2002

On the (v,5,λ)-Family of Bhaskar Rao Designs

G. R. Chaudhry
University of Wollongong

M. Greig
Greig Consulting, Vancouver, Canada

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Publication Details

This article was originally published as Chaudhry, GR, Grieg, M and Seberry, J, On the (v,5,λ)-Family of Bhaskar Rao Designs, Journal of Statistical Planning and Inference, 106, 2002, 303-327.

On the (v,5,λ)-Family of Bhaskar Rao Designs

Abstract
We establish that the necessary conditions for the existence of Bhaskar Rao designs of block size five are : i). $\lambda(v - 1) \equiv 0 \pmod 4$ ii). $\lambda v(v - 1) \equiv 0 \pmod{40}$ iii). $2|\lambda$. We show these conditions are sufficient: for $\lambda = 4$ if $v > 215$, with 10 smaller possible exceptions and one definite exception at $v = 5$; for $\lambda = 10$ if $v > 445$, with 11 smaller possible exceptions, and one definite exception at $v = 5$; and for $\lambda = 20$, with the possible exception of $v = 32$; we also give a few results for other values of λ.

Disciplines
Physical Sciences and Mathematics

Publication Details
This article was originally published as Chaudhry, GR, Grieg, M and Seberry, J, On the (v,5,λ)-Family of Bhaskar Rao Designs, Journal of Statistical Planning and Inference, 106, 2002, 303-327.

On the (v,5,λ)-Family of Bhaskar Rao Designs

Ghulam R Chaudhry
School of IT & CS, University of Wollongong
Wollongong, NSW 2522, AUSTRALIA

Malcolm Greig
Greig Consulting, 5685 Daffodil Drive
West Vancouver, BC, CANADA, V7W 1P2

Jennifer Seberry
School of IT & CS, University of Wollongong
Wollongong, NSW 2522, AUSTRALIA

e-mail:[chaudhry, j.seberry]@uow.edu.au, greig@sfu.ca

October 4, 1999

Abstract

We establish that the necessary conditions for the existence of Bhaskar Rao designs of block size five are :

i). $\lambda(v-1) \equiv 0 \pmod 4$

ii). $\lambda v(v-1) \equiv 0 \pmod{40}$

iii). $2|\lambda$.

We show these conditions are sufficient: for $\lambda = 4$ if $v > 215$, with 10 smaller possible exceptions and one definite exception at $v = 5$; for $\lambda = 10$ if $v > 445$, with 11 smaller possible exceptions, and one definite exception at $v = 5$; and for $\lambda = 20$, with the possible exception of $v = 32$; we also give a few results for other values of λ.

Key words and phrases: Bhaskar Rao Design (BRD), Supplementary Difference Set (SDS)
AMS 1991 *subject classifications*: Primary 05B30

1 Introduction

Bhaskar Rao designs (BRD) with elements $0, \pm 1$ have been studied by a number of authors including Bhaskar Rao [9, 10], Chaudhry and Seberry [11], de Launey [12], de Launey and Sarvate [13], de Launey and Seberry [15, 16], Gibbons and Mathon [18], Lam and Seberry [21], Palmer and Seberry [26], Seberry [28, 29], Singh [30], Street [32], Street and Rodger [31], and Vyas [33]. Bhaskar Rao designs have useful application in cryptographic functions and perfect hashing functions.

BRDs with block size three were studied by Singh [30], Vyas [33], and Seberry [28, 29]. For block size 3, the necessary conditions are sufficient for all elementary Abelian groups and all groups of order less than or equal 8. BRDs with block size four for Z_2 and all elementary Abelian groups were studied by de Launey and Seberry [15, 16]. See [14] for a recent survey. In this paper, we study the necessary conditions for Bhaskar Rao designs with block size five.

A *balanced incomplete block design* (BIBD) is an arrangement of v symbols in b blocks each containing $(k < v)$ symbols, satisfying the following conditions :

i). every symbol occurs at most once in a block,

ii). every symbol occurs in exactly r blocks,

iii). every pair of treatments or symbols occur together in exactly λ blocks.

