j-1)r \leq 0$. Therefore by the definition of w_j, $G_{d,c}/U_{d,c}$ always contains a subgroup of index $p^{(d+c-2j-1)r}$ and exponent at most p^j for each j in the range $1 \leq j \leq c-1$.

In the second case, when $c \leq d-1$, we assume the condition on $j=1$ holds and consider j in the range $2 \leq j \leq c-1$. Take $\beta = 1$ and $C = c$ in (12) and use (11) to deduce that $w_j \leq (\frac{c-j}{c-1})w_1$. Now the condition on $j=1$ can be written as $w_1 \leq (d+c-3)r$ and so $w_j - (d+c-2j-1)r \leq \frac{j-1}{c-1}(c+1-d)r$. Since $c \leq d-1$, we obtain $w_j - (d+c-2j-1)r \leq 0$.

In the third case, when $c = d$ and $i = 0$, we assume the condition on $j = d-1$ holds and consider j in the range $1 \leq j \leq d-2$. We can rewrite (11) as $w_j = (d-j)\alpha_d + \sum_{u=j+1}^{d-1}(u-j)\alpha_u$ and then put $\beta = 0$ and $C = d-1$ in (12) to show that $w_j \leq (d-j)\alpha_d + \frac{d-1-j}{d-1}\sum_{u=j+1}^{d-1} u\alpha_u$. (10) then implies that $w_j \leq (d-j)\alpha_d + \frac{d-1-j}{d-1}((2d-1)r - d\alpha_d)$. Hence $w_j - (2d-2j-1)r \leq \frac{j}{d-1}(\alpha_d - r)$. Now the condition on $j = d-1$ gives $w_{d-1} \leq r$, which from (11) is equivalent to $\alpha_d \leq r$. Therefore $w_j - (2d-2j-1)r \leq 0$.

In the fourth case, when $c = d$ and $i > 0$, we assume the condition on $j = 1$ and $j = d-1$ to hold and consider j in the range $2 \leq j \leq d-2$. Rewrite (11) as $w_j = (d-j)\alpha_d + \sum_{u=j+1}^{d-1}(u-j)\alpha_u$. Take $\beta = 1$ and $C = d-1$ in (12) and use (11) to deduce that $w_j \leq (d-j)\alpha_d + \frac{d-1-j}{d-2}(w_1 - (d-1)\alpha_d)$. Now the condition on $j=1$ gives $w_1 \leq (2d-3)r$ and so $w_j - (2d-2j-1)r \leq \frac{j-1}{d-2}(\alpha_d - r)$. The condition on $j = d-1$ then gives $w_{d-1} = \alpha_d \leq r$, and so $w_j - (2d-2j-1)r \leq 0$.

This completes the proof. □

The condition on $G_{d,d}/U_{d,d}$ in Corollary 7.7 is a consequence of the increase in group exponent from p^{d-1} to p^d. The condition on $\mathrm{rank}(G_{d,c}/U_{d,c})$ derives from the initial BS, which is defined on Z_p^{2r+i}. We note that the range of values of d, i and c in Corollary 7.7 for which $G_{d,c}/U_{d,c}$ must be constrained could be slightly improved because it is sufficient to ensure that $w_j - (d+c-2j-1)r < 1$ in the proof rather than $w_j - (d+c-2j-1)r \leq 0$. We have chosen the presented form for clarity; it is straightforward to check in individual cases whether the conditions are guaranteed to hold.

Corollary 7.8 *Let p be an odd prime and let i and r satisfy $0 \leq i < 2r$. There exists a $(p^{r+i}, p^{(r+i)/2}, 1)$ BS on Z_p^{2r+i} relative to Z_p^r. For each d and c satisfying $1 \leq c \leq d$, there exists a $(p^{(d+c)r+i}, p^{((2d+1)r+i)/2}, p^{(d-c+1)r})$ BS on any group $G_{d,c}$ of order $p^{(d+c+1)r+i}$ and exponent at most p^c relative to any subgroup $U_{d,c} \cong Z_p^r$, where, for $d > 1$ and $c = d$, $G_{d,c}/U_{d,c}$ contains a subgroup of index p^r and exponent at most p^{d-1} and where, for c in the range $\max\{1, \frac{dr+i}{2r+i}\} < c \leq d$, $\mathrm{rank}(G_{d,c}/U_{d,c}) \geq 3r+i$.*

Proof: By Theorem 7.6 (ii) and Lemma 4.5 there exists $(p^{r+i}, p^{(r+i)/2}, 1)$ BS on Z_p^{2r+i} relative to Z_p^r, as required. Then by Theorem 4.3 there exists a $(p^{2r+i}, p^{(3r+i)/2}, p^r)$ BS on Z_p^{3r+i} relative to Z_p^r. This provides the initial BS on $G_{\bar{c},\bar{c}}$ relative to $U_{\bar{c},\bar{c}}$ in Theorem 7.5, taking $a = p^{r+i}$ and $t = \bar{c} = 1$. We then obtain the required BS on $G_{d,c}$ relative to $U_{d,c}$ provided that, for each c in the range $1 \leq c \leq d$, the following condition on j is satisfied for each j in the range $1 \leq j \leq c-1$: $G_{d,c}/U_{d,c}$ contains a subgroup of index $p^{(d+c-2j-1)r}$ and exponent at most p^j. These conditions on j are identical to those in the

that we can reduce this factor to p^2 by producing BSs which give RDSs with parameters $(p^{2dr+2i}, p^r, p^{2dr+2i}, p^{(2d-1)r+2i})$ for each i in the range $0 \le i < r$. We do so by contracting the initial BSs using Lemma 4.5 before applying Theorem 7.5. (This is preferable to first applying Theorem 7.5 and then contracting, because it allows us to keep the group rank small.) In the second and third corollaries we will achieve a reduction in the corresponding factor from p^r to p.

Corollary 7.7 *Let p be prime and let i and r satisfy $0 \le i < r$. For each d and c satisfying $1 \le c \le d$, there exists a $(p^{(d+c-1)r+i}, p^{dr+i}, p^{(d-c+1)r+i})$ BS on any group $G_{d,c}$ of order $p^{(d+c)r+i}$ and exponent at most p^c relative to any subgroup $U_{d,c} \cong Z_p^r$, where, for $d > 1$ and $c = d$, $G_{d,c}/U_{d,c}$ contains a subgroup of index p^r and exponent at most p^{d-1} and where, for $i > 0$ and c in the range $\max\{1, \frac{(d-1)r+i}{r+i}\} < c \le d$, $\mathrm{rank}(G_{d,c}/U_{d,c}) \ge 2r + i$.*

Proof: We begin with a $(p^{r+i}, p^{r+i}, p^{r+i})$ BS on $Z_p^{2(r+i)}$ relative to Z_p^{r+i} from Theorem 7.6 (i), and use Lemma 4.5 with $W = Z_p^i$ to obtain a $(p^{r+i}, p^{r+i}, p^{r+i})$ BS on Z_p^{2r+i} relative to Z_p^r. This provides the initial BS on $G_{\bar{c},\bar{c}}$ relative to $U_{\bar{c},\bar{c}}$ in Theorem 7.5, taking $a = t = p^i$ and $\bar{c} = 1$. We then obtain the required BS on $G_{d,c}$ relative to $U_{d,c}$ provided that, for each c in the range $1 \le c \le d$, the following condition on j is satisfied for each j in the range $1 \le j \le c-1$: $G_{d,c}/U_{d,c}$ contains a subgroup of index $p^{(d+c-2j-1)r}$ and exponent at most p^j. We now show that this set of conditions can be replaced by the smaller set stated in the theorem by distinguishing four cases: firstly $c \le \frac{(d-1)r+i}{r+i}$, when no condition on j will be needed; secondly $c \le d-1$, when the condition on $j = 1$ will suffice; thirdly $c = d$ and $i = 0$, when the condition on $j = d-1$ will suffice; and fourthly $c = d$ and $i > 0$, when the condition on $j = 1$ and $j = d-1$ will together suffice. (In the theorem, the condition on $j = 1$ is written in the equivalent form: $\mathrm{rank}(G_{d,c}/U_{d,c}) \ge 2r + i$.) Since the range of j is $1 \le j \le c-1$, we shall assume $c > 1$ throughout.

The group $G_{d,c}/U_{d,c}$ has order $p^{(d+c-1)r+i}$ and exponent at most p^c, so we can write it as $\prod_{u=1}^{c} Z_{p^u}^{\alpha_u}$, where $\alpha_u \ge 0$ and

$$\sum_{u=1}^{c} u\alpha_u = (d+c-1)r + i. \tag{10}$$

Clearly $G_{d,c}/U_{d,c}$ contains a subgroup of index p^{w_j} and exponent at most p^j, where

$$w_j = \sum_{u=j+1}^{c} (u-j)\alpha_u. \tag{11}$$

We shall repeatedly use the fact that

$$\sum_{u=j+1}^{C} (u-j)\alpha_u \le \left(\frac{C-j}{C-\beta}\right) \sum_{u=j+1}^{C} (u-\beta)\alpha_u \tag{12}$$

for any integer $\beta \le j$.

In the first case, when $c \le \frac{(d-1)r+i}{r+i}$, we consider j in the range $1 \le j \le c-1$. Put $\beta = 0$ and $C = c$ in (12) and substitute from (11) to show that $w_j \le \frac{c-j}{c} \sum_{u=j+1}^{c} u\alpha_u$. (10) then

Finally, for $\bar{c} \geq 2$, let $U_{d,c}$ be additionally constrained to be contained within a subgroup of $G_{d,c}$ isomorphic to $Z_{p^2}^r$ for each $d \geq \bar{c}$ and for each c in the range $\bar{c} \leq c \leq d$. The above induction step for $d > \bar{c}$ can be modified as follows. The required BS on $G_{d,c}/H_i$ relative to $Q_{d,c}/H_i$ exists provided $Q_{d,c}/H_i$ is contained in a subgroup of $G_{d,c}/H_i$ isomorphic to $Z_{p^2}^r$ when $c \leq d-1$, and provided $Q_{d,d}/H_i$ is contained in a subgroup of S/H_i isomorphic to $Z_{p^2}^r$. Apply Lemma 4.4 with $G = G_{d,c}$, $H_0 = U_{d,c}$ and $Q = Q_{d,c}$ to show that $Q_{d,c}/H_i$ is contained in a subgroup of $G_{d,c}/H_i$ isomorphic to $Z_{p^2}^r$ for $c \leq d$. This establishes the result when $c \leq d-1$. It remains to show that if $Q' = Q_{d,d}/H_i$ is contained in a subgroup of $G' = G_{d,d}/H_i$ isomorphic to $Z_{p^2}^r$ (as just demonstrated) then we can choose $S' = S/H_i$ consistently with the previous procedure so that Q' is also contained in a subgroup of S' isomorphic to $Z_{p^2}^r$. In other words, given that the r direct factors of G'/Q' corresponding to the position of Q' in G' each attains an exponent of at least p, we must choose the subgroup S'/Q' consistently so that none of these direct factors is removed. The reduction in exponent to p^{d-2} can proceed as before since $d-2 \geq \bar{c}-1 \geq 1$, and the choice of S'/Q' with minimal exponent does not require the removal of any of the r direct factors unless $|G'/Q'| \leq p^{2r-1}$. It is straightforward to show that this inequality is false and so the induction proof carries over. □

Theorem 7.5 gives conditions on subgroups of $G_{d,c}/U_{d,c}$ for each c in the range $\bar{c} \leq c \leq d$ and for each j in the range $\bar{c} \leq j \leq c-1$. We shall show in the following four corollaries that in particular cases some of these conditions are implied by others while some are guaranteed to hold because of the order and exponent restrictions on $G_{d,c}$. Each of the corollaries is based on one of the following four sources, to which we apply Theorem 4.3 if necessary to obtain initial BSs comprising $p^r t$ building blocks on any p-group $G_{\bar{c},\bar{c}}$ of fixed order and bounded exponent relative to any subgroup $U_{\bar{c},\bar{c}} \cong Z_p^r$.

Theorem 7.6 *For each $r \geq 1$, the following exist:*

(i) *A (p^r, p^r, p^r) BS on Z_p^{2r} relative to Z_p^r, where p is prime and $r \geq 1$.*

(ii) *A $(p^r, p^{r/2}, 1)$ BS on Z_p^{2r} relative to Z_p^r, where p is an odd prime and $r \geq 1$.*

(iii) *A $(2^r, 2^{r/2}, 1)$ BS on Z_4^r relative to Z_2^r, where $r \geq 1$.*

(iv) *A $(8, 4, 2)$ BS on $Z_4^2 \times Z_2$ relative to the subgroup Z_2^2 of Z_4^2.*

Theorem 7.6 (i) is just a restatement of Corollary 4.2. Theorem 7.6 (ii) and (iii) are equivalent to Jungnickel's result [24] that semi-regular RDSs, with parameters $(p^r, p^r, p^r, 1)$ and $(2^r, 2^r, 2^r, 1)$ respectively, exist for the stated groups and subgroups. (Nonexistence results for RDSs show that no other abelian group and subgroup can be substituted in Theorem 7.6 (ii) for $r = 1$ [22] or $r = 2$ [31], or in Theorem 7.6 (iii) for any r [20].) Theorem 7.6 (iv) is due to Arasu and Sehgal [3], as described in Section 2.

Suppose we apply Theorem 7.5 directly to the BSs of Theorem 7.6 (i) to obtain BSs with parameters $(p^{(d+c-1)r}, p^{dr}, p^{(d-c+1)r})$. By Theorem 2.2 this gives semi-regular RDSs with parameters $(p^{2dr}, p^r, p^{2dr}, p^{(2d-1)r})$ for $d \geq 1$. For fixed p^r, successive values of the first RDS parameter p^{2dr} differ by a factor p^{2r}. We show in the first corollary

For $c \leq d-1$ or $c = d$, let

$$G_{d,c} = \prod_{u=1}^{r} Z_{p^{1+\alpha_u}} \times \prod_{u=1}^{w} Z_{p^{1+\beta_u}}, \tag{7}$$

where $w \geq r$, $Q_{d,c}$ is contained in the first $2r$ direct factors of $G_{d,c}$, $U_{d,c}$ is contained in the first r direct factors of $G_{d,c}$, $c-1 \geq \alpha_u \geq 0$ for each u, and $c-1 \geq \beta_1 \geq \beta_2 \geq \ldots \geq \beta_w \geq 0$. By the third isomorphism theorem for groups, $(G_{d,c}/H_i)/(Q_{d,c}/H_i) \cong G_{d,c}/Q_{d,c}$ and so

$$(G_{d,c}/H_i)/(Q_{d,c}/H_i) \cong \prod_{u=1}^{r} Z_{p^{\alpha_u}} \times \prod_{u=1}^{r} Z_{p^{\beta_u}} \times \prod_{u=r+1}^{w} Z_{p^{1+\beta_u}}. \tag{8}$$

Furthermore from (7),

$$G_{d,c}/U_{d,c} \cong \prod_{u=1}^{r} Z_{p^{\alpha_u}} \times \prod_{u=1}^{w} Z_{p^{1+\beta_u}}, \tag{9}$$

and by assumption (9) contains a subgroup T of index $p^{(d+c-2j-1)r}$ and exponent at most p^j for each j in the range $\bar{c} \leq j \leq c-1$. Let $s = s(j)$ be the largest u for which $\beta_u \geq j$. If $s \geq r$ then it clearly follows that (8) contains a subgroup (isomorphic to T) of index $p^{(d+c-2j-1)r}/p^r$ and exponent at most p^j. If $s < r$ then $\beta_u < j$ for all $u > s$ and so (8) contains a subgroup of exponent at most p^j and index at most $p^{(c-1-j)r+(c-1-j)s} < p^{(c-1-j)r+(d-1-j)r}$ (since $c \leq d$). Therefore for $s \geq r$ or $s < r$, (8) contains a subgroup of index $p^{(d+c-2j-2)r}$ and exponent at most p^j. This completes the proof when $c \leq d-1$.

When $c = d$ the above argument shows that, for each j in the range $\bar{c} \leq j \leq d-2$, G'/Q' contains a subgroup of index $p^{(2d-2j-2)r}$ and exponent at most p^j, where $G' = G_{d,d}/H_i$ and $Q' = Q_{d,d}/H_i$. Let S'/Q' be any subgroup of G'/Q' of index p^r and minimal exponent for which the exponent is attained in a minimal number of direct factors. Then any subgroup of S'/Q' of index $p^{(2d-2j-2)r}/p^r$ and minimal exponent has exponent at most p^j. The pre-image $S' = S/H_i$ of S'/Q' under the quotient mapping from G' to G'/Q' will be the subgroup of $G' = G_{d,d}/H_i$ of index p^r we are seeking. It remains to show that for some choice of S'/Q' as specified above, S' has exponent at most p^{d-1}. Now by definition $1+\alpha_u \leq d$ and $1+\beta_u \leq d$ for all u, and by assumption (taking $c = d$ and $j = d-1$) (9) contains a subgroup of index p^r and exponent at most p^{d-1}. Therefore the largest u for which $1+\beta_u = d$ is at most r. Hence from (8), G'/Q' has exponent at most p^{d-1} and from (7), if $G_{d,d}$ attains the exponent p^d it does so only in the first $2r$ direct factors. Lemma 4.4 then implies that if $G' = G_{d,d}/H_i$ attains the exponent p^d it does so in at most r direct factors, and moreover we can rewrite the generators of $G_{d,d}$ if necessary so that all such direct factors belong to a subgroup of rank r containing $Q' = Q_{d,d}/H_i$. The exponent attained in these direct factors will be reduced to p^{d-1} in G'/Q' (and we have already established that the exponent of G'/Q' is at most p^{d-1}). We can therefore ensure that S' has exponent at most p^{d-1} by insisting that the selection of S'/Q', as a subgroup of G'/Q' of index p^r and minimal exponent attained a minimal number of times, reduces the exponent attained in these direct factors of G'/Q' to p^{d-2} in preference to any other direct factors of G'/Q' attaining the exponent p^{d-1}. This completes the proof when $c = d$.

the set of all ordered pairs $(G_{3,3}, U_{3,3})$ for which $G_{3,3}$ has order p^{6r} and exponent at most p^3, subject to two constraints. The first, that $G_{3,3}/U_{3,3}$ contains a subgroup of index p^r and exponent at most p^2, arises directly from condition (ii) as a result of the increase in exponent from p^2 to p^3. The second, that $G_{3,3}/U_{3,3}$ contains a subgroup of index p^{3r} and exponent p, is inherited via condition (ii) from the constraint on $\mathcal{K}_{2,2}$. Note that $\mathcal{K}_{2,2}$ contains $(Z_{p^2}^{2r}, Z_p^r)$ and $\mathcal{K}_{3,3}$ contains $(Z_{p^3}^{2r}, Z_p^r)$. This illustrates that the rank of the Sylow p-subgroup of $G_{d,c}$ need not increase from the minimum value of $2r$, as required so that the subgroup $Q \cong Z_p^{2r}$ exists.

