A New Family of Relative Difference Sets in 2-Groups

James A. Davis*, Jonathan Jedwab
Networked Systems Department
HP Laboratories Bristol
HPL-98-124
July, 1998

relative difference sets, recursive, building sets, characters

We recursively construct a new family of $(2^{6d+4}, 8, 2^{6d+4}, 2^{6d+1})$ semi-regular relative difference sets in abelian groups G relative to an elementary abelian subgroup U. The initial case $d = 0$ of the recursion comprises examples of (16,8,16,2) relative difference sets for four distinct pairs (G, U).

*Department of Mathematics and Computer Science, University of Richmond, Richmond, Virginia

A new family of relative difference sets in 2-groups

James A. Davis, Department of Mathematics and Computer Science,
University of Richmond, Virginia 23173, U.S.A.

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

June 22, 1998

Abstract

We recursively construct a new family of $(2^{6d+4}, 8, 2^{6d+4}, 2^{6d+1})$ semi-regular relative difference sets in abelian groups G relative to an elementary abelian subgroup U. The initial case $d = 0$ of the recursion comprises examples of $(16, 8, 16, 2)$ relative difference sets for four distinct pairs (G, U).

The square root problem

Let G be a group of order mu and U a normal subgroup of G of order u. If R is a k-subset of G then R is a (m, u, k, λ) *relative difference set* (RDS) in G relative to U provided that the multiset of differences rr'^{-1} for $r, r' \in R, r \neq r'$, contains every element of $G \setminus U$ exactly λ times and contains no element of U. If $k = u\lambda$ then the RDS is called *semi-regular* and the parameters are $(u\lambda, u, u\lambda, \lambda)$. In this paper we consider semi-regular RDSs with parameters of the form

$$(2^a, 2^b, 2^a, 2^{a-b}). \tag{1}$$

Several families of such RDSs have been constructed for $b \leq a/2$ [3]. However for $b > a/2$ the only known existence results for abelian groups are as follows:

Theorem 1 *There is a $(2^a, 2^b, 2^a, 2^{a-b})$ RDS in the group $\mathbb{Z}_4^b \times \mathbb{Z}_2^{a-b}$, relative to the subgroup $U \cong \mathbb{Z}_2^b$ contained in $\mathbb{Z}_4^b$, for each b satisfying $a/2 < b \leq a$.*

Theorem 2 *There is a $(2^{2b-1}, 2^b, 2^{2b-1}, 2^{b-1})$ RDS in any abelian group G of order 2^{3b-1} and exponent 4 relative to $U \cong \mathbb{Z}_2^b$, where U is contained within a subgroup of G isomorphic to $\mathbb{Z}_4^b$, for each odd $b \geq 1$.*

Theorem 1 is due to Jungnickel [6] (taking into account the well-known method of contraction [7]). Theorem 2 is due to Chen, Ray-Chaudhuri and Xiang [2]. Ganley [5] has shown that when $b = a$ the only abelian group G containing an RDS with parameters (1) is $\mathbb{Z}_4^a$, and Schmidt [9] has given further nonexistence results for $b > a/2$. Nonetheless there is a large gap of understanding between the known existence and nonexistence results when $b > a/2$. We refer to this gap as the "square root problem" because it corresponds to the parameter relationship $u > \sqrt{k}$. In this section we give new solutions to the square root problem by exhibiting a $(16, 8, 16, 2)$ RDS for four distinct pairs (G, U).

Relative difference sets are often studied in the context of a group ring $\mathbb{Z}[G]$ and group characters. The definition of a RDS immediately yields the group ring equation $RR^{(-1)} = k1_G + \lambda(G - U)$, where we identify R, $R^{(-1)}$ and G with the respective group ring elements $R = \sum_{r \in R} r$, $R^{(-1)} = \sum_{r \in R} r^{-1}$ and $G = \sum_{g \in G} g$. Characters of an abelian group G are homomorphisms from G to the multiplicative group of complex roots of unity, and we extend this homomorphism to the entire group ring in the natural way. The element R of $\mathbb{Z}[G]$ then satisfies the definition of a semi-regular RDS if and only if two conditions hold [7]: first, any character that is nonprincipal (*i.e.* nontrivial) on the subgroup U has a character sum over R of modulus $\sqrt{u\lambda}$, and second, any character that is principal (*i.e.* trivial) on the subgroup U but nonprincipal on the group G has a character sum of 0 over R.