The incidence matrix $N = (n_{ij})$ of a BIBD has entry one if symbol i is in block number j. The parameters (v, b, r, k, λ) of $BIBD$ satisfy:
(i) $vr = bk$ (ii) $\lambda(v-1) = r(k-1)$.
A *Bhaskar Rao design*, BRD(v, b, r, k, λ) is a matrix of order $v \times b$ with $(0, \pm 1$ entries), satisfying the following conditions :

i). the inner product of any pair of distinct rows is zero,

ii). when its non-zero entries are replaced by $+1$'s, the resulting matrix becomes the incidence matrix of a BIBD(v, b, r, k, λ).

In this paper, we will discuss Bhaskar Rao designs of block size five. We use the notations BIBD(v, k, λ) for BIBD(v, b, r, k, λ) and BRD(v, k, λ) for BRD(v, b, r, k, λ), omitting b and r as they are dependent on v, k, λ. In the examples, we write '$-$' for '-1'. The following example gives a BRD of block size five.

Example 1.1 There exists a BRD$(6, 5, 4)$ constructed from BIBD$(6, 5, 4)$.

BIBD$(6, 5, 4)$

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

BRD$(6, 5, 4)$

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{bmatrix}$$

In fact, a BRD$(k+1, k, k-1)$ exists whenever k is an odd prime power [17].

Theorem 1.2 (Bhaskar Rao [10]) *A necessary condition for the existence of BRD is that λ must be even.*

A *generalised Bhaskar Rao design*, GBRD$(v, b, r, k, \lambda; G)$, is a matrix of order $v \times b$ whose nonzero entries are drawn from the group G of finite order g so that

i). for any pair of distinct rows $(x_1, x_2, \ldots, x_b)$ and $(y_1, y_2, \ldots, y_b)$, the list $(x_1 y_1^{g-1}, x_2 y_2^{g-1}, \ldots, x_b y_b^{g-1})$ contains each nonzero group element exactly λ/g time.

ii). when its non-zero entries are replaced by $+1$'s, the resulting matrix becomes the incidence matrix of a BIBD(v, b, r, k, λ).

Clearly, we need $g|\lambda$, analogous to Theorem 1.2. A BRD is a GBRD where $g = 2$.

A *pairwise balanced design*, PBD(v, K, λ), of order v with block sizes from K, where K a set of positive integers, is a pair $(\mathcal{V}, \mathcal{B})$ where $\mathcal{V}$ is a finite set of cardinality v and $\mathcal{B}$ is a family of blocks of $\mathcal{V}$ which satisfies the properties:

i). If $B \in \mathcal{B}$, then $|B| \in K$

ii). Every pair of distinct elements of $\mathcal{V}$ occurs in exactly λ blocks of $\mathcal{B}$.

If $K = \{k\}$, then the PBD is a BIBD; we usually write $K = k$, rather than the more formal $k = \{k\}$ in this case.

A *group divisible design*, $\mathrm{GDD}_\lambda(K, G)$, of order v, where K a set of positive integers, is a triple $(\mathcal{V}, \mathcal{G}, \mathcal{B})$ where $\mathcal{V}$ is a finite set of cardinality v, $\mathcal{G}$ is a partition of $\mathcal{V}$ into groups $G_1, G_2, \ldots, G_s$, and the vector of group sizes $G = (|G_1|, |G_2|, \ldots, |G_s|)$ (often written in exponential notation) is known as the type of the GDD, and $\mathcal{B}$ is a family of blocks of $\mathcal{V}$ which satisfies the properties :

i). If $B \in \mathcal{B}$, then $|B| \in K$;

ii). Every pair of distinct elements of $\mathcal{V}$ occurs in exactly λ blocks or one group, but not both.

When the index is one, (i.e., $\lambda = 1$), the subscript is often omitted. A GDD with group type $G = 1^v$ is a PBD.