Following the pattern of the above example, we now produce an explicit form for allowable ordered pairs $(G_{d,c}, U_{d,c})$ from Theorem 7.1, involving the existence of a subgroup of $G_{d,c}/U_{d,c}$ of exponent p^j for each j in the range $\bar{c} \le j \le c-1$. Although the following theorem constructs many such ordered pairs, it is necessary to check only that the subgroup conditions hold for a particular ordered pair $(G_{d,c}, U_{d,c})$ and a particular value of d and c to conclude that the stated BS exists for this ordered pair. For the moment we take $G_{d,c}$ to be a p-group.

Theorem 7.5 *Let p be prime and let $r \ge 1$. Suppose there exists a $(p^r a, p^r\sqrt{at}, p^r t)$ BS on any p-group $G_{\bar{c},\bar{c}}$ of order $p^{2r}a$ and exponent at most $p^{\bar{c}}$ relative to any subgroup $U_{\bar{c},\bar{c}} \cong Z_p^r$, where $a > p^{\bar{c}(2r-1)-2r-1}$ and $\bar{c} \ge 1$. Then for each d and c satisfying $\bar{c} \le c \le d$, there exists a $(p^{(d+c-2\bar{c}+1)r}a, p^{(d-\bar{c}+1)r}\sqrt{at}, p^{(d-c+1)r}t)$ BS on any p-group $G_{d,c}$ of order $p^{(d+c-2\bar{c}+2)r}a$ and exponent at most p^c relative to any subgroup $U_{d,c} \cong Z_p^r$, where, for each j in the range $\bar{c} \le j \le c-1$, $G_{d,c}/U_{d,c}$ contains a subgroup of index $p^{(d+c-2j-1)r}$ and exponent at most p^j.*

Furthermore the theorem remains true for $\bar{c} \ge 2$ if $U_{\bar{c},\bar{c}}$ is additionally constrained to be contained within a subgroup of $G_{\bar{c},\bar{c}}$ isomorphic to $Z_{p^2}^r$, provided that each $U_{d,c}$ is likewise contained within a subgroup of $G_{d,c}$ isomorphic to $Z_{p^2}^r$.

Proof: We shall apply Theorem 7.1, taking $\mathcal{K}_{d,c}$ to be the set of all ordered pairs $(G_{d,c}, U_{d,c})$ for which $G_{d,c}$ is any p-group of order $p^{(d+c-2\bar{c}+2)r}a$ and exponent at most p^c and $U_{d,c}$ is any subgroup isomorphic to Z_p^r provided that, for each j in the range $\bar{c} \le j \le c-1$, $G_{d,c}/U_{d,c}$ contains a subgroup of index $p^{(d+c-2j-1)r}$ and exponent at most p^j. The condition on $\mathcal{K}_{\bar{c},\bar{c}}$ is true by assumption. Consider d and c satisfying $d > \bar{c}$ and $\bar{c} \le c \le d$. Since $G_{d,c}$ has order $p^{(d+c-2\bar{c}+2)r}a$ and exponent at most p^c, and by assumption $a > p^{\bar{c}(2r-1)-2r-1}$, it is straightforward to show that $\mathrm{rank}(G_{d,c}) > 2r-1$. Therefore $G_{d,c}$ contains a subgroup $Q_{d,c} \cong Z_p^{2r}$ containing $U_{d,c}$. Choose the subgroups H_i of $G_{d,c}$ corresponding to hyperplanes of $Q_{d,c}$ so that $H_0 = U_{d,c}$, and consider $H_i \ne H_0$. The result follows from Theorem 7.1 subject to the following two conditions. Firstly, when $c \le d-1$, $(G_{d,c}/H_i)/(Q_{d,c}/H_i)$ contains a subgroup of index $p^{(d+c-2j-2)r}$ and exponent at most p^j for each j in the range $\bar{c} \le j \le c-1$. Secondly, $G_{d,d}/H_i$ contains a subgroup S/H_i (containing $Q_{d,d}/H_i$) of index p^r and exponent at most p^{d-1} such that, for each j in the range $\bar{c} \le j \le d-2$, $(S/H_i)/(Q_{d,d}/H_i)$ contains a subgroup of index $p^{(2d-2j-3)r}$ and exponent at most p^j. We now demonstrate the existence of the required subgroups when $c \le d-1$ and when $c = d$ to complete the proof.

chosen as above so that Q/H_i is contained in a subgroup of S/H_i isomorphic to Z_4 when $d > 2$. □

The examples of BSs used at the beginning of this section to introduce Theorem 7.1 are given by the extreme cases $c = 1$ and $c = d$ of Corollary 7.3 (i). We now show the condition in Corollary 7.3 (ii), that $U_{d,c}$ is contained within a subgroup of $G_{d,c}$ isomorphic to Z_4, to be necessary. This is a consequence of the character sum modulus $2^{(2d-1)/2}m$ being non-integer.

Lemma 7.4 *Suppose there exists a (a, m, t) BS on a group $G \times W$ relative to a subgroup U of G, where G is a 2-group and m is not integer. Then* $\mathrm{rank}(G/U) = \mathrm{rank}(G)$.

Proof: Suppose, for a contradiction, that $\mathrm{rank}(G/U) < \mathrm{rank}(G)$. Then U contains a nonidentity element u for which there is no $g \in G \times W$ satisfying $g^2 = u$. Then we can define χ to be the character mapping u to -1 and mapping every element of $G \times W$ not in $\langle u \rangle$ to 1. χ is nonprincipal on U and so by the definition of BS there is a building block B_i for which $|\chi(B_i)| = m$. But $\chi(B_i)$ is the sum of terms each of which is 1 or -1 whereas by assumption m is not integer. □

A RDS in a group $U \times W$ relative to U is said to be "splitting"; the conclusion $\mathrm{rank}(G/U) = \mathrm{rank}(G)$ implies in particular that the BS in Lemma 7.4 cannot have this form.

We have seen how to apply Theorem 7.1 when $p^r = 2$. We now examine conditions (i) and (ii) of the Theorem more closely in order to indicate how we shall apply it when $p^r > 2$. Suppose we begin with the BSs of Corollary 4.2, taking $a = t = 1$ and $\mathcal{K}_{1,1} = \{(Z_p^{2r}, Z_p^r)\}$. Then clearly we can satisfy condition (i) by choosing $\mathcal{K}_{2,1} = \{(Z_p^{3r}, Z_p^r)\}$. We can satisfy condition (ii) by choosing $\mathcal{K}_{2,2}$ to be the set of all ordered pairs $(G_{2,2}, U_{2,2})$ for which $G_{2,2}$ has order p^{4r} and exponent at most p^2 subject to the constraint, for each $H_i \neq H_0$, that $G_{2,2}/H_i$ contains a subgroup of index p^r and exponent p containing Q/H_i. We shall show that these constraints on the $H_i \neq H_0$ are all implied by the single constraint that $G_{2,2}/U_{2,2}$ contains a subgroup of index p^r and exponent p (by suitable choice of the subgroup $Q \cong Z_p^{2r}$). In other words, the single constraint is that $G_{2,2}/U_{2,2}$ attains its maximum exponent p^2 at most r times. For example, if $G_{2,2} = Z_p^{2r-2} \times Z_{p^2}^{r+1}$ (where $r > 1$) and we write the subgroup $U_{2,2} \cong Z_p^r$ as being contained within r direct factors of $G_{2,2}$ then all choices of $U_{2,2}$ are allowed, except possibly $U_{2,2}$ being contained within the subgroup Z_p^{2r-2}. This demonstrates that even when all positions of $U_{\bar{c},\bar{c}}$ within $G_{\bar{c},\bar{c}}$ are allowed, not all positions of $U_{d,c}$ within $G_{d,c}$ are necessarily allowed.

Continuing to the next level $d = 3$, we can similarly take $\mathcal{K}_{3,1} = \{(Z_p^{4r}, Z_p^r)\}$. We then satisfy condition (i) by choosing $\mathcal{K}_{3,2}$ to be the set of all ordered pairs $(G_{3,2}, U_{3,2})$ for which $G_{3,2}$ has order p^{5r} and exponent at most p^2, provided that $(G_{3,2}/H_i, Q/H_i)$ is contained in $\mathcal{K}_{2,2}$. This requires $(G_{3,2}/H_i)/(Q/H_i)$ to contain a subgroup of index p^r and exponent p for each $H_i \neq H_0$. We shall show that these constraints are all implied by the single constraint that $G_{3,2}/U_{3,2}$ contains a subgroup of index p^{2r} and exponent p. Thus, a constraint for $(d, c) = (2, 2)$ forces a constraint for $(d, c) = (3, 2)$ and will likewise propagate to all $(d, 2)$ with $d > 2$. We then satisfy condition (ii) by choosing $\mathcal{K}_{3,3}$ to be

Theorem 7.1 is particularly straightforward to apply when $p^r = 2$ and we now do so, after giving another construction for a BS from a covering EBS similar to Lemma 6.3.

Lemma 7.2 *Let M be a group of odd order m^2. Suppose there exists a $(m^2, m, 2, -)$ covering EBS on $Z_2 \times M$. Then there exists a $(4m^2, 2^{3/2}m, 2)$ BS on $Z_4 \times Z_2 \times M$ relative to the subgroup of order 2 contained within Z_4.*

Proof: Let $Z_4 \times Z_2 = \langle x, y \mid x^4 = y^2 = 1 \rangle$ and let $\{A, B\}$ be a $(m^2, m, 2, -)$ covering EBS on $G = \langle y \rangle \times M$. Define the subsets $C = (1 + x)(A + x^2(G \setminus A))$ and $D = (1 + x)(B + x^2(G \setminus B))$ of $Z_4 \times Z_2 \times M$. A similar method to the proof of Lemma 6.3 shows that $\{C, D\}$ is a $(4m^2, 2^{3/2}m, 2)$ BS on $\langle x \rangle \times G$ relative to $\langle x^2 \rangle$. □

Corollary 7.3 *Let M be either the trivial group or the group $\prod_i Z_{3^{\alpha_i}}^2 \times \prod_j Z_{p_j}^4$, where $\alpha_i \geq 1$ and where p_j is a prime congruent to 3 modulo 4 or $p_j = 5$, and let $|M| = m^2$.*

(i) *For each d and c satisfying $1 \leq c \leq d$, there exists a $(2^{d+c-1}m^2, 2^d m, 2^{d-c+1})$ BS on $G_{d,c} \times M$ relative to any subgroup of order 2, where $G_{d,c}$ is any group of order 2^{d+c} and exponent at most 2^c.*

(ii) *For each d and c satisfying $2 \leq c \leq d$, there exists a $(2^{d+c-2}m^2, 2^{(2d-1)/2}m, 2^{d-c+1})$ BS on $G_{d,c} \times M$ relative to any subgroup $U_{d,c}$ of order 2 which is contained within a subgroup of $G_{d,c}$ isomorphic to Z_4, where $G_{d,c}$ is any group of order 2^{d+c-1} and exponent at most 2^c.*

Proof: By Corollary 6.7 (i) there exists a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on M. Therefore (as in the proof of Corollary 6.4) there exists a $(m^2, m, 2, -)$ covering EBS on $Z_2 \times M$. We shall now apply Theorem 7.1 with $p^r = 2$.

For (i), let $a = m^2$ and $\bar{c} = t = 1$ and take $\mathcal{K}_{d,c}$ to be the set of all ordered pairs $(G_{d,c} \times M, U_{d,c})$ for which $G_{d,c}$ is a group of order 2^{d+c} and exponent at most 2^c and $U_{d,c}$ is a subgroup of order 2. By Lemma 6.3 there exists a $(2m^2, 2m, 2)$ BS on $Z_2^2 \times M$ relative to Z_2, which satisfies the condition on $\mathcal{K}_{\bar{c},\bar{c}}$. Let $Q \cong Z_2^2$ be a subgroup of $G_{d,c}$ containing $H_0 = U_{d,c}$ and let the subgroups of $G_{d,c}$ of order 2, corresponding to hyperplanes when viewed as subgroups of Q, be H_0, H_1 and H_2. For $H_i \neq H_0$ and $d > 1$, clearly $G_{d,c}/H_i$ has order 2^{d+c-1} and exponent at most 2^c when $c \leq d - 1$, and it is easily shown that $G_{d,d}/H_i$ contains a subgroup S/H_i (containing Q/H_i) of index 2 and exponent at most 2^{d-1}. The result follows from Theorem 7.1.

For (ii), let $a = 2m^2$, $\bar{c} = 2$ and $t = 1$ and take $\mathcal{K}_{d,c}$ to be the set of all ordered pairs $(G_{d,c} \times M, U_{d,c})$ for which $G_{d,c}$ is a group of order 2^{d+c-1} and exponent at most 2^c and $U_{d,c}$ is a subgroup of order 2 contained within a subgroup of $G_{d,c}$ isomorphic to Z_4. By Lemma 7.2 there exists a $(4m^2, 2^{3/2}m, 2)$ BS on $Z_4 \times Z_2 \times M$ relative to the subgroup of order 2 contained within Z_4, which satisfies the condition on $\mathcal{K}_{\bar{c},\bar{c}}$. The remainder of the proof is similar to that of (i), with an additional condition on Q/H_i which we now demonstrate. By Lemma 4.4, Q/H_i is contained in a subgroup of $G_{d,c}/H_i$ isomorphic to Z_4 for $c \leq d$. In the case $c = d$, this implies that the subgroup S/H_i of $G_{d,d}/H_i$ can be

minimum value $\bar{c}$ up to d, which will be used in applications of Theorem 7.1 to indicate the maximum exponent p^c of the Sylow p-subgroup of the group $G_{d,c}$.

Theorem 7.1 *Let p be prime and let $r \geq 1$ and $\bar{c} \geq 1$. For each $d \geq \bar{c}$ and for each c in the range $\bar{c} \leq c \leq d$ let $\mathcal{K}_{d,c}$ be a set of ordered pairs $(G_{d,c}, U_{d,c})$, where $G_{d,c}$ is a group of order $p^{(d+c-2\bar{c}+2)r}a$ containing a subgroup $U_{d,c} \cong Z_p^r$. Suppose that for each $(G_{\bar{c},\bar{c}}, U_{\bar{c},\bar{c}}) \in \mathcal{K}_{\bar{c},\bar{c}}$ there exists a $(p^r a, p^r\sqrt{at}, p^r t)$ BS on $G_{\bar{c},\bar{c}}$ relative to $U_{\bar{c},\bar{c}}$. Suppose also that, for each $d > \bar{c}$ and for each c in the range $\bar{c} \leq c \leq d$ and for each $(G_{d,c}, U_{d,c}) \in \mathcal{K}_{d,c}$, $G_{d,c}$ contains a subgroup $Q \cong Z_p^{2r}$ and subgroups $H_0 = U_{d,c}, H_1, \ldots H_{p^r}$ of order p^r (corresponding to hyperplanes when viewed as subgroups of Q) such that, for all $H_i \neq H_0$,*

(i) *$\mathcal{K}_{d-1,c}$ contains an ordered pair isomorphic to $(G_{d,c}/H_i, Q/H_i)$ for each c in the range $\bar{c} \leq c \leq d-1$, and*

(ii) *$G_{d,d}/H_i$ contains a subgroup S/H_i of index p^r such that $\mathcal{K}_{d-1,d-1}$ contains an ordered pair isomorphic to $(S/H_i, Q/H_i)$.*

Then for each $d \geq \bar{c}$ and for each c in the range $\bar{c} \leq c \leq d$ and for each $(G_{d,c}, U_{d,c}) \in \mathcal{K}_{d,c}$ there exists a $(p^{(d+c-2\bar{c}+1)r}a, p^{(d-\bar{c}+1)r}\sqrt{at}, p^{(d-c+1)r}t)$ BS on $G_{d,c}$ relative to $U_{d,c}$.