Davis and Jedwab [3] describe a theoretical framework for constructing RDSs a piece at a time. We define a (a, m, t) building set (BS) on an abelian group G relative to a subgroup U to be a collection of t subsets of G (called building blocks), each of size a, such that for any nonprincipal character χ of G:

(i) Exactly one building block has a character sum of modulus m and all other building blocks have character sum 0 if χ is nonprincipal on U and

(ii) All building blocks have character sum 0 if χ is principal on U.

Theorem 3 ([3], Theorem 2.2) *Suppose there exists a $(a, \sqrt{at}, t)$ BS $\{B_1, B_2, \ldots, B_t\}$ on an abelian group G relative to a subgroup U of order u, where $at > 1$. Then $\cup_{i=1}^{t} g_i' B_i$ is a $(at, u, at, at/u)$ semi-regular RDS in G' relative to U, where G' is any abelian group containing G as a subgroup of index t and the g_i' lie in distinct cosets of G in G'.*

All the new RDSs of this paper arise from the following example.

Example 4 *Let G be the group $\langle x, y, z, w | x^4 = y^4 = z^2 = w^2 = 1\rangle \cong \mathbb{Z}_4^2 \times \mathbb{Z}_2^2$ and let U be the subgroup $\langle x^2, y^2, w\rangle \cong \mathbb{Z}_2^3$. The subsets $B_1 = 1 + x + y + xyw + z(1 + x^3 + y^3 + x^3y^3w)$ and $B_2 = 1 + xy^2 + x^2yw + x^3y^3 + y^2zw(1 + x^3y^2 + x^2y^3w + xy)$ form a $(8, 4, 2)$ BS on G relative to U.*

By Theorem 3 this implies there is a $(16, 8, 16, 2)$ RDS R in G' relative to U as follows:

1. $G' = \langle x'^8 = y^4 = z^2 = w^2 = 1\rangle \cong \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2^2$; $U = \langle x'^4, y^2, w\rangle$; $R = B_1 \cup x' B_2$.

2. $G' = \langle x^4 = y^4 = z'^4 = w^2 = 1\rangle \cong \mathbb{Z}_4^3 \times \mathbb{Z}_2$; $U = \langle x^2, y^2, w\rangle$; $R = B_1 \cup z' B_2$.

3. $G' = \langle x^4 = y^4 = z^2 = w'^4 = 1\rangle \cong \mathbb{Z}_4^3 \times \mathbb{Z}_2$; $U = \langle x^2, y^2, w'^2\rangle$; $R = B_1 \cup w' B_2$.

4. $G' = \langle x^4 = y^4 = z^2 = w^2 = v'^2 = 1\rangle \cong \mathbb{Z}_4^2 \times \mathbb{Z}_2^3$; $U = \langle x^2, y^2, w\rangle$; $R = B_1 \cup v' B_2$.

The following Mathematica commands can be used to verify that the building blocks of Example 4 satisfy the definition of a $(8, 4, 2)$ BS:

```
B1[x_,y_,z_,w_]:=1 + x + y + x y w + z (1 + x^3 + y^3 + x^3 y^3 w);
B2[x_,y_,z_,w_]:=1 + x y^2 + x^2 y w + x^3 y^3 +
y^2 z w (1 + x^3 y^2 + x^2 y^3 w + x y);
Do[Print[i,j,k,l,B1[I^i,I^j,(-1)^k,(-1)^l],B2[I^i,I^j,(-1)^k,(-1)^l]],
{i,0,3},{j,0,3},{k,0,1},{l,0,1}]
```

The evaluation of B1 and B2 in the Do loop runs through all the possible character values. The output indicates that exactly one of the two blocks has character sum of modulus 4 for the appropriate characters, and that they both have character sum 0 for the other characters (the first character that prints out is the principal character, and that has a sum of 8 for both characters).

The quotient group $G/\langle w \rangle$ in Example 4 is isomorphic to $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ and under this contraction the building blocks B_1 and B_2 are similar to the building blocks of the Arasu-Sehgal example [1]. In other words, the building blocks B_1 and B_2 can be viewed as "lifts" of the Arasu-Sehgal building blocks. This observation, together with a better understanding of the structure of B_1 and B_2, might lead to a generalisation to higher order groups that would give further solutions to the square root problem.