A *transversal design*, $\mathrm{TD}_\lambda(k, n)$, of order n, block size k, and index λ is a $\mathrm{GDD}_\lambda(k, n^k)$.

A *resolvable* design is a design whose block set admits a partition into parallel classes, or resolution sets, each of which contains every point exactly once. Resolvable designs are indicated by the prefix R.

A set of $k-1$ mutually orthogonal Latin squares, (or MOLS), of order n, a $\mathrm{RTD}(k, n)$ and a $\mathrm{TD}(k+1, n)$ are three equivalent combinatorial objects. A $\mathrm{RTD}(k, k)$ exists whenever k is a prime power. Note that if we have a $\mathrm{RTD}(k, n)$, we also have a $\mathrm{RTD}(k', n)$ for $k' < k$; (just throw away $k - k'$ of the MOLS).

We introduce a *Bhaskar Rao GDD*, a $\mathrm{BRGDD}_\lambda(K, G)$ of group type $G = (|G_1|, |G_2|, \ldots, |G_g|)$, is a matrix of order $v \times b$ with $(0, \pm 1$ entries), satisfying the following conditions :

i). the inner product of any pair of distinct rows is zero,

ii). when its non-zero entries are replaced by $+1$'s, the resulting matrix becomes the incidence matrix of a $\mathrm{GDD}_\lambda(K, G)$ of group type G.

BRGDDs with a uniform group size, signed over more general groups, were studied by Palmer under the name partial generalized Bhaskar Rao designs, in [25].

Theorem 1.3 (Seberry [28]) *A Bhaskar Rao design $BRD(v,k,\lambda)$ can only exist if the equation*

(i) $x_3 + 3x_5 + 6x_7 + ... + ((k^2-1)/8)x_k = b(k-1)/8$ *for k odd,*

(ii) $x_0 + 3x_4 + 8x_6 + ... + ((k^2-4)/4)x_k = b(k-4)/4$ *for k even,*

has integral solutions. In particular, for $k \equiv 3 \bmod 4$, a Bhaskar Rao design can only exist if $4|b$; for $k \equiv 0,1,4 \bmod 8$ no restriction is obtained; for $k \equiv 2,5,6 \bmod 8$ we must have $2|b$. Thus, for $k = 5$, $b/2$ must be an integer.

Theorem 1.4 *Suppose that the BIBD underlying a $BRD(v,k,\lambda)$ has λ identical blocks. If $k \geq 3$, then it is necessary that $\lambda \geq k$ and $4|\lambda$.*

Proof: Suppose the repeated block contains $(a,b,c,...)$, and suppose w.l.o.g. that all a's get $+$, then since half the (a,b) pairs have mixed sign, half the b's are $+$ and half $-$; (similarly the c's). Also half the (b,c) pairs have mixed sign. Now suppose there are x (b,c) pairs of type $(+1,+1)$; then there are $\lambda/2 - x$ mixed pairs with b positive, and the same number with c positive, hence $\lambda/2 = 2(\lambda/2 - x)$, which implies $4|\lambda$. Finally, consider the $k \times \lambda$ submatrix, M, within the signed incidence matrix that corresponds to these blocks. We have $MM^T = \lambda I$, which has rank k, and so therefore does M, and we cannot have a dimension smaller than the rank. ∎

Theorem 1.5 *A $BRD(k,k,4t)$ exists whenever a Hadamard design of order $4t$ exists, with $4t \geq k$.*

Proof: Take the first k rows of the Hadamard design as the BRD. ∎

Theorem 1.6 (de Launey [12]) *For all $k,t > 0$, there is an integer M such that if $2t(v-1)/(k-1)$ and $2tv(v-1)/k(k-1)$ are integers and $v > M$, then a $BRD(v,k,2t;Z_2)$ exists.*

2 General Constructions

We start by adapting some classical constructions to Bhaskar Rao type designs. The most useful is a generalization of Wilson's Fundamental Construction (WFC):