Proof: The proof is by induction on d. The case $d = \bar{c}$ is true by assumption. Assume the case $d-1$ to be true (for each value of c in the range $\bar{c} \leq c \leq d-1$) and consider $H_i \neq H_0$. For each value of c in the range $\bar{c} \leq c \leq d$ we can apply Theorem 4.3 with $G = G_{d,c}$ and $H_0 = U_{d,c}$ to establish the case d, provided there exists a $(p^{(d+c-2\bar{c})r}a, p^{(d-\bar{c})r}\sqrt{at}, p^{(d-c)r}t)$ BS on $G_{d,c}/H_i$ relative to Q/H_i. The subsequent analysis depends on whether $c \leq d-1$ or $c = d$. When $c \leq d-1$, by assumption $\mathcal{K}_{d-1,c}$ contains an ordered pair isomorphic to $(G_{d,c}/H_i, Q/H_i)$ so the required BS is given by the inductive hypothesis with the value c. When $c = d$, there is no inductive hypothesis with the value c. But by assumption $G_{d,d}/H_i$ contains a subgroup S/H_i of index p^r such that $\mathcal{K}_{d-1,d-1}$ contains an ordered pair isomorphic to $(S/H_i, Q/H_i)$. Therefore by the inductive hypothesis there exists a $(p^{(2d-2\bar{c}-1)r}a, p^{(d-\bar{c})r}\sqrt{at}, p^r t)$ BS on S/H_i relative to Q/H_i. Then Lemma 2.1 with $s = p^r$ gives the required BS on $G_{d,d}/H_i$ relative to Q/H_i. This completes the induction. □

The special case $\bar{c} = c = 1$ of Theorem 7.1 is similar to Theorem 4.6. We shall consider groups $G_{d,c}$ in Theorem 7.1 whose Sylow p-subgroup has exponent at most p^c. The minimum value of c is $\bar{c}$, which will be either 1 or 2. (For example, we must take $\bar{c} = 2$ when considering an initial $(4, 2\sqrt{2}, 2)$ BS on a group G of order 8 relative to a subgroup U of order 2, which we shall later show exists only if U is contained in a subgroup of G isomorphic to Z_4.) Then, since $G_{d,c}$ has order $p^{(d+c-2\bar{c}+2)r}a$, for fixed $d > 2$ we see that for larger values of c the number of building blocks $p^{(d-c+1)r}t$ is smaller but the Sylow p-subgroup is allowed to have smaller rank (and larger exponent). Furthermore by Theorem 2.2 we can construct a semi-regular RDS in groups $G'_{d,c}$ for which the exponent of the Sylow p-subgroup is a multiple of $p^{c+(d-c+1)r}$. For $r > 1$ this means we can achieve a smaller rank for $G'_{d,c}$, by taking c large, at the cost of a smaller maximum exponent. For further details see Section 8.

(iv) *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}.*

Proof: For (i), apply Theorem 6.5 to the initial covering EBSs of Theorem 6.6. Then (ii), (iii) and (iv) follow from Corollary 6.4. □

Corollary 6.7 (iv) is one of the central results of the paper, together with Corollary 5.3 (once again, the groups involved are implicitly abelian). There are no other abelian groups known to contain Hadamard difference sets. The case where M is trivial is due to Kraemer [26]. When combined with an exponent bound given by Turyn [49], Kraemer's result states that Hadamard difference sets exist in abelian groups of order 2^{2d+2} if and only if the exponent is at most 2^{d+2}. For the case where M is nontrivial many nonexistence results depending on number theoretic conditions are known (for details see Davis and Jedwab [11]).

7 Families of building sets

In this section we demonstrate the full power of the recursive construction for BSs of Section 4 by applying Theorem 4.3 systematically to a small initial set of BSs. This produces several families of BSs, including as special cases all those previously found in Sections 5 and 6 for the purpose of constructing difference sets. The BSs constructed here will be used in Section 8 to deduce the existence of families of semi-regular RDSs, and in Section 9 when we discuss nonabelian groups. Since the construction is based on Theorem 4.3, all the BSs are defined on a group G relative to an elementary abelian subgroup U, although G will not necessarily be a p-group. We are now interested not only in the groups G on which BSs with given parameters exist, but also in the different possible subgroups U. The arguments in this section are probably the most difficult in the paper!

In general, we wish to find $(a, \sqrt{at}, t)$ BSs for which the number of building blocks t is large. We have seen in Section 5 that difference sets in several parameter families can be constructed from BSs using Theorem 3.2 only when t is large, and by Lemma 2.1 a $(a, \sqrt{at}, t)$ BS on a group G is clearly a more general object than a $(as, \sqrt{at}, t/s)$ BS on a group G' containing G as a subgroup of index s. On the other hand, we have seen in Section 6 that it is possible to trade the growth in t under the recursive application of Theorem 4.3 for a more general form for the group G. For example, for any $d \geq 1$, by Theorem 5.1 (i) there is a $(2^d, 2^d, 2^d)$ BS on Z_2^{d+1} relative to Z_2 whereas by Corollary 6.7 (ii) there is a $(2^{2d-1}, 2^d, 2)$ BS on any group of order 2^{2d} and exponent at most 2^d relative to any subgroup of order 2. The first set of BSs is more general in that the number of building blocks is 2^d rather than 2, but the second set of BSs is more general in that the group rank can be as small as 2 rather than $d+1$. (Lemma 2.1 allows some of the second set of BSs to be constructed from the first, but not when the group rank is less than $d+1$). We now present a general recursive application of Theorem 4.3 which gives the result of applying Lemma 2.1 prior to Theorem 4.3 as desired, throughout the recursion, to the BSs with the smallest number of building blocks. As before, the recursion is controlled by the parameter d. We introduce a new parameter c, ranging from a

D has nonzero character sum (with modulus $m_1 m_2$). By symmetry in the subscripts 1 and 2 in the equations (6), it is now sufficient to consider the case when χ is principal on M_1 and nonprincipal on M_2. Exactly one of the building blocks A_2, B_2, C_2 and D_2 then has a nonzero character sum. If this building block is A_2 then $\chi(B) = \chi(D) = 0$, $\chi(C) = (|M_1| - |C_1| - |D_1|)\chi(A_2) = 0$ and $\chi(A) = (|M_1| - |A_1| - |B_1|)\chi(A_2) = m_1\chi(A_2)$, which has modulus $m_1 m_2$. If instead the building block with nonzero character sum is B_2, C_2 or D_2 then similar calculations show that C, B or D respectively has nonzero character sum (with modulus $m_1 m_2$) while the rest of A, B, C and D have zero character sum. □

Theorem 6.5 is based on a construction of Turyn [50] involving incidence matrices of Hadamard difference sets known as Williamson matrices. (The form of the construction given in [50] corresponds to the equations for the S_i in the above proof). In Theorem 6.5 we have established additional character properties of Turyn's construction for use in Corollary 6.4. The construction of Hadamard difference sets now relies on finding initial $(m(\frac{m-1}{2}), m, 4, +)$ covering EBSs on groups of order m^2 (which, from the relationship between covering EBS parameters given after Theorem 2.4, must be odd). The following examples are known.

Theorem 6.6 *There exists a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on the following groups M of order m^2:*

(i) *M is the trivial group.*

(ii) *$M = Z_{3^\alpha}^2$, where $\alpha \geq 1$.*

(iii) *$M = Z_p^4$, where p is a prime congruent to 3 modulo 4.*

(iv) *$M = Z_5^4$.*

Theorem 6.6 (ii) is due to Arasu, Davis, Jedwab and Sehgal [2]. Theorem 6.6 (iii) is due to Xiang and Chen [52], who showed that Xia's construction [51] of Hadamard difference sets in $Z_4 \times Z_p^4$ could be viewed as depending on subsets whose character properties correspond to those of a covering EBS. Theorem 6.6 (iv) is due to van Eupen and Tonchev [18], whose example of a reversible Hadamard difference set in $Z_2^2 \times Z_5^4$ we have verified to correspond to a $(300, 25, 4, +)$ covering EBS on Z_5^4.

Corollary 6.7 *Let M be either the trivial group or the group $\prod_i Z_{3^{\alpha_i}}^2 \times \prod_j Z_{p_j}^4$, where $\alpha_i \geq 1$ and where p_j is a prime congruent to 3 modulo 4 or $p_j = 5$, and let $|M| = m^2$. Then the following exist:*

(i) *A $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on M.*

(ii) *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.*

(iii) *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.*

supplementary quadruple," which is the initial object for the recursive constructions in [23].) We believe the method presented here to be much clearer.

We have chosen in Corollary 6.4 to begin with a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on M, although it is clear from the proof that it would be sufficient to begin with a $(m^2, m, 2, -)$ covering EBS on $Z_2 \times M$. (In the running example of this section, a $(3, 3, 4, +)$ covering EBS on Z_3^2 implies the existence of the required $(9, 3, 2, -)$ covering EBS on $Z_2 \times Z_3^2$.) The reason is the following composition theorem for $(m(\frac{m-1}{2}), m, 4, +)$ covering EBSs.

Theorem 6.5 *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 $(m_1 m_2(\frac{m_1 m_2-1}{2}), m_1 m_2, 4, +)$ covering EBS on $M_1 \times M_2$.*

Proof: For $i = 1, 2$ let $\{A_i, B_i, C_i, D_i\}$ be a $(m_i(\frac{m_i-1}{2}), m_i, 4, +)$ covering EBS on M_i and let the building block containing $m_i(\frac{m_i+1}{2})$ elements be D_i. Define the following elements of the group ring $Z[M_1 \times M_2]$:

$$\left.\begin{array}{rcl} A &=& M_1A_2 + A_1M_2 - A_1A_2 + B_1B_2 - A_1B_2 - B_1A_2, \\ B &=& M_1C_2 + A_1M_2 - A_1C_2 + B_1D_2 - A_1D_2 - B_1C_2, \\ C &=& M_1A_2 + C_1M_2 - C_1A_2 + D_1B_2 - C_1B_2 - D_1A_2, \\ D &=& M_1C_2 + C_1M_2 - C_1C_2 + D_1D_2 - C_1D_2 - D_1C_2. \end{array}\right\} \quad (6)$$

We firstly show that each of these elements can be regarded as a subset of $M_1 \times M_2$ (so the coefficients in the group ring are 0 or 1). Consider the following subsets of $M_1 \times M_2$:

$$\begin{array}{rcl} S_1 &=& (A_1 \cap B_1) \times (M_2 \setminus A_2), \\ S_2 &=& ((M_1 \setminus A_1) \cap (M_1 \setminus B_1)) \times A_2, \\ S_3 &=& (A_1 \cap (M_1 \setminus B_1)) \times (M_2 \setminus B_2), \\ S_4 &=& ((M_1 \setminus A_1) \cap B_1) \times B_2. \end{array}$$

By inspection the S_i have empty pairwise intersection. Let $T = A_1 \cap B_1$, and note that we can write $(M_1 \setminus A_1) \cap (M_1 \setminus B_1)$ as $(M_1 \setminus A_1) \setminus (B_1 \setminus T)$. Then in the group ring we have $S_1 = T(M_2 - A_2)$, $S_2 = (M_1 - A_1 - B_1 + T)A_2$, $S_3 = (A_1 - T)(M_2 - B_2)$ and $S_4 = (B_1 - T)B_2$, from which $S_1 + S_2 + S_3 + S_4 = A$. Since the S_i have empty pairwise intersection, A is therefore a subset of $M_1 \times M_2$. Similar arguments hold for B, C and D.

We claim that $\{A, B, C, D\}$ is a $(m_1 m_2(\frac{m_1 m_2-1}{2}), m_1 m_2, 4, +)$ covering EBS on $M_1 \times M_2$. To show that A, B, C and D have the correct size, note that for $i = 1, 2$ we have $|M_i| = m_i^2$, $|A_i| = |B_i| = |C_i| = m_i(\frac{m_i-1}{2})$ and $|D_i| = m_i(\frac{m_i+1}{2})$. Then from (6) we have $|A| = |M_1A_2| + |A_1M_2| - |A_1A_2| + |B_1B_2| - |A_1B_2| - |B_1A_2| = m_1m_2(\frac{m_1m_2-1}{2})$, and similar calculations show that $|B| = |C| = m_1m_2(\frac{m_1m_2-1}{2})$ and $|D| = m_1m_2(\frac{m_1m_2+1}{2})$. It remains to establish the character properties for $\{A, B, C, D\}$.

Let χ be a nonprincipal character of $M_1 \times M_2$. Firstly consider the case when χ is nonprincipal on M_1 and M_2. Then the terms in (6) involving M_1 or M_2 have a character sum of 0. By the definition of covering EBS, for $i = 1, 2$ exactly one of A_i, B_i, C_i and D_i has nonzero character sum (with modulus m_i). Since each term X_1Y_2, where $X, Y \in \{A, B, C, D\}$, occurs exactly once in (6) it follows that exactly one of A, B, C and

Lemma 6.3 *Let M be a group of odd order m^2. Suppose there exists a $(m^2, m, 2, -)$ covering EBS on $Z_2 \times M$. Then there exists a $(2m^2, 2m, 2)$ BS on $Z_2^2 \times M$ relative to Z_2.*

Proof: Let $Z_2^2 = \langle x, y \mid x^2 = y^2 = 1 \rangle$ and let $\{A, B\}$ be a $(m^2, m, 2, -)$ covering EBS on $G = \langle y \rangle \times M$, where the building block containing $m^2 - m$ elements is A. Define the subsets $C = A + x(G \setminus A)$ and $D = B + x(G \setminus B)$ of $Z_2^2 \times M$.

Let χ be a nonprincipal character of $\langle x \rangle \times G$. Firstly consider the case when χ is nonprincipal on G. By the definition of covering EBS, $\{|\chi(A)|, |\chi(B)|\} = \{0, m\}$ so $\{|\chi(C)|, |\chi(D)|\} = \{0, m|1 - \chi(x)|\}$. Therefore if χ is also nonprincipal on $\langle x \rangle$ (so χ maps x to -1) we have $\{|\chi(C)|, |\chi(D)|\} = \{0, 2m\}$ whereas if χ is principal on $\langle x \rangle$ then $\chi(C) = \chi(D) = 0$. Next consider the case when χ is principal on G (and so nonprincipal on $\langle x \rangle$). This gives $\chi(C) = |A| - (|G| - |A|) = -2m$ and $\chi(D) = |B| - (|G| - |B|) = 0$.

Combining the two cases, $\{C, D\}$ is a $(2m^2, 2m, 2)$ BS on $\langle x \rangle \times G$ relative to $\langle x \rangle$. □

For example, at the beginning of this section we assumed the existence of a $(9, 3, 2, -)$ covering EBS on $Z_2 \times Z_3^2$ and a $(18, 6, 2)$ BS on $Z_2^2 \times Z_3^2$ relative to Z_2. By Lemma 6.3 the existence of the second is implied by the existence of the first.

We now combine Theorems 6.1 and 6.2 and Lemma 6.3 to show that only an initial covering EBS is required for the recursions.

Corollary 6.4 *Suppose there exists a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on a group M of odd order m^2. Then the following exist:*

(i) *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.*

(ii) *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.*

(iii) *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}.*

Proof: For (i), by assumption there exists a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on M. Apply Lemma 2.3 with $s = 2$ to obtain a $(m(m-1), m, 2, +)$ covering EBS on $Z_2 \times M$. This can be equivalently written as a $(m^2, m, 2, -)$ covering EBS on $Z_2 \times M$, so from Lemma 6.3 there is a $(2m^2, 2m, 2)$ BS on $Z_2^2 \times M$ relative to Z_2. Apply Theorem 6.2.

For (ii), as noted above there is a $(m^2, m, 2, -)$ covering EBS on $Z_2 \times M$. Apply Theorem 6.1 to this covering EBS and the BSs of (i).

For (iii), apply Theorem 2.4. The case $d = 0$ results from a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on M, which exists by assumption. Each case $d \geq 1$ results from the covering EBSs of (ii), noting that the group G_d in (iii) contains a subgroup of index 4 and exponent at most 2^d. □

A result broadly equivalent to Corollary 6.4 was proved by Jedwab [23] from the viewpoint of perfect binary arrays, via lengthy computation. (A $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on $\prod_{i=1}^{r} Z_{s_i}$, where $m^2 = \prod_{i=1}^{r} s_i$, implies the existence of a $s_1 \times s_2 \times \ldots \times s_r$ "binary

Theorem 6.1 *Let M be a group of odd order m^2 and for each $d \geq 1$ let $\mathcal{G}_d$ be the set of all groups of order 2^{2d} and exponent at most 2^d. Suppose that there exists a $(m^2, m, 2, -)$ covering EBS on $Z_2 \times M$. Suppose also that for each $d \geq 1$ and for each $G_d \in \mathcal{G}_d$ there exists a $(2^{2d-1}m^2, 2^d m, 2)$ BS on $G_d \times M$ relative to a subgroup U_d (depending on G_d) of order 2. Then for each $d \geq 1$ and for each $G_d \in \mathcal{G}_d$ there exists a $(2^{2d-1}m^2, 2^d m, 4, -)$ covering EBS on $G_d \times M$.*

Proof: The proof is by induction on d. We begin by establishing the case $d = 1$. By assumption there exists a $(m^2, m, 2, -)$ covering EBS on $Z_2 \times M$ and a $(2m^2, 2m, 2)$ BS on $Z_2^2 \times M$ relative to Z_2. Combine these using Theorem 3.2 with $G = Z_2^2 \times M$ and $U = Z_2$ to obtain the case $d = 1$.

Assume the case $d - 1$ to be true. For each $G_d \in \mathcal{G}_d$, by assumption there exists a $(2^{2d-1}m^2, 2^d m, 2)$ BS on $G_d \times M$ relative to a subgroup U_d of order 2. Now G_d/U_d has order 2^{2d-1} and exponent at most 2^d and so attains the exponent 2^d in at most one direct factor. Therefore G_d/U_d contains a subgroup S/U_d of index 2 and exponent at most 2^{d-1}. The inductive hypothesis then implies that there exists a $(2^{2d-3}m^2, 2^{d-1}m, 4, -)$ covering EBS on $(S/U_d) \times M$. Apply Lemma 2.3 with $s = 2$ to obtain a $(2^{2d-2}m^2, 2^{d-1}m, 2, -)$ covering EBS on $(G_d/U_d) \times M$. Combine this covering EBS with the BS on $G_d \times M$ relative to U_d, using Theorem 3.2 with $G = G_d \times M$. This shows the case d is true and completes the induction. □

We next show that the family of BSs required in Theorem 6.1 can be obtained recursively from a single BS using Theorem 4.3. Although Theorem 6.1 requires a BS on $G_d \times M$ relative to only a single subgroup U_d, the recursion produces a BS on $G_d \times M$ relative to any subgroup of order 2. By rewriting the generators of G_d we can assume that such a subgroup is contained within a single direct factor of G_d.