A new family of semi-regular RDSs

In this section we use Example 4 as an initial case to recursively construct a new family of BSs and then, using Theorem 3, to obtain a new family of semi-regular RDSs. (For a summary of the current state of knowledge for semi-regular RDSs in abelian groups relative to an elementary abelian subgroup see [3] and [4].) The recursive construction of BSs follows the method of [3] in making use of the $p^r + 1$ hyperplanes of the group $\mathbb{Z}_p^{2r}$, regarded as a vector space of dimension 2 over $\mathrm{GF}(p^r)$.

Theorem 5 ([3], Theorem 4.3) *Let G be an abelian group of order $p^{2r}a$ containing a subgroup $Q \cong \mathbb{Z}_p^{2r}$, 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.*

To apply Theorem 5 effectively we require information about the form of the quotient groups G/H_i and Q/H_i. We know (see Lemma 7 below) that if G has rank exactly $2r$ then by an 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), whereas r have their exponent reduced by a factor of p. However Example 4 has a feature not previously considered: the subgroup U is contained in a subgroup of G isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4^2$ but not in a subgroup isomorphic to $\mathbb{Z}_4^3$. To deal with this feature we begin with a group theoretic lemma.

Lemma 6 *Let $y_1, y_2, \ldots, y_r$ be elements of an abelian group G and let H be a subgroup of G. If $\langle y_u \rangle \cap \langle y_j \mid j \neq u \rangle = \{1\}$ for each u in the range $1 \leq u \leq r$ and no nonidentity element of the form $\prod_{u=1}^{r} y_u^{j_u}$ is contained in H, then $\langle y_1 H, y_2 H, \ldots, y_r H \rangle \cong \langle y_1 H \rangle \times \langle y_2 H \rangle \times \cdots \times \langle y_r H \rangle$.*

Proof: We prove this by induction on r starting with the case $r = 2$. We claim that $\langle y_1 H \rangle \cap \langle y_2 H \rangle = \{H\}$. Suppose, for a contradiction, that this is not true. Then there are integers α and β for which $(y_1 H)^\alpha = (y_2 H)^\beta \neq H$. The equality $(y_1 H)^\alpha = (y_2 H)^\beta$ implies that $y_1^\alpha y_2^{-\beta} \in H$ and so by the assumption on nonidentity elements we deduce that $y_1^\alpha = y_2^\beta$. By assumption $\langle y_1 \rangle \cap \langle y_2 \rangle = \{1\}$ and so $y_1^\alpha = y_2^\beta = 1$, contradicting the inequality $(y_1 H)^\alpha \neq H$. Therefore the subgroups $\langle y_1 H \rangle$ and $\langle y_2 H \rangle$ have trivial intersection as claimed. By Theorem 2.24 of [8], the subgroup generated by any two normal subgroups which intersect trivially is isomorphic to the (external) direct product of those subgroups, proving the case $r = 2$.

In the inductive step, we use the same argument to show that the groups $\langle y_1 H \rangle$ and $\langle y_2 H, y_3 H, \ldots, y_r H \rangle$ have trivial intersection and therefore that $\langle y_1 H, y_2 H, \ldots, y_r H \rangle \cong \langle y_1 H \rangle \times \langle y_2 H, y_3 H, \ldots, y_r H \rangle$. The inductive hypothesis applied to the elements $y_2, y_3, \ldots, y_r$ then proves the Lemma. □

We can now characterise the form of the quotient groups G/H_i and Q/H_i as discussed. We write $\prod_{u=1}^{r} \mathbb{Z}_{\alpha_u}$ for the direct product $\mathbb{Z}_{\alpha_1} \times \mathbb{Z}_{\alpha_2} \times \cdots \times \mathbb{Z}_{\alpha_r}$.