Theorem 6.2 *Let M be a group of odd order m^2 and for each $d \geq 1$ let $\mathcal{G}_d$ be the set of all groups of order 2^{2d} and exponent at most 2^d. Suppose there exists a $(2m^2, 2m, 2)$ BS on $Z_2^2 \times M$ relative to Z_2. Then for each $d \geq 1$ and for each $G_d \in \mathcal{G}_d$ there exists a $(2^{2d-1}m^2, 2^d m, 2)$ BS on $G_d \times M$ relative to any subgroup of order 2.*

Proof: The proof is by induction on d. The case $d = 1$ is true by assumption. Assume the case $d - 1$ to be true. For each $G_d \in \mathcal{G}_d$, let H_0 be any subgroup of order 2. Choose $Q \cong Z_2^2$ to be a subgroup of G_d containing H_0 and let the subgroups of G_d of of order 2, corresponding to hyperplanes when viewed as subgroups of Q, be H_0, H_1 and H_2. For each i, G_d/H_i has order 2^{2d-1} and exponent at most 2^d and so, as in the proof of Theorem 6.1, G_d/H_i contains a subgroup S/H_i of index 2 and exponent at most 2^{d-1}. Then by the inductive hypothesis there exists a $(2^{2d-3}m^2, 2^{d-1}m, 2)$ BS on $(S/H_i) \times M$ relative to $Q/H_i \cong Z_2$. Apply Lemma 2.1 with $s = 2$ to obtain a $(2^{2d-2}m^2, 2^{d-1}m, 1)$ BS on $(G_d/H_i) \times M$ relative to Q/H_i. Therefore by Theorem 4.3 there exists a $(2^{2d-1}m^2, 2^d m, 2)$ BS on $G_d \times M$ relative to H_0. This shows the case d is true and completes the induction. □

Previously, in Theorem 3.2, we gave a construction for a covering EBS based on the existence of a BS and another covering EBS. We now show how to construct a particular type of BS (required as the initial BS in Theorem 6.2) from a covering EBS.

new $(4608, 272, 16, 256)$ McFarland difference set. (We have imposed exponent 4 in both cases because the self-conjugacy condition from Ma and Schmidt's result [34] is always satisfied when $d = 1$.)

6 Application to Hadamard difference sets

In this section we use the key constructions, Theorem 3.2 for covering EBSs and Theorem 4.3 for BSs, to obtain difference sets with parameters from the Hadamard family (1). Although many of the results were previously known our intention is to show that the various construction methods in the literature can be concisely brought into the unifying framework of this paper. Based on this formulation, we suggest a number of generalisations in Section 9.

Since the Hadamard parameters with $N = 2^d$ are equivalent to the McFarland parameters with $q = 2$, we have already established in Corollary 5.3 (i) that there exists a Hadamard difference set in any group of order 2^{2d+2} and rank at least $d + 1$. This construction depended on the number of building blocks h and t in Theorem 3.2 being large. However we now demonstrate by means of an example that for the Hadamard parameters it is sufficient to take $h = t = 2$, which allows additional freedom in choosing the group G (which need not be a 2-group).

Assume we can find a $(9, 3, 2, -)$ covering EBS on $Z_2 \times Z_3^2$, so that by Theorem 2.4 there exists a $(36, 15, 6, 9)$ Hadamard difference set in $Z_2^2 \times Z_3^2$ and $Z_4 \times Z_3^2$. Assume also that we can find a $(18, 6, 2)$ BS on $Z_2^2 \times Z_3^2$ relative to Z_2. By Theorem 3.2 with $u = 2$, this BS and covering EBS together give a $(18, 6, 4, -)$ covering EBS on $Z_2^2 \times Z_3^2$. Therefore by Theorem 2.4 there exists a $(144, 66, 30, 36)$ Hadamard difference set in $G \times Z_3^2$ for any group G of order 16 and exponent at most 8.

Now apply Lemma 2.1 with $s = 2$ to the $(18, 6, 2)$ BS to obtain a $(36, 6, 1)$ BS on $Z_4 \times Z_2 \times Z_3^2$ and $Z_2^3 \times Z_3^2$ relative to any subgroup of order 2. Then by Theorem 4.3 with $p^r = 2$ there exists a $(72, 12, 2)$ BS on $G \times Z_3^2$ relative to any subgroup of order 2, where G is any group of order 16 and exponent at most 4 (since $G/H_i \cong Z_4 \times Z_2$ or Z_2^3). Furthermore we can apply Lemma 2.3 with $s = 2$ to the $(18, 6, 4, -)$ covering EBS to obtain a $(36, 6, 2, -)$ covering EBS on $Z_4 \times Z_2 \times Z_3^2$ and $Z_2^3 \times Z_3^2$. Then by Theorem 3.2 with $u = 2$, these $(36, 6, 2, -)$ covering EBSs together with the $(72, 12, 2)$ BSs give a $(72, 12, 4, -)$ covering EBS on $G \times Z_3^2$, where G is any group of order 16 and exponent at most 4. Therefore by Theorem 2.4 there exists a $(576, 276, 132, 144)$ Hadamard difference set in $G \times Z_3^2$ for any group G of order 64 and exponent at most 16.

The pattern indicated by this example forms the model for the constructions in this section, each step of the recursion using an initial Hadamard difference set with $N = 2^{d-1}m$ to construct a final Hadamard difference set with $N = 2^d m$, where m is odd. Provided the initial BS and covering EBS can be found, the group of order m^2 (Z_3^2 in the above example) plays no part in the recursion. For example, given a $(1, 1, 2, -)$ covering EBS on Z_2 (which is trivial) and a $(2, 2, 2)$ BS on Z_2^2 relative to Z_2 (which exists by Corollary 4.2), by the same argument as above there exists a $(64, 28, 12, 16)$ Hadamard difference set in any group of order 64 and exponent at most 16. As in Theorem 3.3 we begin by assuming the existence of an initial covering EBS and a family of BSs.

sets, relying on a single group exponent condition, is due to Kraemer [26] for Hadamard difference sets. We shall show in Section 6 that Kraemer's result can also be derived from the framework of this paper.

Corollary 5.3 (iii) is due to Spence [48]. We are not aware of any exponent bounds on the Sylow 3-subgroup for $d \geq 2$.

Corollary 5.3 (iv) describes the first new family of difference set parameters to be discovered since 1977 [48]. Apart from the case $d = 0$, giving Hadamard parameters, all the examples were previously unknown. This also gives a new family of symmetric designs with the same parameters (4). For $d = 1$, Ma and Schmidt [34] have shown that the Sylow 2-subgroup must have exponent at most 4. The only open case for difference set parameters $(320, 88, 24, 64)$ is therefore $Z_4^3 \times Z_5$. For $d > 1$, we can use standard techniques to bound the exponent of the Sylow 2-subgroup. We shall use the following special case of Theorem 4.33 of Lander [27], based on results of Turyn [49].

Theorem 5.4 *Suppose that there exists a (v, k, λ, n)-difference set in an abelian group G containing a subgroup H of index w. Suppose also that p is a prime for which $p \mid w$, $p^{2r} \mid n$ for some $r \geq 1$, p is self-conjugate modulo $\exp(G/H)$, and the Sylow p-subgroup of G/H is cyclic. Then $p^r w \leq v$.*

Corollary 5.5 *The Sylow 2-subgroup of a group containing a difference set with parameters (4) has exponent at most 2^{d+2} for d odd and at most 2^{d+3} for d even.*

Proof: The group G containing the difference set has order $v = 2^{2d+4}\frac{(2^{d+1}+1)(2^{d+1}-1)}{3}$. Let the exponent of the Sylow 2-subgroup be 2^α. We apply Theorem 5.4 with $p = 2$ and $r = 2d + 1$, seeking to take w as large as possible.

For d odd, $\frac{2^{d+1}-1}{3}$ is integer and we can choose the subgroup H so that $w = 2^\alpha(2^{d+1}+1)$ with the Sylow 2-subgroup of G/H cyclic. Now $\exp(G/H)$ divides w and 2 is self-conjugate modulo $2^\alpha(2^{d+1}+1)$, so Theorem 5.4 gives $2^{\alpha-3} \leq \frac{2^{d+1}-1}{3}$ which implies $\alpha \leq d + 2$.

For d even, $\frac{2^{d+1}-1}{3}$ is not integer so we instead choose H so that $w = 2^\alpha(\frac{2^{d+1}+1}{3})$ with the Sylow 2-subgroup of G/H cyclic. A similar argument then gives $\alpha \leq d + 3$. □

The discussion at the beginning of this section identifies the possible parameters for BSs on p-groups which could be used in Theorem 3.2 to produce difference sets. Not all of the identified parameter sets are included in Theorem 5.1. In particular, we have seen that a $(2q^d, q^d, q^d/2)$ BS on a group of order $2q^{d+1}$ relative to a subgroup of order $q = 2^r$ would yield a McFarland difference set with parameters q and d (assuming the appropriate covering EBS existed). However the only groups on which we know that such BSs exist for $q > 4$ are $Z_2^{(d+1)r+1}$ and $Z_4 \times Z_2^{(d+1)r-1}$, using Lemma 2.1 on Theorem 5.1 (i). Construction of such BSs on other groups would give new McFarland difference sets. For example, in the case $q = 8$ and $d = 1$, a $(16, 8, 4)$ BS on a group of order 128 and exponent 4 (other than $Z_4 \times Z_2^5$) relative to a subgroup of order 8 would give a new $(640, 72, 8, 64)$ McFarland difference set. The results of this paper grew out of an unsuccessful attempt to construct such a BS. In the case $q = 16$ and $d = 1$, a $(32, 16, 8)$ BS on a group of order 512 and exponent 4 (other than $Z_4 \times Z_2^7$) relative to a subgroup of order 16 would give a

There are no abelian groups known to contain difference sets in the indicated families which are not covered by this result. (As throughout the paper, the groups involved are implicitly abelian.)

Corollary 5.3 *For each $d \geq 0$, the following exist:*

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

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

(iii) *A Spence difference set in any group of order $3^{d+1}(\frac{3^{d+1}-1}{2})$ containing a subgroup isomorphic to Z_3^{d+1}.*

(iv) *A difference set with parameters (4) 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 Z_4^3 in the case $d = 1$.*

Proof: Apply Theorem 2.4 to the covering EBSs of Theorem 5.2. □

In Corollary 5.3 (i), the Sylow p-subgroup of the group containing the McFarland difference set is isomorphic to $Z_p^{(d+1)r}$ when p is odd, and is isomorphic to $Z_2^{(d+1)r+1}$ or $Z_4 \times Z_2^{(d+1)r-1}$ when $p = 2$, because p divides the index $\frac{q^{d+1}-1}{q-1} + 1$ if and only if $p = 2$. In the remaining parts of Corollary 5.3, the Sylow p-subgroup of the group containing the difference set is isomorphic to the subgroup mentioned (where $p = 2$ in parts (ii) and (iv) and $p = 3$ in part (iii).)

Corollary 5.3 (i) is due to McFarland [37] for p odd and to Dillon [16] for $p = 2$. Ma and Schmidt [35] showed that for p odd, the condition that the Sylow p-subgroup is isomorphic to $Z_p^{(d+1)r}$ is necessary as well as sufficient, provided that p is self-conjugate modulo the group exponent. (The definition of self-conjugate is given before Lemma 1.1.) In a subsequent paper Ma and Schmidt [34] showed that for $p = 2$ and $r > 1$, the Sylow 2-subgroup must have exponent at most 4 provided that 2 is self-conjugate modulo the group exponent. (For $p = 2$ and $r = 1$ the McFarland parameters correspond to Hadamard parameters with $N = 2^d$, which are considered separately in Section 6.)

Corollary 5.3 (ii) extends the set of groups known to contain McFarland difference sets in the case $q = 4$ beyond those identified in Corollary 5.3 (i). None of these additional groups was previously known to contain difference sets with the single exception, due to Arasu and Sehgal [3], of $Z_4^2 \times Z_2 \times Z_3$ in the case $d = 1$. Moreover the self-conjugacy condition from Ma and Schmidt's result [34] above is always satisfied when $q = 4$, since the exponent of a group divides the order and 2 is self-conjugate modulo $2^{2d+3}(\frac{2^{2d+1}+1}{3})$. We have therefore established that a McFarland difference set with $q = 4$ exists in an abelian group if and only if the Sylow 2-subgroup has exponent at most 4. Unlike the above result for McFarland difference sets with $q = p^r$ odd, this result does not depend on a self-conjugacy condition. The only other comparable result for families of difference

and Z_2^6 relative to Z_2^2 contained within two of the largest direct factors of the group. The remainder of the proof is similar to that of (ii) except that we must ensure $G_2/H_i \ncong Z_4^3$ for $H_i \neq H_0$. We achieve this by taking $Q \cong Z_2^4$ to be a subgroup of G_d containing $H_0 = U_d$ for $d > 1$ as before, with the additional constraint that Q be contained within four of the largest direct factors of G_d. □

Note that although the group $G_d = Z_4^3$ is not covered by the case $d = 1$ of Theorem 5.1 (iii), this exception does not propagate to higher values of d under the recursive construction of Theorem 4.6.

We next combine the BSs of Theorem 5.1 with initial covering EBSs whose parameters were previously identified in order to produce families of covering EBSs.

Theorem 5.2 *For each $d \geq 0$, the following exist:*

(i) *A $(p^{dr}, p^{dr}, \frac{p^{(d+1)r}-1}{p^r-1} + 1, -)$ covering EBS on $Z_p^{(d+1)r}$, where p is prime and $r \geq 1$.*

(ii) *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.*

(iii) *A $(3^d, 3^d, \frac{3^{d+1}-1}{2}, +)$ covering EBS on Z_3^{d+1}.*

(iv) *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 Z_4^3 in the case $d = 1$.*

Proof: The proof is by application of Theorem 3.3 to the BSs of Theorem 5.1, together with appropriate initial covering EBSs.

For (i), put $a = m = 1$, $h = 2$ and $t = p^r$, and take $\mathcal{G}_d = \{Z_p^{(d+1)r}\}$ in Theorem 3.3. There exists a trivial $(1, 1, 2, -)$ covering EBS on Z_p^r. The required BSs are provided by Theorem 5.1 (i), and $Z_p^{(d+1)r}/Z_p^r$ is isomorphic to Z_p^{dr}, which is contained in $\mathcal{G}_{d-1}$.

For (ii), put $p = r = 2$, $a = t = 2$ and $m = h = 1$, and take $\mathcal{G}_d$ to be the set of all groups of order 2^{2d+3} and exponent at most 4. There exists a trivial $(2, 1, 1, -)$ covering EBS on $Z_4 \times Z_2$ and Z_2^3. The required BSs on G_d relative to U_d are provided by Theorem 5.1 (ii), and clearly G_d/U_d is a group of order 2^{2d+1} and exponent at most 4.

For (iii), put $p = 3$, $r = 1$, $a = m = h = 1$ and $t = 3$, and take $\mathcal{G}_d = \{Z_3^{d+1}\}$. There exists a $(1, 1, 1, +)$ covering EBS on Z_3 comprising two elements (the complement of a trivial $(2, 1, 1, -)$ covering EBS on Z_3). The required BSs are provided by Theorem 5.1 (i) with $p = 3$ and $r = 1$, and Z_3^{d+1}/Z_3 is isomorphic to Z_3^d.

For (iv), put $p = r = 2$, $a = m = 2$, $h = 1$ and $t = 4$, and take $\mathcal{G}_d$ to be the set of all groups of order 2^{2d+4} and exponent at most 4 but exclude Z_4^3 from $\mathcal{G}_1$. The examples of $(16, 6, 2, 4)$-difference sets in Section 1 are equivalent to a $(4, 2, 1, +)$ covering EBS on Z_4^2, $Z_4 \times Z_2^2$ and Z_2^4. The required BSs are provided by Theorem 5.1 (iii), and G_d/U_d is a group of order 2^{2d+2} and exponent at most 4. Furthermore the choice of U_d ensures that $G_2/U_2 \ncong Z_4^3$. □

We now list the families of difference sets arising from the covering EBSs of Theorem 5.2. The unifying corollary which follows is one of the central results of the paper.

for $d = 1$, a $(2, 2, 2, +)$ covering EBS on a group of order 8. When $a = 2$ we require a $(2^{2d+2}, 2^{2d+1}, 2^{2d})$ BS on a group of order 2^{2d+4} relative to a subgroup of order 4 and, for $d = 1$, a $(4, 2, 1, +)$ covering EBS on a group of order 16.

In each case it is straightforward to find an appropriate covering EBS, so the application of the recursive construction depends on finding families of BSs as described above. We now show how to construct some of the identified families using the recursive construction for BSs of Theorem 4.6. The initial BSs can be traced to three sources: the (p^r, p^r, p^r) BS of Corollary 4.2, due to Davis [8]; the $(8, 4, 2)$ BS described in Section 2, due to Arasu and Sehgal [3]; and the $(4, 2, 1)$ BS on Z_4^2 relative to Z_2^2 described in Section 4, due to Jungnickel [24].

Theorem 5.1 *For each $d \geq 1$, the following exist:*

(i) *A (p^{dr}, p^{dr}, p^{dr}) BS on $Z_p^{(d+1)r}$ relative to Z_p^r, where p is prime and $r \geq 1$.*

(ii) *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 $U_d \cong Z_2^2$ contained within two of the largest direct factors of G_d.*

(iii) *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 $U_d \cong Z_2^2$ contained within two of the largest direct factors of G_d, except possibly $G_1 = Z_4^3$.*

Proof: The proof is by application of Theorem 4.6, using initial BSs introduced in earlier sections.

For (i), put $a = t = p^r$ and take $\mathcal{K}_d = \{(Z_p^{(d+1)r}, Z_p^r)\}$, where $H_0 = Z_p^r$ is contained within r direct factors of $Z_p^{(d+1)r}$. There exists a (p^r, p^r, p^r) BS on Z_p^{2r} relative to the subgroup Z_p^r contained within r direct factors of Z_p^{2r}, by Corollary 4.2. For $d > 1$, let $Q \cong Z_p^{2r}$ be a subgroup of $Z_p^{(d+1)r}$ containing H_0. For each subgroup $H_i \neq H_0$ of $Z_p^{(d+1)r}$ of order p^r, corresponding to a hyperplane when viewed as a subgroup of Q, Lemma 4.4 shows that $Z_p^{(d+1)r}/H_i \cong Z_p^{dr}$, and $Q/H_i \cong Z_p^r$ is contained within r direct factors of Z_p^{dr}. Therefore $\mathcal{K}_{d-1}$ contains an ordered pair isomorphic to $(Z_p^{(d+1)r}/H_i, Q/H_i)$ and the result follows from Theorem 4.6.

For (ii), put $p = r = 2$, $a = 8$ and $t = 2$, and take $\mathcal{K}_d$ to be the set of all ordered pairs (G_d, U_d) for which G_d is a group of order 2^{2d+3} and exponent at most 4 and $U_d \cong Z_2^2$ is a subgroup contained within two of the largest direct factors of G_d. An example in Section 4 shows that there exists a $(8, 4, 2)$ BS on each of the groups $Z_4^2 \times Z_2$, $Z_4 \times Z_2^3$ and Z_2^5 relative to Z_2^2 contained within two of the largest direct factors of the group. For $d \geq 2$, let $Q \cong Z_2^4$ be a subgroup of G_d containing $H_0 = U_d$. For each subgroup $H_i \neq H_0$ of G_d corresponding to a hyperplane, Lemma 4.4 shows that G_d/H_i is a group of order 2^{2d+1} and exponent at most 4 and $Q/H_i \cong Z_2^2$ is contained in two of the largest direct factors of G_d/H_i.

For (iii), put $p = r = 2$, $a = 16$ and $t = 4$, and take $\mathcal{K}_d$ to be the set of all ordered pairs (G_d, U_d) included in the statement of the theorem (so that $(Z_4^3, U_1) \notin \mathcal{K}_1$). An example in Section 4 shows that there exists a $(16, 8, 4)$ BS on each of the groups $Z_4^2 \times Z_2^2$, $Z_4 \times Z_2^4$

on G/U) to produce a final difference set (based on the covering EBS on G). We now examine the parameters u, a, m, t and h of Theorem 3.2 in more detail. By assumption G is a p-group of order u^2am, so u and m are powers of the prime p. Let $u = p^r$, and write $m = p^{(d-1)r+\alpha}$ for some $d \geq 1$ and $0 \leq \alpha < r$. The assumption $um = at$ of Theorem 3.2 can then be written as $at = p^{dr+\alpha}$, and the parameter relationship $ah(u-1) = mu \mp (u-2)$ following the Theorem can be written as $ah = \frac{p^{dr+\alpha} \pm 1}{p^r - 1} \mp 1$. The last equality implies that $p^r - 1$ divides $p^{dr+\alpha} \pm 1 = (p^r - 1)(p^{(d-1)r+\alpha} + p^{(d-2)r+\alpha} + \ldots + p^\alpha) + p^\alpha \pm 1$, and so $p^r - 1$ divides $p^\alpha \pm 1$ for some α satisfying $0 \leq \alpha < r$. This condition only holds in three cases: with the lower sign and $\alpha = 0$; with the upper sign and $\alpha = 0$, $p = 3$ and $r = 1$; and with the upper sign and $\alpha = 1$, $p = 2$ and $r = 2$. In each case the values of u, m, at and ah fix the parameters of the initial and final difference set.

In the first case, with the lower sign and $\alpha = 0$, we have $u = p^r$, $m = p^{(d-1)r}$, $at = p^{dr}$ and $ah = \frac{p^{dr}-1}{p^r-1} + 1$. Theorem 2.4 then gives the parameters of both difference sets as being from the McFarland family, the initial with the values $q = p^r$ and $d - 1$ and the final with the values $q = p^r$ and d. The special case $p^r = 2$ corresponds to Hadamard parameters, the initial and final difference sets having the values $N = 2^{d-1}$ and $N = 2^d$. We return to this special case in Section 6, where we shall in addition make use of BSs which are not defined on p-groups.

In the second case, with the upper sign and $\alpha = 0$, $p = 3$ and $r = 1$, we have $u = 3$, $m = 3^{d-1}$, $at = 3^d$ and $ah = \frac{3^d-1}{2}$. Theorem 2.4 gives the parameters of both difference sets as being from the Spence family, the initial with the value $d - 1$ and the final with the value d.

In the third case, with the upper sign and $\alpha = 1$, $p = 2$ and $r = 2$, we have $u = 4$, $m = 2^{2d-1}$, $at = 2^{2d+1}$ and $ah = 2(\frac{2^{2d}-1}{3})$. Theorem 2.4 gives the parameters of both difference sets as being from the new family (4), the initial with the value $d - 1$ and the final with the value d.

The above argument determines the parameter family for the initial and final difference sets in each of the three cases. Since the application of Theorem 3.2 increases the value d by 1 without changing the associated difference set parameter family, it is natural to apply the construction recursively using Theorem 3.3. The above analysis almost completely determines the required parameter values for the covering EBSs and BSs, by comparison of the equations for ah and at.

In the first case we have $ah = \frac{p^{dr}-1}{p^r-1} + 1 = p^{(d-1)r} + p^{(d-2)r} + \ldots + p^r + 2$ and $at = p^{dr}$. The only solutions are $a = 1$ or, in the case $p = 2$, $a = 2$. The solution $a = 1$ requires a (p^{dr}, p^{dr}, p^{dr}) BS on a group of order $p^{(d+1)r}$ relative to a subgroup of order p^r and the solution $a = 2$ requires a $(2^{dr+1}, 2^{dr}, 2^{dr-1})$ BS on a group of order $2^{(d+1)r+1}$ relative to a subgroup of order 2^r. To begin the recursion with the smallest value $d = 1$ we require a $(1, 1, 2, -)$ covering EBS on a group of order p^r and a $(2, 1, 1, -)$ covering EBS on a group of order 2^{r+1} respectively.

Similarly, in the second case we require a $(3^d, 3^d, 3^d)$ BS on a group of order 3^{d+1} relative to a subgroup of order 3 and, to begin the recursion with $d = 1$, a $(1, 1, 1, +)$ covering EBS on a group of order 3.

Likewise in the third case we have $a = 1$ or $a = 2$. When $a = 1$ we require a $(2^{2d+1}, 2^{2d+1}, 2^{2d+1})$ BS on a group of order 2^{2d+3} relative to a subgroup of order 4 and,

for exactly one j, by the definition of BS. If χ is principal on U, so that ϕ is principal on U/W, then $\chi(B_j) = 0$ for each j, by the definition of BS. This completes the proof. □

We shall defer until Section 7 a full examination of the consequences of Theorem 4.3 for constructing families of BSs. For now our goal is to obtain quickly and easily just the BSs required for the construction of difference sets using Theorems 2.4 and 3.3. In this spirit we now give a recursive application of Theorem 4.3 to large classes of groups, which will be generalised in Section 7. While it was not important in Theorem 3.3 to keep track of the subgroup U associated with the BS on the group G, here we specify ordered pairs (G, U) to assist in applying Theorem 4.3 recursively.

Theorem 4.6 *Let p be prime, let $r \geq 1$, and for each $d \geq 1$ let $\mathcal{K}_d$ be a set of ordered pairs (G_d, U_d), where G_d is a group of order $p^{dr}a$ containing a subgroup $U_d \cong Z_p^r$. Suppose that for each $(G_1, U_1) \in \mathcal{K}_1$ there exists a $(a, \sqrt{at}, t)$ BS on G_1 relative to U_1. Suppose also that, for each $d > 1$ and for each $(G_d, U_d) \in \mathcal{K}_d$, G_d contains a subgroup $Q \cong Z_p^{2r}$ and subgroups $H_0, H_1, \ldots H_{p^r}$ of order p^r (corresponding to hyperplanes when viewed as subgroups of Q), where $H_0 = U_d$ and where $\mathcal{K}_{d-1}$ contains an ordered pair isomorphic to $(G_d/H_i, Q/H_i)$ for each $H_i \neq H_0$. Then for each $d \geq 1$ and for each $(G_d, U_d) \in \mathcal{K}_d$ there exists a $(p^{(d-1)r}a, p^{(d-1)r}\sqrt{at}, p^{(d-1)r}t)$ BS on G_d relative to U_d.*

Proof: The proof is by induction on d. The case $d = 1$ is true by assumption. Assume the case $d - 1$ to be true and consider $H_i \neq H_0$. Since $\mathcal{K}_{d-1}$ contains an ordered pair isomorphic to $(G_d/H_i, Q/H_i)$, by the inductive hypothesis there exists a $(p^{(d-2)r}a, p^{(d-2)r}\sqrt{at}, p^{(d-2)r}t)$ BS on G_d/H_i relative to Q/H_i. It follows from Theorem 4.3 that the case d is true, completing the induction. □

In Section 5 we shall apply Theorem 4.6, usually taking $\mathcal{K}_d$ to be the set of all ordered pairs (G_d, U_d) for which G_d is a p-group of order $p^{dr}a$ with bounded exponent (independent of d), and for which $U_d \cong Z_p^r$ is contained in r of the largest direct factors of G_d. This will allow the construction of difference sets with parameters from the families (2), (3) and (4). In Section 6 we shall present a different recursive application of Theorem 4.3 for the construction of difference sets with parameters from the Hadamard family (1).

5 Application to difference sets

In this section we use the recursive construction of Theorem 4.6 to obtain families of BSs on p-groups, from which the recursive construction of Theorem 3.3 produces families of covering EBSs on p-groups. Using Theorem 2.4 we deduce the existence of difference sets with parameters from the McFarland family, the Spence family, and the new parameter family (4).

We firstly show that by restricting the BSs to be on p-groups, the resulting difference set parameters must belong to the Hadamard family (1), the McFarland family (2), the Spence family (3), or the new family (4). By Theorem 2.4, the construction of Theorem 3.2 can be viewed as using an initial difference set (based on the covering EBS

difference set in any group of order 1408 whose Sylow 2-subgroup has exponent at most 4. The above procedure indicates the recursive construction for McFarland difference sets which we shall present in Section 5.

As a further example, we show there exists a $(16, 8, 4)$ BS on each of the groups $Z_4^2 \times Z_2^2$, $Z_4 \times Z_2^4$ and Z_2^6 relative to a subgroup $U \cong Z_2^2$ contained within two of the largest direct factors of the group. We firstly consider the group $Z_4^2 \times Z_2^2$. Now Jungnickel [24] has shown that $\{1, x, y, x^3y^3\}$ is a $(4, 4, 4, 1)$ semi-regular RDS in $Z_4^2 = \langle x, y \mid x^4 = y^4 = 1\rangle$ relative to $\langle x^2, y^2\rangle \cong Z_2^2$. Since this is equivalent to a $(4, 2, 1)$ BS on Z_4^2 relative to Z_2^2, we obtain the required BS by Theorem 4.3 and Lemma 4.4. We cannot deal with the groups $Z_4 \times Z_2^3$ and Z_2^5 in the same way because this would require a $(4, 4, 4, 1)$ semi-regular RDS on $Z_4 \times Z_2^2$ or Z_2^4 relative to $U \cong Z_2^2$, which does not exist [20]. But from Corollary 4.2 there is a $(8, 8, 8)$ BS on Z_2^6 relative to Z_2^3. We show in the following lemma how this can be used to provide a $(8, 8, 8)$ BS on Z_2^5 relative to Z_2^2, which allows the required BS to be constructed using Lemma 2.1 with $s = 2$. An example in Section 3 then shows that there is a $(320, 88, 24, 64)$-difference set in $Z_4^2 \times Z_2^2 \times Z_5$, $Z_4 \times Z_2^4 \times Z_5$ and $Z_2^6 \times Z_5$. Although the group $Z_4^3 \times Z_5$ has order 320 and exponent 4 it is excluded from this result because Z_4^3 does not contain a subgroup $Q \cong Z_2^4$ and so Theorem 4.3 cannot be applied. In Section 5 we present a recursive construction for difference sets with parameters (4) based on these initial examples, and show that the exceptional case $Z_4^3 \times Z_5$ does not propagate to larger groups under this construction.

We now describe the method of "contraction" of BSs required in the preceding example, modelled on that given by Elliott and Butson [17] for RDSs.

Lemma 4.5 *Suppose there exists a $(a, \sqrt{at}, t)$ BS on a group G relative to a subgroup U. Let W be a subgroup of U. Then there exists a $(a, \sqrt{at}, t)$ BS on G/W relative to U/W.*

Proof: Let $\{B_1, B_2 \ldots, B_t\}$ be a $(a, \sqrt{at}, t)$ BS on G relative to U. Let $B_j' = \{gU \in G/U \mid g \in B_j\}$ be the image of B_j under the quotient mapping from G to G/U and let $B_j'' = \{gW \in G/W \mid g \in B_j\}$ be the image of B_j under the quotient mapping from G to G/W.

We show firstly that for each j, $B_j' = G/U$ in the group ring $Z[G/U]$. Every nonprincipal character ψ of G/U can be regarded as being induced by a character χ that is nonprincipal on G and principal on U, so that $\psi(B_j') = \chi(B_j) = 0$ by the definition of BS. Therefore $B_j' = c\,G/U$ in $Z[G/U]$ for some integer c. Now $|B_j| = a$ by the definition of BS, and $|G|/|U| = a$ from the relationship between BS parameters given after Theorem 2.2, so that $c = 1$.

We next show that for each j, B_j'' contains no repeated elements. Since $B_j' = G/U$ in $Z[G/U]$, each coset of U in G contains exactly one element of B_j. It follows that each coset of W in G contains at most one element of B_j.

Finally we show that $\{B_1'', B_2'' \ldots, B_t''\}$ is a $(a, \sqrt{at}, t)$ BS on G/W relative to U/W. For each j, we have shown that B_j'' is a subset of G/W comprising a elements. Every nonprincipal character ϕ of G/W can be regarded as being induced by a character χ that is nonprincipal on G and principal on W, so that $\phi(B_j'') = \chi(B_j)$. If χ is nonprincipal on U, so that ϕ is nonprincipal on U/W, then $\chi(B_j)$ is nonzero (having modulus $\sqrt{at}$)

H_0 do not necessarily correspond to the direct factors of G/H_i containing Q/H_i.

Clearly we require some information about the form of G/H_i and Q/H_i in order to apply Theorem 4.3 effectively. We now show that by appropriate choice of generators, exactly r direct factors of G retain the same exponent in G/H_i (these are the direct factors which contain Q/H_i) and r are reduced by a factor of p.

Lemma 4.4 *Let G be the group $\prod_{u=1}^{2r} Z_{p^{1+\alpha_u}}$ containing a subgroup $Q \cong Z_p^{2r}$, 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 $G/H_i \cong \prod_{u \notin S} Z_{p^{1+\alpha_u}} \times \prod_{u \in S} Z_{p^{\alpha_u}}$. Moreover, for each H_i a suitable choice of generators of G ensures that $Q/H_i \cong Z_p^r$ is contained in the first r direct factors of G/H_i as specified. Furthermore if H_0 is contained in a subgroup of G isomorphic to $Z_{p^2}^r$ then, for each $H_i \neq H_0$, Q/H_i is contained in a subgroup of G/H_i isomorphic to $Z_{p^2}^r$.*

Proof: Each H_i is a subgroup of Q of order p^r and so $H_i \cong Z_p^r$. Therefore we can choose generators of G such that H_i is contained in r direct factors of G. Let $\{x_u \mid 1 \leq u \leq 2r\}$ be the generators of G, where $x_u^{p^{1+\alpha_u}} = 1$ for all u, and let S be the r-element subset of $\{1, 2, \ldots, 2r\}$ which indexes the r direct factors containing H_i. Then $H_i = \langle x_u^{p^{\alpha_u}} \mid u \in S \rangle$, and the order of $x_u H_i$ in G/H_i is $p^{1+\alpha_u}$ for $u \notin S$ and p^{α_u} for $u \in S$. Therefore $G/H_i = \langle x_u H_i \mid 1 \leq u \leq 2r \rangle \cong \prod_{u \notin S} Z_{p^{1+\alpha_u}} \times \prod_{u \in S} Z_{p^{\alpha_u}}$ as required. With this choice of generators, $Q/H_i = \langle x_u^{p^{\alpha_u}} H_i \mid 1 \leq u \leq 2r \rangle = \langle x_u^{p^{\alpha_u}} H_i \mid u \notin S \rangle$, and so $Q/H_i \cong Z_p^r$ and Q/H_i is contained in the first r direct factors of G/H_i as specified.