Lemma 7 *Let G be the group $\prod_{u=1}^{2r} \mathbb{Z}_{p^{1+\alpha_u}}$ containing a subgroup $Q \cong \mathbb{Z}_p^{2r}$, where p is prime and $\alpha_u \geq 0$. Let $H_0, H_1, \ldots, H_{p^r}$ be the subgroups of G of order p^r corresponding to hyperplanes when viewed as subgroups of Q. Then for each H_i there exists a r-element subset S of $\{1, 2, \ldots, 2r\}$ such that $G/H_i \cong \prod_{u \notin S} \mathbb{Z}_{p^{1+\alpha_u}} \times \prod_{u \in S} \mathbb{Z}_{p^{\alpha_u}}$. Moreover, for each H_i a suitable choice of generators of G ensures that $Q/H_i \cong \mathbb{Z}_p^r$ is contained in the first r direct factors of G/H_i as specified. Furthermore if H_0 is contained in a subgroup of G isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_{p^2}^{r-1}$ then, for each $H_i \neq H_0$, Q/H_i is contained in a subgroup of G/H_i isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_{p^2}^{r-1}$.*

Proof: This result is given as Lemma 4.4 of [3], except for the final sentence in the case when H_0 is not contained in a subgroup of G isomorphic to $\mathbb{Z}_{p^2}^r$. To prove this case, let $\alpha_1 = 0$ and $\alpha_u \geq 1$ for $2 \leq u \leq r$ and let $\{x_u \mid 1 \leq u \leq 2r\}$ be a set of generators of G such that $G = \langle x_u \mid x_u^{p^{1+\alpha_u}} = 1 \rangle$ and $H_0 = \langle x_1, x_2^{p^{\alpha_2}}, \ldots, x_r^{p^{\alpha_r}} \rangle$. Fix $H_i \neq H_0$ and put $y_1 = x_1$ and $y_u = x_u^{p^{\alpha_u}}$ for $2 \leq u \leq r$. Clearly $\langle y_u \rangle \cap \langle y_j \mid j \neq u, j \leq r \rangle = \{1\}$ for each u in the range $1 \leq u \leq r$. Since the hyperplanes $H_0, H_1, \ldots, H_{p^r}$ partition the nonidentity elements of Q and by assumption $H_0 = \langle y_1, y_2, \ldots, y_r \rangle$, no nonidentity element of the form $\prod_{u=1}^{r} y_u^{j_u}$ (where $0 \leq j_u < p$) is contained in H_i. Applying Lemma 6 and then substituting for the y_u in terms of the x_u we find that $T = \langle x_1 H_i, x_2^{p^{\alpha_2}} H_i, \ldots, x_r^{p^{\alpha_r}} H_i \rangle \cong \langle x_1 H_i \rangle \times \langle x_2^{p^{\alpha_2}} H_i \rangle \times \cdots \times \langle x_r^{p^{\alpha_r}} H_i \rangle \cong \mathbb{Z}_p^r$. Since T is a subgroup of Q/H_i and has the same order p^r, it follows that $T = Q/H_i$.

Now $T = Q/H_i$ is contained in the subgroup $V = \langle x_1 H_i, x_2^{p^{\alpha_2 - 1}} H_i, \ldots, x_r^{p^{\alpha_r - 1}} H_i \rangle$. Put $z_1 = x_1$ and $z_u = x_u^{p^{\alpha_u - 1}}$ for $2 \leq u \leq r$. We wish to apply Lemma 6 to $z_1, z_2, \ldots, z_r$ to conclude that $V \cong \langle x_1 H_i\rangle \times \langle x_2^{p^{\alpha_2-1}} H_i\rangle \times \cdots \times \langle x_r^{p^{\alpha_r-1}} H_i\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_{p^2}^{r-1}$ as required. We can do so by showing that if $z = \prod_{u=1}^r z_u^{j_u} \in H_i$ (where $0 \le j_1 < p$ and $0 \le j_u < p^2$ for $2 \le u \le r$) then $z = 1$. Now H_i is isomorphic to $\mathbb{Z}_p^r$ and so $z^p = 1$. Writing this equation in terms of the y_u defined above we get $\prod_{u=2}^r y_u^{j_u} = 1$, which implies that $j_u = pj'_u$ for each u in the range $2 \le u \le r$ (where $0 \le j'_u < p$). Therefore $z = z_1^{j_1} \prod_{u=2}^r (z_u^p)^{j'_u}$, and since $H_0 = \langle z_1, z_2^p, \ldots, z_r^p\rangle$ we have shown that $z \in H_0 \cap H_i = \{1\}$. This completes the proof. □

We shall apply Lemma 7 with $p = 2$ and $r = 3$ to reduce the inductive step of the proof of our main result to two possibilities, depending on whether the quotient group Q/H_i is contained in a subgroup isomorphic to $\mathbb{Z}_4^3$ or not (in which case it must be contained in a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4^2$). When Q/H_i is contained in a subgroup isomorphic to $\mathbb{Z}_4^3$ we shall make use of BSs whose existence is given by the following special case ($r = 3$, $i = 1$) of Corollary 7.9 of [3]:

Theorem 8 *For each d and c satisfying $2 \le c \le d$, there exists a $(2^{3(d+c)-5}, 2^{3d-1}, 2^{3(d-c)+3})$ BS on any abelian group $G_{d,c}$ of order $2^{3(d+c)-2}$ and exponent at most 2^c relative to any subgroup $U_{d,c} \cong \mathbb{Z}_2^3$, where $U_{d,c}$ is contained in a subgroup of $G_{d,c}$ isomorphic to $\mathbb{Z}_4^3$ and where both of the following hold:*

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

(ii) *For $d > 2$ and $c = d - 1$, $G_{d,c}/U_{d,c}$ contains a subgroup of index 2^4 and exponent at most 2^{d-2}.*

Finally we require the following result on transferring BSs from a smaller group to a larger group, given as Lemma 2.1 in [3]:

Lemma 9 *Suppose there exists a $(a, \sqrt{at}, t)$ BS on an abelian 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 abelian group containing G as a subgroup of index s.*

We are now ready to state and prove the main result of the paper, namely the construction of a new family of BSs which leads to a new family of RDSs.

Theorem 10 *There exists a $(8, 4, 2)$ BS on the group $\mathbb{Z}_2 \times \mathbb{Z}_4^2 \times \mathbb{Z}_2$ relative to the subgroup $\mathbb{Z}_2^3$ contained in the first three direct factors. There exists a $(2^6, 2^5, 2^4)$ BS on the group $\mathbb{Z}_2 \times \mathbb{Z}_4^2 \times \mathbb{Z}_2^4$ relative to the subgroup $\mathbb{Z}_2^3$ contained in the first three direct factors. For each d and c satisfying $2 \le c \le d$, there exists a $(2^{3(d+c)-2}, 2^{3d+2}, 2^{3(d-c)+6})$ BS on any abelian group $G_{d,c}$ of order $2^{3(d+c)+1}$ and exponent at most 2^c relative to any subgroup $U_{d,c} \cong \mathbb{Z}_2^3$, where $U_{d,c}$ is contained in a subgroup of $G_{d,c}$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4^2$ but not in a subgroup isomorphic to $\mathbb{Z}_4^3$ and where, for $c = d$, $G_{d,c}/U_{d,c}$ contains a subgroup of index 2^4 and exponent at most 2^{d-1}.*

Proof: The required $(8,4,2)$ BS is given by Example 4. The required $(2^6,2^5,2^4)$ BS is given by Theorem 5 and Lemma 7. Then by Lemma 9 with $s=2$, there exists a $(2^7,2^5,2^3)$ BS on both of the groups $\mathbb{Z}_2\times\mathbb{Z}_4^3\times\mathbb{Z}_2^3$ and $\mathbb{Z}_2\times\mathbb{Z}_4^2\times\mathbb{Z}_2^5$ relative to the subgroup $\mathbb{Z}_2^3$ contained in the first three direct factors.

We next establish the case $d=c=2$ by showing there exists a $(2^{10},2^8,2^6)$ BS on any group $G_{2,2}$ of order 2^{13} and exponent 4 relative to $U_{2,2}\cong\mathbb{Z}_2^3$, where $U_{2,2}$ is contained in a subgroup of $G_{2,2}$ isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_4^2$ but not in a subgroup isomorphic to $\mathbb{Z}_4^3$. We shall apply Theorem 5, choosing the subgroup $Q_{2,2}\cong\mathbb{Z}_2^6$ of $G_{2,2}$ to contain $U_{2,2}$ and to contain direct factors $\mathbb{Z}_4$ of $G_{2,2}$ in preference to direct factors $\mathbb{Z}_2$, and choosing the subgroups H_i of $G_{2,2}$ corresponding to hyperplanes of $Q_{2,2}$ so that $H_0=U_{2,2}$. The required $(2^{10},2^8,2^6)$ BS exists provided that, for each hyperplane $H_i\neq H_0$, there exists a $(2^7,2^5,2^3)$ BS on $G_{2,2}/H_i$ relative to $Q_{2,2}/H_i$. Now by Lemma 7, $G_{2,2}/H_i$ is isomorphic to one of the groups $\mathbb{Z}_2\times\mathbb{Z}_4^3\times\mathbb{Z}_2^3$, $\mathbb{Z}_2\times\mathbb{Z}_4^2\times\mathbb{Z}_2^5$, $\mathbb{Z}_4^4\times\mathbb{Z}_2^2$ and $\mathbb{Z}_4^3\times\mathbb{Z}_2^4$, with $Q_{2,2}/H_i$ contained in the first three direct factors of the group. For the first two groups the required $(2^7,2^5,2^3)$ BS is given in the preceding paragraph; for the second two groups it is given by the case $d=c=2$ of Theorem 8.