Suppose now that H_0 is contained in a subgroup of G isomorphic to $Z_{p^2}^r$. Since H_0 is isomorphic to Z_p^r this is equivalent to the statement that each $h_0 \in H_0$ can be written as $h_0 = g^p$ for some $g \in G$. For any $H_i \neq H_0$ let qH_i be an element of Q/H_i. The proof of Lemma 4.1 shows that $Q = H_0 H_i$ and so $q = h_0 h_i$ for some $h_0 \in H_0$ and some $h_i \in H_i$. Since $h_0 = g^p$ for some $g \in G$ we obtain $qH_i = g^p h_i H_i = g^p H_i = (gH_i)^p$, and so $Q/H_i \cong Z_p^r$ is contained in a subgroup of G/H_i isomorphic to $Z_{p^2}^r$. □

For example, we can now construct the BSs whose existence we assumed in Section 3. We firstly show there exists a $(8, 4, 2)$ BS on each of the groups $Z_4^2 \times Z_2$, $Z_4 \times Z_2^3$ and Z_2^5 relative to a subgroup $U \cong Z_2^2$ contained within two of the largest direct factors of the group. The group $Z_4^2 \times Z_2$ is dealt with by the example in Section 2. For the other two groups, by Corollary 4.2 there is a $(4, 4, 4)$ BS on Z_2^4 relative to Z_2^2, from which the desired BS can be obtained using Lemma 2.1 with $s = 2$. An example in Section 3 then shows that there is a $(96, 20, 4, 16)$ McFarland difference set in any group of order 96 whose Sylow 2-subgroup has exponent at most 4.

Next we show there exists a $(32, 16, 8)$ BS on any group G of order 128 and exponent at most 4 relative to a subgroup $U \cong Z_2^2$ contained within two of the largest direct factors of G. Let $Q \cong Z_2^4$ be a subgroup of G containing $H_0 = U$. By Lemma 4.4, for each $H_i \neq H_0$, we find G/H_i has order 32 and exponent at most 4 and $Q/H_i \cong Z_2^2$ is contained in two of the largest direct factors of G/H_i. By the preceding example there is a $(8, 4, 2)$ BS on G/H_i relative to Q/H_i and so by Theorem 4.3 we obtain the desired BS on G. An example in Section 3 then shows that there is a $(1408, 336, 80, 256)$ McFarland

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 4.3 describes a procedure for constructing the BS explicitly. Given a 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 $B_{ij} = \{g \in G \mid gH_i \in B'_{ij}\}$. This produces the $p^r t$ building blocks of a $(p^r a, p^r\sqrt{at}, p^r t)$ BS on G relative to H_0.

To illustrate this procedure in detail, suppose we wish to construct a $(32, 16, 8)$ BS on $G = Z_4^3 \times Z_2 = \langle x, y, z, w \mid x^4 = y^4 = z^4 = w^2 = 1\rangle$ relative to $H_0 = \langle x^2, y^2\rangle \cong Z_2^2$. We firstly choose the subgroup $Q \cong Z_2^4$ 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 GF(4). Since $x^2 + x + 1$ is an irreducible polynomial of degree 2 over GF(2) we can regard GF(4) as having multiplicative generator δ, where $\delta^2 = \delta + 1$. Then the hyperplanes of GF(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 the isomorphism from GF(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 $G/H_i \cong Z_4^2 \times Z_2$, and $Q/H_i \cong Z_2^2$ is contained within Z_4^2, for each $i \neq 0$. We therefore require a $(8, 4, 2)$ BS on $\langle a, b, c \mid a^4 = b^4 = c^2\rangle$ relative to $\langle a^2, b^2\rangle$. An example of such a BS was given in Section 2, comprising 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 $G/H_1 = \langle xH_1, yH_1, zH_1\rangle$, $G/H_2 = \langle xH_2, yH_2, xzH_2\rangle$, $G/H_3 = \langle xH_3, yH_3, yzH_3\rangle$ and $G/H_4 = \langle xH_4, yH_4, xyzH_4\rangle$, 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, $B'_{21} = H_2 + xH_2 + x^2zH_2 + x^3zH_2 + x^3yzH_2 + xyH_2 + x^2y^3zH_2 + y^3H_2$. Each of the expressions B'_{ij} is a group ring element in $Z[G/H_i]$ comprising 8 elements of the quotient group G/H_i. We finally obtain $B_{ij} = \{g \in G \mid gH_i \in B'_{ij}\}$ by regarding the formal expression for B'_{ij} as a group ring element in $Z[G]$ comprising 32 elements of G. The 8 building blocks $\{B_{ij} \mid 1 \leq i \leq 4,\ 1 \leq j \leq 2\}$ then form a $(32, 16, 8)$ BS on G relative to H_0.

In general the quotient groups G/H_i for $i \neq 0$ need not be isomorphic. For example, let $G = Z_2 \times Z_4 = \langle x, y \mid x^2 = y^4 = 1\rangle$. The subgroups of G corresponding to hyperplanes are $H_0 = \langle x\rangle$, $H_1 = \langle y^2\rangle$ and $H_2 = \langle xy^2\rangle$, so the quotient groups $G/H_1 \cong Z_2^2$ and $G/H_2 \cong Z_4$ are not isomorphic. (Since there exists a $(2, 2, 2)$ BS on Z_2^2 relative to Z_2 but not on Z_4 relative to Z_2, we cannot use Theorem 4.3 to construct a $(4, 4, 4)$ BS on G relative to H_0.) This example also demonstrates (for $i = 2$) that the direct factors of G containing

We now show how to exploit the hyperplane structure of Lemma 4.1 to obtain a more general result than Corollary 4.2. Take a group G containing a subgroup Q isomorphic to Z_p^{2r} and consider those subgroups H_i of G which correspond to hyperplanes when viewed as subgroups of Q. We 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 (in a similar manner to the lifting of a covering EBS in Lemma 3.1) to collectively form a BS on G relative to H_0.

Theorem 4.3 *Let G be a group of order $p^{2r}a$ containing a subgroup $Q \cong Z_p^{2r}$, where p is prime. 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 $(a, \sqrt{at}, t)$ BS on G/H_i relative to Q/H_i for each $i = 1, 2, \ldots, p^r$. Then there exists a $(p^r a, p^r\sqrt{at}, p^r t)$ BS on G relative to H_0.*

Proof: For each $i \geq 1$, let $\{B'_{i1}, B'_{i2}, \ldots, B'_{it}\}$ be a $(a, \sqrt{at}, t)$ BS on G/H_i relative to Q/H_i. Following the proof of Lemma 3.1, for each $i \geq 1$ and for each j let $B_{ij} = \{g \in G \mid gH_i \in B'_{ij}\}$. Since B_{ij} is the union of $|B'_{ij}| = a$ distinct cosets of H_i, $|B_{ij}| = p^r a$ and for every nonprincipal character χ of G and for each $i \geq 1$ and for each j

$$\chi(B_{ij}) = \begin{cases} 0 & \text{if } \chi \text{ nonprincipal on } H_i \\ p^r \psi(B'_{ij}) & \text{if } \chi \text{ principal on } H_i, \end{cases} \tag{5}$$

where $\psi(B'_{ij})$ is the induced nonprincipal character on G/H_i. By the definition of BS, for each $i \geq 1$, $\psi(B'_{ij})$ is nonzero (having modulus $\sqrt{at}$) for exactly one value of j if ψ is nonprincipal on Q/H_i, and is nonzero for no value of j if ψ is principal on Q/H_i.

We claim that $\{B_{ij} \mid 1 \leq i \leq p^r, 1 \leq j \leq t\}$, comprising $p^r t$ subsets B_{ij} of G, is a $(p^r a, p^r\sqrt{at}, p^r t)$ BS on G relative to H_0. To establish this, let χ be a nonprincipal character of G. Lemma 4.1 implies that if χ is nonprincipal on Q then it is principal on one of the subgroups H_i and nonprincipal on all the others. We therefore distinguish three cases: χ is principal on H_I for some $I \neq 0$ and nonprincipal on H_i for each $i \neq I$; χ is principal on H_0 and nonprincipal on H_i for each $i \neq 0$; and χ is principal on Q and nonprincipal on G.

In the first case, where χ is principal on H_I for some $I \neq 0$ and nonprincipal on H_i for each $i \neq I$, $\chi(B_{ij}) = 0$ for each $i \neq I$ and $\chi(B_{Ij}) = p^r \psi(B'_{Ij})$, from (5). Since χ is nonprincipal on Q, ψ is nonprincipal on Q/H_I and so $\psi(B'_{Ij})$ is nonzero (having modulus $\sqrt{at}$) for exactly one value of j. Therefore $\chi(B_{ij})$ is nonzero (having modulus $p^r\sqrt{at}$) for exactly one ordered pair (i, j). In the second case, where χ is principal on H_0 and nonprincipal on H_i for each $i \neq 0$, $\chi(B_{ij}) = 0$ for each ordered pair (i, j), from (5). In the third case, where χ is principal on Q and nonprincipal on G, 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 (5). 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 $H_0 \cong Z_p^r$ on which we wish to construct a BS using Theorem 4.3, we are free to choose Q to be any subgroup of G isomorphic to Z_p^{2r}

The construction depends on a vector space P of dimension 2 over GF(p^r). Let δ be a multiplicative generator of GF(p^r). We can write the additive group of GF(p^r) as $\langle \delta^i \mid 0 \leq i \leq r-1 \rangle$ and so P is an additive group which can be written as $\langle (\delta^i, 0), (0, \delta^j) \mid 0 \leq i, j \leq r-1 \rangle$. We construct an isomorphism from P to $Z_p^{2r} = \langle x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_r \rangle$ by $(\delta^i, 0) \mapsto x_{i+1}$ and $(0, \delta^j) \mapsto y_{j+1}$. The subspaces of P of dimension 1 (the hyperplanes) $H_0, H_1, \ldots, H_{p^r}$ each contain p^r elements and have as their bases $\{(1,0)\}, \{(0,1)\}, \{(1,1)\}, \{(\delta,1)\}, \{(\delta^2,1)\}, \{(\delta^3,1)\}, \ldots, \{(\delta^{p^r-2},1)\}$.

Lemma 4.1 *Let P be a vector space of dimension 2 over GF(p^r), where p is prime. Any nonprincipal character of P is principal on exactly one of the hyperplanes of P.*

Proof: We show firstly that the kernels of the nonprincipal characters χ of P are precisely the subgroups of P of order p^{2r-1}. Since χ is a homomorphism from P onto the p^{th} roots of unity, $|\text{Ker}(\chi)| = |P|/p = p^{2r-1}$ and so Ker(χ) is a subgroup of P of order p^{2r-1}. Furthermore any subgroup of P of order p^{2r-1} is the kernel of some nonprincipal character of P.

We next show that a subgroup of P of order p^{2r-1} contains at most one hyperplane. P is a vector space of dimension 2 over GF(p^r) and each hyperplane is a subspace of dimension 1. Hence two distinct hyperplanes intersect in a subspace of dimension 0: the identity element. Therefore the product of two distinct hyperplanes is the whole of P, so a subgroup of order p^{2r-1} cannot contain two distinct hyperplanes.

Finally we use a counting argument to show that a subgroup of P of order p^{2r-1} contains exactly one hyperplane. Let H_i be a hyperplane for some $i = 0, 1, \ldots, p^r$. Since $P \cong Z_p^{2r}$ we have $P/H_i \cong Z_p^r$. Therefore P/H_i contains $(p^r-1)/(p-1)$ subgroups of order p^{r-1}. Each such subgroup of P/H_i is associated with a subgroup of P of order p^{2r-1} containing H_i, using the quotient mapping from P to P/H_i. Therefore there are at least $(p^r-1)/(p-1)$ distinct subgroups of P of order p^{2r-1} containing H_i. Since i can take p^r+1 values, there are at least $(p^r+1)(p^r-1)/(p-1) = (p^{2r}-1)/(p-1)$ distinct subgroups of P of order p^{2r-1} containing some hyperplane (since we have already shown that the subgroups of P arising from different values of i must be distinct). But the total number of subgroups of P of order p^{2r-1} is $(p^{2r}-1)/(p-1)$ and so every subgroup of P of order p^{2r-1} contains exactly one hyperplane.

We have now shown that for any nonprincipal character χ of P, Ker(χ) contains exactly one hyperplane of P. This completes the proof. □

Lemma 4.1 implies the following result, due to Davis [8], which was discussed when introducing building sets in Section 2.

Corollary 4.2 *There exists a (p^r, p^r, p^r) BS on Z_p^{2r} relative to Z_p^r, where p is prime and $r \geq 1$.*

Proof: Let $H_0, H_1, \ldots, H_{p^r}$ be the subgroups of Z_p^{2r} of order p^r corresponding to hyperplanes of P under the isomorphism from Z_p^{2r} to P. Label the subgroups so that $H_0 = Z_p^r$. Then Lemma 4.1 implies that $\{H_1, H_2, \ldots, H_{p^r}\}$ is a (p^r, p^r, p^r) BS on Z_p^{2r} relative to Z_p^r. □

As a further example, we show that the covering EBS on G/U can comprise more than one building block. Take G to be any group of order 128 and exponent at most 4, and let $U \cong Z_2^2$ be a subgroup of G such that G/U is isomorphic to $Z_4 \times Z_2^3$ or Z_2^5. From the first example above, there is a $(8,4,3,-)$ covering EBS on G/U. Assume we can find a $(32,16,8)$ BS on G relative to U. Then there exists a $(32,16,11,-)$ covering EBS on G and therefore a $(1408,336,80,256)$-difference set in $G \times Z_{11}$. These difference set parameters belong to the McFarland family with $q = 4$ and $d = 2$, for which the only abelian groups previously known to contain difference sets were $Z_2^7 \times Z_{11}$ [37] and $Z_4 \times Z_2^5 \times Z_{11}$ [16].

We shall show in Section 4 how to construct the BSs whose existence was assumed in the above examples. Following the pattern indicated by the examples, we now apply Theorem 3.2 recursively to large classes of groups, assuming for now that the required BSs are available.

Theorem 3.3 *Let p be prime, let $r \geq 1$, and for each $d \geq 0$ let $\mathcal{G}_d$ be a set of groups of order $p^{(d+1)r}am$. Suppose there exists a $(am, m, h, \pm)$ covering EBS on each $G_0 \in \mathcal{G}_0$. Suppose also that, for each $d \geq 1$, there exists a $(p^{(d-1)r}a^2t, p^{(d-1)r}at, p^{(d-1)r}t)$ BS on each $G_d \in \mathcal{G}_d$ relative to a subgroup U_d (depending on G_d) of order p^r, where $p^rm = at$ and where $\mathcal{G}_{d-1}$ contains a group isomorphic to G_d/U_d. Then for each $d \geq 0$ there exists a $(p^{dr}am, p^{dr}m, h + \frac{p^{dr}-1}{p^r-1}t, \pm)$ covering EBS on each $G_d \in \mathcal{G}_d$.*

Proof: The proof is by induction on d. The case $d = 0$ is true by assumption. Assume the case $d-1$ to be true. For each $G_d \in \mathcal{G}_d$, by assumption there exists a $(p^{(d-1)r}a^2t, p^{(d-1)r}at, p^{(d-1)r}t)$ BS on G_d relative to a subgroup U_d. Since $\mathcal{G}_{d-1}$ contains a group isomorphic to G_d/U_d (of order $p^{dr}am$), by the inductive hypothesis there exists a $(p^{(d-1)r}am, p^{(d-1)r}m, h + \frac{p^{(d-1)r}-1}{p^r-1}t, \pm)$ covering EBS on G_d/U_d. It follows from Theorem 3.2 that the case d is true, completing the induction. □

When applying the recursive construction for covering EBSs of Theorem 3.3 we shall usually take $\mathcal{G}_d$ to be the set of all p-groups of order $p^{(d+1)r}am$ with bounded exponent (independent of d). The condition that $\mathcal{G}_{d-1}$ contains a group isomorphic to G_d/U_d will then automatically be satisfied. In order to apply this theorem we require suitable families of BSs. We shall show how to obtain these in Section 4 by means of a second recursive construction. In Section 5 we shall deduce the existence of families of covering EBSs which, by Theorem 2.4, implies the existence of families of difference sets. In Section 6 we shall use a similar procedure to construct difference sets with parameters from the Hadamard family (1), applying Theorem 3.2 directly instead of Theorem 3.3.

4 Recursive construction of building sets

In this section we give a recursive construction for BSs relative to an elementary abelian subgroup. This will be used to provide the families of BSs needed for both the construction of difference sets in Sections 5 and 6 and for the construction of semi-regular RDSs in Section 8.

$B_j = \{g \in G \mid gU \in B'_j\}$ 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 nonprincipal character χ of G

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

where ψ is the induced nonprincipal character 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. □

We can now construct a covering EBS on G from two ingredients: a covering EBS on G/U (a special form of difference set) and a BS on G relative to U (a special form of semi-regular RDS). The following theorem is the key construction of the paper.

Theorem 3.2 *Let G be a group of order u^2am containing a subgroup U of order u. Suppose there exists a $(am, m, h, \pm)$ covering EBS on G/U and there exists a (a^2t, at, t) BS on G relative to U, where $um = at$. Then there exists a $(uam, um, h+t, \pm)$ covering EBS on G.*

Proof: By Lemma 3.1 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. By assumption there exists a (a^2t, at, t) BS, say $\{B_{h+1}, B_{h+2}, \ldots, B_{h+t}\}$, on G relative to U. Since $um = at$ the parameters of the BS can be written as (uam, um, t). By the definitions of EBS and BS, this implies that $\{B_1, B_2, \ldots, B_{h+t}\}$ is a $(uam, um, h+t, \pm)$ covering EBS on G. □

By applying the relationship between covering EBS parameters given after Theorem 2.4 to G/U, we find the parameters of Theorem 3.2 are constrained by $am(amh \pm 2m) = (amh \pm m - m^2)|G/U|$, which reduces to $ah(u-1) = mu \mp (u-2)$.