The remainder of the proof is by induction on d. Assume the case $d-1$ to be true (for each value of c in the range $2\leq c\leq d-1$). Let $U_{d,c}$ be contained in the first three direct factors of $G_{d,c}$ and order the remaining direct factors of $G_{d,c}$ in non-increasing order of their exponent. Choose $Q_{d,c}\cong\mathbb{Z}_2^6$ to be contained in the first six direct factors of $G_{d,c}$ and choose the subgroups H_i as above so that $H_0=U_{d,c}$. By Theorem 5 it is sufficient to show, for each $H_i\neq H_0$, that there exists a $(2^{3(d+c)-5},2^{3d-1},2^{3(d-c)+3})$ BS on $G_{d,c}/H_i$ relative to $Q_{d,c}/H_i$. We distinguish two cases.

Case 1: Q/H_i is contained in a subgroup isomorphic to $\mathbb{Z}_4^3$. In this case Theorem 8, using the same values for d and c, gives the required BS provided the associated conditions (i) and (ii) are met.

Condition (i) is that $(G_{d,d}/H_i)/(Q_{d,d}/H_i)\cong G_{d,d}/Q_{d,d}$ contains a subgroup of index 2 and exponent at most 2^{d-1}. Suppose, for a contradiction, that this is not the case. Since $G_{d,d}$ has exponent at most 2^d it follows that $G_{d,d}/Q_{d,d}$ contains a subgroup isomorphic to $\mathbb{Z}_{2^d}^2$. By the ordering of exponents of all but the first three direct factors of $G_{d,d}$ this implies that $G_{d,d}$ contains a subgroup isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_4^2\times\mathbb{Z}_{2^d}^5$. This contradicts the assumption that $G_{d,d}$ contains a subgroup of index 2^4 and exponent at most 2^{d-1}.

Condition (ii) is that, for $d>2$, $G_{d,d-1}/Q_{d,d-1}$ contains a subgroup of index 2^4 and exponent at most 2^{d-2}. Supposing this not to be the case, it follows similarly that $G_{d,d-1}/Q_{d,d-1}$ contains a subgroup isomorphic to $\mathbb{Z}_{2^{d-1}}^5$ and therefore that $G_{d,d-1}$ contains a subgroup isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_4^2\times\mathbb{Z}_{2^{d-1}}^8$. But then the order of $G_{d,d-1}$ would exceed the stipulated value of 2^{6d-2}, giving a contradiction.

Case 2: Q/H_i is not contained in a subgroup isomorphic to $\mathbb{Z}_4^3$. By Lemma 7, Q/H_i is therefore contained in a subgroup isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_4^2$.

For $c\leq d-1$ we apply the inductive hypothesis, with the same value of c, to give the required BS provided the associated condition is met. For $c\leq d-2$ there is no condition to check; for $c=d-1$ the condition is that $(G_{d,d-1}/H_i)/(Q_{d,d-1}/H_i)\cong G_{d,d-1}/Q_{d,d-1}$ contains a subgroup of index 2^4 and exponent at most 2^{d-2}. The proof of this condition is identical to that given in Case 1 above.