For example, let G be the group $Z_4^2 \times Z_2$, $Z_4 \times Z_2^3$, or Z_2^5. In each case G contains a subgroup $U \cong Z_2^2$ such that $G/U \cong Z_2^3$. Now there exists a trivial $(2, 1, 1, -)$ covering EBS $\{B'_1\}$ on Z_2^3, comprising just the identity element. Following the proof of Lemma 3.1, set $B_1 = \{g \in G \mid gU \in B'_1\} = U$. Assume we can find a $(8, 4, 2)$ BS $\{B_2, B_3\}$ on G relative to U. (Section 2 contains an example of such a BS for the case $G = Z_4^2 \times Z_2$.) Then by Theorem 3.2, $\{B_1, B_2, B_3\}$ is a $(8, 4, 3, -)$ covering EBS on G and by Theorem 2.4 there exists a $(96, 20, 4, 16)$-difference set in $G \times Z_3$.

In the above example B_1 is a subgroup of G, but this need not be the case. Take G to be the group $Z_4^2 \times Z_2^2$, $Z_4 \times Z_2^4$, or Z_2^6 and let $U \cong Z_2^2$ be a subgroup of G such that $G/U \cong Z_2^4$. Now we have seen in Section 1 that Z_2^4 contains a $(16, 6, 2, 4)$-difference set, which can be viewed as a $(4, 2, 1, +)$ covering EBS $\{B'_1\}$ on Z_2^4. Again set $B_1 = \{g \in G \mid gU \in B'_1\}$, which is not a subgroup of G. Assume we can find a $(16, 8, 4)$ BS $\{B_2, B_3, B_4, B_5\}$ on G relative to U. Then by Theorem 3.2, $\{B_1, B_2, B_3, B_4, B_5\}$ is a $(16, 8, 5, +)$ covering EBS on G and by Theorem 2.4 there exists a $(320, 88, 24, 64)$-difference set in $G \times Z_5$. These difference set parameters belong to the new family (4) with $d = 1$, for which no examples of difference sets were previously known.

$(32, 16, 11, -)$ covering EBSs on groups of order 128, which by Theorem 2.4 produce difference sets with parameters $(320, 88, 24, 64)$ and $(1408, 336, 80, 256)$ respectively. In Sections 5 and 6 we apply the recursive constructions and use Theorem 2.4 to provide a unifying framework for difference sets in the McFarland, Spence and Hadamard parameter families as well as the new parameter family (4). Section 5 deals with BSs on p-groups only, whereas Section 6 uses BSs on groups whose order need not be a prime power. In Section 7 we show that the construction of Section 4 is sufficiently strong to provide many further existence results for families of BSs. From Theorem 2.2 we deduce the existence of several families of semi-regular RDSs in Section 8 and provide a unifying framework for many previously known results on RDSs. We conclude in Section 9 with a selection of open problems and a discussion of how the definitions and constructions of this paper might be generalised to deal with nonabelian groups.

3 Recursive construction of extended building sets

In this section we give a recursive construction for covering EBSs. By Theorem 2.4, this central result implies a recursive construction for difference sets, which is the unifying construction of the title of the paper.

We shall construct a covering EBS on a group G as the multiset union of two collections of building blocks. The first collection will be a $(uam, um, h, \pm)$ EBS on G with respect to a subgroup U of order u. By the definition of EBS, the nonprincipal characters of G giving a nonzero character sum on these building blocks are precisely those which are principal on U. The second collection will be a (uam, um, t) BS on G relative to U, where $um = at$ (so the BS parameters can equivalently be written as (a^2t, at, t).) By the definition of BS, the nonprincipal characters of G giving a nonzero character sum on these building blocks are precisely those which are nonprincipal on U. Moreover, since each building block of a BS or EBS has nonzero character sum for at most one nonprincipal character, the multiset union of these two collections will be a $(uam, um, h + t, \pm)$ covering EBS on G. In this way we shall combine the favourable properties of the two collections of blocks without introducing unwanted interactions between them.

We can fix $|G| = u^2am$ from the relationship between BS parameters given after Theorem 2.2. By Theorem 2.2, the second collection of building blocks can be viewed as a special form of $(u^2m^2, u, u^2m^2, u^2m)$ semi-regular RDS relative to U in a group having G as a subgroup of index t. To form the first collection of building blocks we begin with a covering $(am, m, h, \pm)$ EBS on the quotient group G/U, which by Theorem 2.4 can be viewed as a special form of $(uamh, m(ah \pm 1), m(ah \pm 1 - m), m^2)$-difference set in a group having G/U as a subgroup of index h. We now show how to take u copies of this covering EBS on G/U to produce a EBS on G with respect to U, as required for the first collection of building blocks.

Lemma 3.1 *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 a $(uam, um, h, \pm)$ EBS on G with respect to U.*

Proof: Let $\{B'_1, B'_2, \ldots, B'_h\}$ be a $(am, m, h, \pm)$ covering EBS on G/U. For each j let

Combining these two cases, $\{D_1, D_2, \ldots, D_{h/s}\}$ is a $(as, m, h/s, \pm)$ covering EBS on G'. $\Box$

Theorem 2.4 *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.*

Proof: Apply Lemma 2.3 with $s = h$ to obtain a $(ah, m, 1, \pm)$ covering EBS on G'. This is equivalent to a $(h|G|, ah \pm m, ah \pm m - m^2, m^2)$-difference set in G'. $\Box$

For example, the hyperplane construction of McFarland [37] and Dillon [16] discussed at the beginning of this section can be interpreted as a $(q^d, q^d, h+1, -)$ covering EBS $\{\phi, H_0, H_1, \ldots, H_{h-1}\}$ on the elementary abelian group G of order q^{d+1}, where $h = \frac{q^{d+1}-1}{q-1}$. By Theorem 2.4, this implies the existence of a McFarland difference set in any group G' containing G as a subgroup of index $h+1$.

We have already given an example of a $(8,4,2)$ BS $\{B_1, B_2\}$ on $Z_4^2 \times Z_2 = \langle x, y, z \mid x^4 = y^4 = z^2 = 1\rangle$ relative to $\langle x^2, y^2\rangle \cong Z_2^2$, due to Arasu and Sehgal [3]. If we define a third building block $B_3 = \langle x^2, y^2\rangle$ then $\{B_1, B_2, B_3\}$ is a $(8,4,3,-)$ covering EBS and then by Theorem 2.4 there exists a $(96, 20, 4, 16)$-difference set in $Z_4^2 \times Z_2 \times Z_3$. The main purpose of [3] was to demonstrate the existence of such a difference set, but the embedded $(8,4,2)$ BS will be of great use in the construction of families of difference sets and semi-regular RDSs in later sections.

We now derive some constraints on the parameters a, m, h and $|G|$ of a $(a, m, h, \pm)$ covering EBS on a group G. The relationship between difference set parameters (v, k, λ, n) can be written as $k^2 - n = \lambda v$, so from Theorem 2.4 we find $a(ah \pm 2m) = (ah \pm m - m^2)|G|$. Provided $\lambda = ah \pm m - m^2 > 0$, this implies that $ah \pm m - m^2$ divides $a(ah \pm 2m)$. (The exceptional case $\lambda = 0$ corresponds to $k = 1$, namely a trivial $(0, 1, h, +)$ or $(2, 1, 1, -)$ or $(1, 1, 2, -)$ covering EBS on G.) Let the covering EBS be $\{B_1, B_2, \ldots, B_h\}$ and let B_1 be the building block containing $a \pm m$ elements. By the same argument as previously used for a BS, $\sum_{\chi \in G^*} |\chi(B_i)|^2 = |B_i| \cdot |G|$. Therefore if w_i is the number of nonprincipal characters of G giving a nonzero character sum over B_i then $a^2 + m^2 w_i = a|G|$ for all $i > 1$ and $(a \pm m)^2 + m^2 w_1 = (a \pm m)|G|$, so that $w_i = a(|G| - a)/m^2$ for all $i > 1$ and $w_1 = a(|G| - a)/m^2 - 1 \pm (|G| - 2a)/m$. It follows that, for $h > 1$, m divides $|G|$ and $m \mid a$.

Notice that we can construct a difference set or RDS by fixing one building block at a time. The character properties of the building blocks already fixed do not change as further building blocks are determined. This is an important advantage over the binary array viewpoint, in which we must consider the cross-correlation of a new array with each of those previously fixed.

The remainder of the paper is concerned with describing and applying constructions for covering EBSs and BSs. In Section 3 we give a recursive construction for covering EBSs which assumes the existence of certain families of BSs. These families are provided by a recursive construction for BSs presented in Section 4. We shall illustrate the constructions of Sections 3 and 4 by reference to $(16, 8, 5, +)$ covering EBSs on groups of order 64 and

$u \mid at$ for $at > 1$ (which derives from the condition that λ be integer in Lemma 1.1 (ii)). Theorem 2.2, together with the trivial case $at = 1$, also implies that $|G| = ua$. Furthermore we can show that $t \mid a(u-1)$, as we now outline. Let G^* be the group of characters of G. For any building block B_i, $\sum_{\chi \in G^*} |\chi(B_i)|^2 = \sum_{\chi \in G^*} \sum_{g_1 \in B_i} \sum_{g_2 \in B_i} \chi(g_1)\overline{\chi(g_2)} = \sum_{\chi \in G^*} \sum_{g_1 \in B_i} \sum_{g_2 \in B_i} \chi(g_1 g_2^{-1}) = \sum_{g_1 \in B_i} \sum_{\chi \in G^*} \chi(1_G) = |B_i| \cdot |G|$. Therefore if w_i is the number of nonprincipal characters of G giving a nonzero character sum over B_i then $a^2 + atw_i = ua^2$, so that $w_i = a(u-1)/t$ for all i.

We have seen how to construct a semi-regular RDS from a BS. We now define a modification of a BS for the purpose of constructing difference sets in an analogous way. For integers $a \geq 0$, $m \geq 1$, and $h \geq 1$, we define a $(a, m, h, +)$ *extended building set (EBS) on a group G with respect to a subgroup U* to be 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 nonprincipal character χ of G

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

(ii) no building block has nonzero character sum if χ is nonprincipal 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 shall treat both cases simultaneously by referring to a $(a, m, h, \pm)$ EBS. Notice that the role of principal and nonprincipal characters on U is the reverse of that used in the definition of a BS. Notice also that for a EBS we must have m integer, because one building block contains $a \pm m$ elements, whereas for a BS m need not be integer. We call the EBS *covering* in the case $U = \{1\}$, when exactly one building block has nonzero character sum for every nonprincipal character of G. (The use of "covering" refers not to the intersection or union of the building blocks but to their character properties.) It follows immediately from Lemma 1.1 (i) that a $(a, m, 1, \pm)$ covering EBS on a group G is equivalent to a $(|G|, a \pm m, a \pm m - m^2, m^2)$-difference set in G.

We now 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. In particular we shall construct a difference set as a single building block on a group containing G. We shall exploit this result in Section 5 to deduce the existence of difference sets from covering EBSs.

Lemma 2.3 *Suppose there exists a $(a, m, h, \pm)$ covering EBS on a group G. Then there exists a $(as, m, h/s, \pm)$ covering EBS on G', where s divides h and G' is any group containing G as a subgroup of index s.*

Proof: The proof is modelled on that of Lemma 2.1. Let $\{B_1, B_2, \ldots, B_h\}$ be a $(a, m, h, \pm)$ covering EBS on G and let the building block containing $a \pm m$ elements be B_1. For each $j = 1, 2, \ldots, h/s$ let D_j be the subset $\cup_{i=1}^{s} g'_i B_{i+(j-1)s}$ of G', where $g'_1, g'_2, \ldots, g'_s \in G'$ are coset representatives of G in G'. If χ is a principal character of G and nonprincipal on G' (so $h > 1$) then $\chi(D_j) = \chi(g'_1)|B_{1+(j-1)s}| + \sum_{i=2}^{s} \chi(g'_i)|B_{i+(j-1)s}| = \chi(g'_1)(|B_{1+(j-1)s}| - a) + a\sum_{i=1}^{s} \chi(g'_i) = \chi(g'_1)(|B_{1+(j-1)s}| - a)$, because the induced character on G'/G is nonprincipal. Therefore $|\chi(D_j)|$ equals m for $j = 1$ and equals 0 for all $j > 1$. If χ is a nonprincipal character of G then by assumption $|\chi(B_{i+(j-1)s})|$ equals m for exactly one ordered pair (i, j) and equals 0 for all other ordered pairs (i, j). Therefore $|\chi(D_j)|$ equals m for exactly one value of j and equals 0 for all other values of j.

coset representatives of G in G'. Let χ be a nonprincipal 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: χ is principal on G and nonprincipal on G'; χ is principal on U and nonprincipal on G; and χ is nonprincipal on U. In the first case, when χ is principal on G and nonprincipal on G' (so $s > 1$), $\chi(B_{i+(j-1)s}) = |B_{i+(j-1)s}| = a$ 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 nonprincipal character on G'/G, and the induced character sum over this group is 0. In the second case, when χ is principal on U and nonprincipal 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. In the third case, when χ is nonprincipal on U, by assumption $|\chi(B_{i+(j-1)s})|$ equals $\sqrt{at}$ for exactly one ordered pair (i,j) (say (I,J)) and equals 0 for all other ordered pairs (i,j). Therefore $|\chi(R_J)| = |\chi(g'_I)||\chi(B_{I+(J-1)s})| = \sqrt{at}$ 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 $(as, \sqrt{at}, t/s)$ BS on G' relative to U. □

We next show that in the case $s = t$ of Lemma 2.1 we can obtain a semi-regular RDS in G' from a BS on G, and we shall exploit this result in Section 8 to deduce the existence of semi-regular RDSs from BSs.

Theorem 2.2 *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 2.1 with $s = t$ to obtain a $(at, \sqrt{at}, 1)$ BS on G' relative to U. For $at > 1$, this is equivalent to a $(at, u, at, at/u)$ semi-regular RDS in G' relative to U. □

For example, the hyperplane construction of Davis [8] and Pott [8] discussed at the beginning of this section can be interpreted as a $(q^d, q^d, h-1)$ BS $\{H_1, H_2, \ldots, H_{h-1}\}$ on G relative to H_0, where G is the elementary abelian subgroup of order q^{d+1} and $h = \frac{q^{d+1}-1}{q-1}$. By Theorem 2.2, the case $d = 1$ implies the existence of a (q^2, q, q^2, q) semi-regular RDS in any group G' containing G as a subgroup of index q. We shall develop a powerful generalisation of this hyperplane construction in Section 4.

In this paper we consider only the case $m = \sqrt{at}$ of a (a, m, t) BS. We have given the more general definition because of the apparent connection with divisible difference sets. It seems that many other known constructions for divisible difference sets can be analysed in terms of BSs.

A second example, due to Arasu and Sehgal [3], is a $(8, 4, 2)$ BS on $Z_4^2 \times Z_2 = \langle x, y, z \mid x^4 = y^4 = z^2 = 1\rangle$ relative to $\langle x^2, y^2\rangle \cong Z_2^2$, where the building blocks are $\{1, x, xz, x^2z, x^2yz, xy, xy^3z, y^3\}$ and $\{1, x^3, x^3y^2z, x^2y^2z, yz, xy^3z, xy^3, x^2y\}$. By Theorem 2.2, this implies the existence of a $(16, 4, 16, 4)$ semi-regular RDS in each of the groups $Z_8 \times Z_4 \times Z_2$, Z_4^3, and $Z_4^2 \times Z_2^2$ relative to a subgroup isomorphic to Z_2^2 contained within two of the largest direct factors of the group.

Given a $(a, \sqrt{at}, t)$ BS $\{B_1, B_2, \ldots B_t\}$ on a group G relative to a subgroup U of order u we can find several constraints on the parameters a, t, u and $|G|$. Theorem 2.2 implies that

which are nonprincipal on G, the required character sum modulus of $\sqrt{n} = q^d$ is provided by a contribution of q^d from one subset and 0 from all the other subsets. For nonprincipal characters of G' which are principal on G, we shall see that the required character sum modulus of q^d follows easily as a consequence of the subset sizes.

A construction for semi-regular RDSs depending on the same property, in the case $d = 1$, is due to Davis [8]. Let G' be any group (not necessarily abelian) containing G as a central subgroup of index $h - 1 = q$ and let $g'_1, g'_2, \ldots g'_{h-1}$ be coset representatives of G in G'. Then $\cup_{i=1}^{h-1} g'_i H_i$ is a (q^2, q, q^2, q) semi-regular RDS in G' relative to H_0. The RDS is comprised of $h-1$ subsets of G, namely $h-1$ of the h hyperplanes. In the case when G' is abelian, Lemma 1.1 (ii) can be used to verify that the construction produces a RDS, as follows. If a nonprincipal character χ of G is principal on H_0 then each subset provides a contribution to the character sum modulus of 0, and if χ is nonprincipal on H_0 then one subset contributes $\sqrt{k} = q$ and the rest contribute 0. This gives the required character sum modulus for characters of G' which are nonprincipal on G. For nonprincipal characters of G' which are principal on G, the required character sum modulus of 0 is again a consequence of the subset sizes. [8] reports an observation of Pott's that, in the case $d > 1$, the same construction produces a $(q(h-1), q^d, q^d(h-1), q^{d+1}(\frac{q^{d-1}-1}{q-1}), q^d(\frac{q^d-1}{q-1}))$ semi-regular divisible difference set in G' relative to H_0 because of the mutual character properties of the hyperplanes (see Jungnickel [24] for a definition and discussion of divisible difference sets).