For $c = d$ there is no inductive hypothesis with the value c to provide the required $(2^{6d-5}, 2^{3d-1}, 2^3)$ BS on $G_{d,d}/H_i$ relative to $Q_{d,d}/H_i$. Instead we shall use the inductive hypothesis with the value $c = d-1$, together with Lemma 9, in the following way. Firstly we claim that $G_{d,d}/Q_{d,d}$ contains a subgroup of index 2^7 and exponent at most 2^{d-2}. To show this, note that $G_{d,d}$ has exponent at most 2^d and by assumption contains a subgroup of index 2^4 and exponent at most 2^{d-1}, so that $G_{d,d}$ contains at most four direct factors $\mathbb{Z}_{2^d}$. By the ordering of exponents of all but the first three direct factors of $G_{d,d}$ this implies that $G_{d,d}/Q_{d,d}$ contains at most one direct factor $\mathbb{Z}_{2^d}$. Therefore, if the claim were false, $G_{d,d}/Q_{d,d}$ would contain a subgroup isomorphic to either $\mathbb{Z}_{2^d} \times \mathbb{Z}_{2^{d-1}}^6$ or $\mathbb{Z}_{2^{d-1}}^8$ and in either case the order of $G_{d,d}/Q_{d,d}$ would exceed its stipulated value of 2^{6d-5}; this establishes the claim. Now it can be verified that the claim implies that $G_{d,d}/H_i$ contains a subgroup S/H_i (containing $Q_{d,d}/H_i$ in a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4^2$ but not in a subgroup isomorphic to $\mathbb{Z}_4^3$) of index 8 and exponent at most 2^{d-1} such that $(S/H_i)/(Q_{d,d}/H_i) \cong S/Q_{d,d}$ contains a subgroup of index 2^4 and exponent at most 2^{d-2}. (This is achieved by choosing a suitable subgroup $S/Q_{d,d}$ of $G_{d,d}/Q_{d,d}$ of index 8 for which the pre-image S/H_i of $(S/H_i)/(Q_{d,d}/H_i)$, under the quotient mapping from $G_{d,d}/H_i$ to $(G_{d,d}/H_i)/(Q_{d,d}/H_i)$, has exponent at most 2^{d-1}. For a detailed justification of a similar implication see the proof of Theorem 7.5 of [3].) Then the inductive hypothesis with the value $c = d-1$ gives a $(2^{6d-8}, 2^{3d-1}, 2^6)$ BS on S/H_i relative to $Q_{d,d}/H_i$, and the required $(2^{6d-5}, 2^{3d-1}, 2^3)$ BS is obtained by applying Lemma 9 with $s = 8$. □

Although each value of c in Theorem 10 gives rise, under Theorem 3, to semi-regular RDSs not occurring for any other value of c, we consider the small rank case $c = d$ to be of most interest and so state the resulting RDSs explicitly. (For clarity we have not stated the result of applying Theorem 3 to the $(8,4,2)$ and $(2^6, 2^5, 2^4)$ BSs of Theorem 10.)

Corollary 11 *For each $d \geq 2$, there exists a $(2^{6d+4}, 8, 2^{6d+4}, 2^{6d+1})$ semi-regular RDS in any abelian group G_d of order 2^{6d+7} relative to any subgroup $U_d \cong \mathbb{Z}_2^3$, where G_d contains a subgroup S_d of index 64 and exponent at most 2^d such that U_d is contained in a subgroup of S_d isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4^2$ but is not contained in a subgroup of S_d isomorphic to $\mathbb{Z}_4^3$ and such that S_d/U_d contains a subgroup of index 16 and exponent at most 2^{d-1}.*

The best previously known results for semi-regular RDSs of small rank having these parameters are those given by putting $r = 3$ and $j = 4$ in Corollary 8.4 of [3]. However Corollary 8.4 (ii) of [3] requires the rank of G_d to be at least 8 and Corollary 8.4 (v) of [3] requires U_d to be contained in a subgroup of G_d isomorphic to $\mathbb{Z}_4^3$. Corollary 11 improves on both of these results, for example by establishing for each $d \geq 2$ the existence of a $(2^{6d+4}, 8, 2^{6d+4}, 2^{6d+1})$ semi-regular RDS in $G_d = \mathbb{Z}_2 \times \mathbb{Z}_{2^{d+1}}^6$ (having rank 7) relative to the subgroup $U_d \cong \mathbb{Z}_2^3$ contained in the first three direct factors.

This section illustrates that the discovery of a single new example of a semi-regular RDS can be used to construct recursively an infinite family of such RDSs using Theorems 5 and 3 (although the only new solutions to the square root problem in this paper are those given in the previous section).

References

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

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

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

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

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

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

[7] 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.

[8] J.J. Rotman. *An Introduction to the Theory of Groups*. Allyn and Bacon, Inc., Boston, 3rd edition, 1984.

[9] B. Schmidt. On (p^a, p^b, p^a, p^{a-b})-relative difference sets. *J. Algebraic Combin.*, **6**:279–297, 1997.