Motivated by these examples, we define a *building block in a group G with modulus m* to be a subset of G such that all nonprincipal character sums over the subset have modulus either 0 or m. Here and subsequently in the paper, all groups will be implicitly assumed to be abelian unless otherwise stated. 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. For integers $a \geq 1$ and $t \geq 1$ we define a (a, m, t) *building set (BS) on a group G relative to a subgroup U* to be a collection of t building blocks in G with modulus m, each containing a elements, such that for every nonprincipal character χ of G

(i) exactly one building block has nonzero character sum if χ is nonprincipal on U and

(ii) no building block has nonzero character sum if χ is principal on U.

It follows immediately from Lemma 1.1 (ii) and the relationship between RDS parameters that, for $a > 1$, a $(a, \sqrt{a}, 1)$ BS on a group G relative to a subgroup U of order u is equivalent to a $(a, u, a, a/u)$ semi-regular RDS in G relative to U. (A trivial $(1, 1, 1)$ BS is equivalent to a $(1, u, 1, 0)$ RDS.)

We now show 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 particular we shall construct a semi-regular RDS as a single building block on a group containing G.

Lemma 2.1 *Suppose there exists a $(a, \sqrt{at}, t)$ BS on a group G relative to a subgroup U. Then there exists a $(as, \sqrt{at}, t/s)$ BS on G' relative to U, where s divides t and G' is any group containing G as a subgroup of index s.*

Proof: Let $\{B_1, B_2, \ldots, B_t\}$ be a $(a, \sqrt{at}, t)$ BS on G relative to U. For each $j = 1, 2, \ldots, t/s$ 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

the character sum $\chi(C)$ is 0 for all nonprincipal characters χ of G if and only if C is a multiple of G (regarded as a group ring element), and that $\sum_{\chi \in G^*} \chi(g)$ is nonzero if and only if $g = 1_G$. If a character χ is nonprincipal on G and principal on a subgroup U then χ induces a nonprincipal character ψ on G/U defined by $\psi(gU) = \chi(g)$. (ψ is well-defined because if $g_1U = g_2U$ then $g_1 = ug_2$ for some $u \in U$ and $\chi(u) = 1$ for every element u of U.)

The use of character sums to study difference sets in abelian groups was introduced by Turyn in his seminal paper [49] and subsequently extended to RDSs:

Lemma 1.1

(i) *The k-element subset D of an abelian group G of order v is a (v, k, λ, n)-difference set in G if and only if $|\chi(D)| = \sqrt{n}$ for every nonprincipal character χ of G.*

(ii) *The k-element subset R of an abelian group G of order mu 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 nonprincipal character χ of G*

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

The existence of a subset D or R in Lemma 1.1 with the character properties described forces the implicitly defined parameters n and λ respectively to be integer. Lemma 1.1 indicates a general strategy for constructing difference sets and RDSs, namely to choose a group subset for which all nonprincipal character sums have the correct modulus. In Section 2 we show that the determination of character sums can be greatly facilitated by selecting the group subset as a collection of "building blocks" which interact in a simple way. This formalises many ideas which have been used implicitly in previous papers. At the end of Section 2 we give an overview of the paper in terms of the concepts introduced.

2 Building sets

Many of the key ideas in this paper were developed from studying a construction due to McFarland [37], and a modification given by Dillon [16], for difference sets with parameters (2). The construction regards the elementary abelian group G of order q^{d+1} as a vector space P of dimension $d + 1$ over GF(q), where q is a prime power. There are $h = \frac{q^{d+1}-1}{q-1}$ subspaces $H_0, H_1, \ldots, H_{h-1}$ of P of dimension d, called hyperplanes. Let G' be any group (not necessarily abelian) containing G as a central subgroup of index $h + 1$ and let $g'_0, g'_1, \ldots g'_h \in G'$ be coset representatives of G in G'. Then $\cup_{i=0}^{h-1} g'_i H_i$ is a McFarland difference set in G'. The construction can be viewed as depending crucially on the following property: for any nonprincipal character of G there is exactly one hyperplane H_i having a nonzero character sum, and this nonzero character sum always has the same modulus q^d. The difference set is comprised of $h+1$ subsets of G, namely the hyperplanes together with the empty set. In the case when G' is abelian, Lemma 1.1 (i) can be used to verify that the construction produces a difference set, as follows. For characters of G'

regular RDS in G. This RDS construction produces the families of RDSs needed for the recursive difference set construction. It also establishes an extensive pattern of existence for semi-regular RDSs relative to subgroups $U \cong Z_p^r$, for each $r \geq 1$. This significantly improves on the previous state of knowledge for semi-regular RDSs, particularly when $r > 1$. The position of the subgroup U within the group G is of crucial importance in these results. We show that the order of G can grow without bound while its Sylow p-subgroup has fixed rank and that this rank can be as small as $2r$. In the case $p^r = 2$ we obtain results for groups G whose order need not be a prime power, so that the RDS parameters have the form $(2\lambda, 2, 2\lambda, \lambda)$ where λ need not be a power of 2. In all other cases our results are for p-groups G and so the RDS parameters have the form (p^w, p^r, p^w, p^{w-r}) for p prime. In particular, we improve on Ma and Schmidt's result [33] to show that there exists a (p^w, p, p^w, p^{w-1}) semi-regular RDS in any abelian group G of order p^{w+1} relative to any subgroup U of order p except possibly when p is odd, $w = 2d+1$ is odd, and either $G = Z_{p^{d+1}}^2$ or $G = U \times Z_{p^{d+1}} \times Z_{p^d}$. We are not aware of any abelian groups G known to contain semi-regular RDSs relative to an elementary abelian subgroup which are not covered by our results.

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

An alternative viewpoint for considering difference sets and RDSs, predominant in engineering papers, is via the correlation properties of binary arrays [23]. The $(1, 0)$ binary array A corresponding to a subset D of G is $(a_g \mid g \in G)$ 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 $Z[G]$, where $R_A(g) = \sum_{h \in G} a_h a_{gh}$ is the autocorrelation of the array A at displacement g. The $(+1, -1)$ binary array $B = (b_g \mid g \in G)$ is given by the linear transformation $b_g = 1 - 2a_g$. When G is abelian the binary arrays A and B can be represented as matrices. Although binary arrays do not appear in this exposition we have found the $(+1, -1)$ matrix representation to be an invaluable tool for visualisation.

We now give some definitions and results which will be used freely throughout the paper without reference. We shall follow the practice (standard in the difference set literature) of abusing notation by identifying sets with group ring elements, as described above. Since we shall be concerned principally with abelian groups, all groups will be implicitly abelian unless otherwise stated. We write $\prod_{i=1}^r Z_{\alpha_i}$ for the direct product $Z_{\alpha_1} \times Z_{\alpha_2} \times \cdots \times Z_{\alpha_r}$. For w a positive integer and p prime, we call p *self-conjugate modulo* w if $p^i \equiv -1 \pmod{w_p}$ for some integer i, where w_p is the largest divisor of w coprime to p. In the abelian case, a *character* of the group G is a homomorphism from G to the multiplicative group of complex roots of unity. Under pointwise multiplication the set 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 is $\chi(C) = \sum_{c \in C} \chi(c)$. It is well-known that

time, unifies the Hadamard, McFarland and Spence families. No abelian group known to contain a difference set with parameters from one of these families lies outside the scope of this result. The construction also yields the new parameter family

$$(v,k,\lambda,n) = \left(2^{2d+4}\left(\frac{2^{2d+2}-1}{3}\right), 2^{2d+1}\left(\frac{2^{2d+3}+1}{3}\right), 2^{2d+1}\left(\frac{2^{2d+1}+1}{3}\right), 2^{4d+2}\right) \tag{4}$$

for integer $d \geq 0$, for which the smallest previously unknown abelian examples occur in the groups $Z_2^6 \times Z_5$, $Z_4 \times Z_2^4 \times Z_5$ and $Z_4^2 \times Z_2^2 \times Z_5$ with parameters $(320, 88, 24, 64)$. This family of difference sets also represents a new family of symmetric designs with the same parameters (4). In addition the construction establishes that a McFarland difference set with $q = 4$ exists in an abelian group of order $2^{2d+3}(2^{2d+1}+1)/3$ if and only if the Sylow 2-subgroup has exponent at most 4. This necessary and sufficient condition is analogous to Kraemer's [26] result for the case $q = 2$. The smallest previously unknown examples occur in the groups $Z_4^2 \times Z_2^3 \times Z_{11}$ and $Z_4^3 \times Z_2 \times Z_{11}$ with parameters $(1408, 336, 80, 256)$. The essential idea of the construction is to combine multiple copies of a difference set with a semi-regular relative difference set to generate a difference set in a larger group. A preliminary announcement of these results was given in [10].

A k-element subset R of a finite multiplicative group G of order mu 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 $\{r_1 r_2^{-1} \mid r_1, r_2 \in R, r_1 \neq r_2\}$ 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. For example, $R = \{1, x, y, xy^3, z, xy^2z, x^2y^3z, x^3y^3z\}$ is a $(8, 4, 8, 2)$ RDS in $Z_4^2 \times Z_2 = \langle x, y, z \mid x^4 = y^4 = z^2 = 1\rangle$ relative to $\langle x^2, y^2\rangle \cong Z_2^2$. 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 [24]. For a recent survey of RDSs see Pott [43]. The central problem is to determine, for each parameter set (m, u, k, λ), the groups G of order mu and the 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 $(u\lambda, u, u\lambda, \lambda)$. In contrast to the situation for difference sets, the complement $G \setminus R$ of a RDS R is not in general a RDS. The trivial cases $k = 0$ and $k = 1$ are usually excluded. A difference set can be considered as a RDS with $u = 1$. Furthermore the image of a (m, u, k, λ) RDS in G relative to U under the quotient mapping from G to G/U is a $(m, k, u\lambda, k - u\lambda)$-difference set in G/U. In particular, the image of a semi-regular $(u\lambda, u, u\lambda, \lambda)$ RDS in G relative to U is a trivial $(u\lambda, u\lambda, u\lambda, 0)$-difference set in G/U. A great deal of attention has been paid to semi-regular RDSs in p-groups, whose parameters have the form (p^w, p^r, p^w, p^{w-r}) for p prime. Indeed Pott [43] calls the central problem for these RDSs "one of the most interesting questions about RDSs". Ma and Schmidt [33] have recently solved the central problem for $r = 1$ in the abelian case, with some exceptions when w and p are odd, but describe the case $r > 1$ as "much more difficult".

In this paper we present a recursive construction for semi-regular RDSs in a group G relative to a subgroup $U \cong Z_p^r$, where the Sylow p-subgroup of G has rank at least $2r$. The essential idea is to combine semi-regular RDSs in p^r quotient groups of G to form a semi-

for q a prime power and integer $d \geq 0$ (see Ma and Schmidt [35] for a summary and new results). 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 regular Hadamard matrix [25], [49]. The Hadamard and McFarland families intersect in 2-groups: the Hadamard family with $N = 2^d$ corresponds to the McFarland family with $q = 2$. The most recent discovery of a new family of parameters for which difference sets exist was given by Spence [48] in 1977:

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

for integer $d \geq 0$. Other families of difference set parameters include the Projective Geometries, the Paley-Hadamard family and the Twin Prime Power family [4].

For each of these parameter families, difference sets have been constructed for infinitely many values of the parameters, but not necessarily in all possible groups of each order. A notable exception is abelian 2-groups, for which Kraemer [26] completely solved the central problem: a Hadamard difference set exists in an abelian group G of order 2^{2d+2} if and only if $\exp(G) \leq 2^{d+2}$. (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 $g \in G$.)

A powerful stimulus to the discovery of new results on difference sets has been the identification of open cases in groups of relatively small order. For example, Dillon [14] led a research programme to examine constructions and nonexistence results for Hadamard difference sets in all 267 groups of order 64, which highlighted a single outstanding case. The solution of this last case by Liebler and Smith [30] demonstrated that Turyn's exponent bound [49] of 2^{d+2} for Hadamard difference sets in abelian groups of order 2^{2d+2} can be exceeded in the nonabelian case. A subsequent collaborative effort to examine Hadamard difference sets in groups of order 100 led to Smith's surprising discovery [47] of a nonabelian group of order 100 which contains a Hadamard difference set even though no abelian group of this order does so! Another example is the table of existence of difference sets in abelian groups with $k \leq 50$ produced by Lander [27], of which the last open cases have recently been settled by J.E. Iiams [private communication, 1994]. In 1992 Jungnickel [25] modified the parameter range of this table to $n \leq 30$ and listed three open cases, the last of which was settled when Arasu and Sehgal [3] exhibited a $(96,20,4,16)$ McFarland difference set in $Z_4^2 \times Z_2 \times Z_3$, having $q = 4$ and $d = 1$. This was the first example of a McFarland difference set having $q = 2^r > 2$ in a group whose Sylow 2-subgroup does not have the form $Z_2^{(d+1)r+1}$, as constructed by McFarland [37], or $Z_4 \times Z_2^{(d+1)r-1}$, as constructed by Dillon [16]. Arasu and Sehgal's discovery sparked a search for a similar McFarland difference set in a larger group, for which the most likely candidate was generally presumed to be a $(640,72,8,64)$-difference set in $Z_4^2 \times Z_2^3 \times Z_5$ or $Z_4^3 \times Z_2 \times Z_5$, having $q = 8$ and $d = 1$. We were unable to settle these cases but managed to construct new difference sets by transferring partial results from one of these groups to a group of order 320. This new example led to many insights and eventually to the results reported in this paper. In retrospect we believe that the natural generalisation of Arasu and Sehgal's example has $q = 4$ and $d > 1$ rather than $q > 4$ and $d = 1$.

In this paper we present a recursive construction for difference sets which, for the first

1 Introduction

A k-element subset D of a finite multiplicative group G of order v is called a (v,k,λ,n)-*difference set in* G provided that the multiset of "differences" $\{d_1 d_2^{-1} \mid d_1, d_2 \in D, d_1 \neq d_2\}$ contains each nonidentity element of G exactly λ times; we write $n = k - \lambda$. For example, $D = \{x, x^2, x^4\}$ is a $(7,3,1,2)$-difference set in $Z_7 = \langle x \mid x^7 = 1\rangle$. It is easy to check that $\{y, x, xy, xy^2, x^2y, x^3y^3\}$, $\{z, xz, z^2, yz^2, z^3, xyz^3\}$ and $\{z, xz, w, yw, zw, xyzw\}$ are examples of $(16,6,2,4)$-difference sets in the abelian groups $Z_4^2 = \langle x, y \mid x^4 = y^4 = 1\rangle$, $Z_4 \times Z_2^2 = \langle x, y, z \mid z^4 = x^2 = y^2 = 1\rangle$ and $Z_2^4 = \langle x, y, z, w \mid x^2 = y^2 = z^2 = w^2 = 1\rangle$ respectively.

Difference sets arise in a wide variety of theoretical and applied contexts. They are important in design theory because a (v,k,λ,n)-difference set in G is equivalent to a symmetric (v,k,λ,n)-design with a regular automorphism group G [27]. The study of difference sets is also deeply connected with coding theory because the code, over a field F, of the symmetric design corresponding to a (v,k,λ,n)-difference set may be considered as the right ideal generated by D in the group algebra FG [25], [27]. Difference sets in abelian groups are the natural solution to many problems of signal design in digital communications, including synchronization [21], radar [1], coded aperture imaging [19], [46] and optical image alignment [36]. For a recent survey of difference sets see Jungnickel [25].

The central problem is to determine, for each parameter set (v,k,λ,n), which groups of order v contain a difference set with these parameters. An extensive literature has been devoted to this problem, exposing considerable interplay between difference sets and such diverse branches of mathematics as algebraic number theory, character theory, representation theory, finite geometry and graph theory. Nonetheless the central problem remains open, both for abelian and nonabelian groups, except for heavily restricted parameter sets. One of the most popular techniques for constructing a difference set or for ruling out its existence is to consider the image of a hypothetical difference set under mappings from the group G to one or more quotient groups G/U (see Ma and Schmidt [32] for a recent example).

By a counting argument the parameters (v,k,λ,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,λ,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 we shall use trivial examples as the initial case of some recursive constructions). Besides these constraints, difference sets are classified into families according to further relationships between the parameters. A great deal of research on difference sets has focussed on two particular families of parameters: the Hadamard family given by

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

for integer $N \geq 1$ (see Davis and Jedwab [11] for a survey), and the McFarland family given by

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

A unifying construction for difference sets

James A. Davis*, Department of Mathematics,
University of Richmond, Virginia 23173, U.S.A.

Jonathan Jedwab, Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford, Bristol BS12 6QZ, U.K.

February 1996

Abstract

We present a recursive construction for difference sets which unifies the Hadamard, McFarland and Spence parameter families and deals with all abelian groups known to contain such difference sets. The construction yields a new family of difference sets with parameters $(v, k, \lambda, n) = (2^{2d+4}(2^{2d+2}-1)/3,\ 2^{2d+1}(2^{2d+3}+1)/3,\ 2^{2d+1}(2^{2d+1}+1)/3,\ 2^{4d+2})$ for $d \geq 0$. The construction establishes that a McFarland difference set exists in an abelian group of order $2^{2d+3}(2^{2d+1}+1)/3$ if and only if the Sylow 2-subgroup has exponent at most 4. The results depend on a second recursive construction, for semi-regular relative difference sets with an elementary abelian forbidden subgroup of order p^r. This second construction deals with all abelian groups known to contain such relative difference sets and significantly improves on previous results, particularly for $r > 1$. We show that the group order need not be a prime power when the forbidden subgroup has order 2. We also show that the group order can grow without bound while its Sylow p-subgroup has fixed rank and that this rank can be as small as $2r$. Both of the recursive constructions generalise to nonabelian groups.

*The author thanks Hewlett-Packard for their generous hospitality and support during his sabbatical year 1995–6. This work is also partially supported by NSA grant # MDA904-94-2062.