Theorem 2.1 *Suppose we have a master $GDD_\lambda(K', G)$ with group type $G = (|G_1|, \ldots, |G_s|)$. Suppose $w(x)$ is a positive weighting function defined for each point of the master design. For each block $B = \{b_1, \ldots, b_{k'}\}$, assume we have an ingredient $GDD_\mu(K, W(B))$ with group type $W(B) = (|w(b_1)|, \ldots, |w(b_{k'})|)$. Then there is a $GDD_{\lambda\mu}(K, W(G))$ with group type*

$$W(G) = \left(\sum_{x \in G_1} w(x), \ldots, \sum_{x \in G_s} \right).$$

Furthermore, if either the master design, or all the ingredient designs are BRGDDs, (or both), then so is the resultant design.

Proof: The proof of the basic WFC is available in, for example, [8, IX.3.2]; in our variant, again the resultant's K is not directly dependent on the master's K'. For the BRGDD version, suppose we are looking at a master block containing b_i with a sign of $g_1(b_i)$, and in a block of the appropriate ingredient design, we have $w_j(b_i)$ with a sign of $g_2(w_j(b_i))$, then in the resultant design we give the point a sign of $g_1(b_i) * g_2(w_j(b_i))$. ∎

Remark 2.2 This theorem can be generalized to BRGDDs over groups other than Z_2.

We next look at filling in the groups of the BRGDD. The first construction is usually applied to each group in turn.

Theorem 2.3 *Suppose we have a $BRGDD_\lambda(K, G)$ with group type G, where $G = (G_1, G_2, \ldots, G_s)$. Let $H = (H_1, H_2, \ldots, H_t)$, and $|G_1| = \sum |H_j|$; if we also have a $BRGDD_\lambda(K, H)$, then we have a $BRGDD_\lambda(K, F)$ with group type*

$$F = (|H_1|, |H_2|, \ldots, |H_t|, |G_2|, \ldots, |G_s|).$$

Theorem 2.4 *Let $\omega \geq 0$. Suppose we have a $BRGDD_\lambda(K, G)$ with group type $G = (|G_1|, |G_2|, \ldots, |G_s|)$, and for the i-th group (with $i > 1$), we have a $BRGDD_\lambda(K, H_i)$ with group type $H_i = (\omega, |H_{i1}|, |H_{i2}|, \ldots, |H_{it_i}|)$, and $|G_i| = \sum_j H_{ij}$; then we have a $BRGDD_\lambda(K, F)$ with group type*

$$F = (\omega + |G_1|, |H_1|, |H_2|, \ldots, |H_s|).$$

We can derive known results as corollaries of these constructions. We give an example:

Theorem 2.5 (Lam and Seberry [21]) *Let $w \in \{0, 1\}$. Suppose there exists a $BRD(v, k, \lambda)$ and $BRD(u + w, k, \lambda)$, further suppose there is a $TD(k, u)$; then there exists a $BRD(uv + w, k, \lambda)$.*

Proof: Take the $BRD(v, k, \lambda)$ as the master in the WFC, and give each point a weight of u. The TD provides the ingredient, and generates a $BRGDD_\lambda(k, u^v)$. Then use Theorem 2.4 with the $BRD(u + w, k, \lambda)$ providing a group type of 1^{u+w} to get the result. ∎

Remark 2.6 Actually, the original construction of Theorem 2.5 was weaker than our current version; they required a $TD(k + 1, u)$, only allowed $w = 0$, and got a larger final index.

Another derivable general construction is the following singular direct product construction:

Theorem 2.7 (de Launey and Seberry [15]) *Suppose there exists a $BRD(u, k, \lambda)$ with a subdesign on w points, a $BRD(v, k, \lambda)$ and $k - 2$ mutually orthogonal latin squares of order $u - w$. Then there exists a $BRD(v(u - w) + w, k, \lambda)$ with sub-designs on u, v and w points, ($w = 0, 1$ are allowed).*

Proof: Take the $BRD(v, k, \lambda)$ as the master design (with type 1^v) and give points a weight of $u - w$ in WFC, then use Theorem 2.4 to get the result. ∎

Remark 2.8 Actually, we do not need the $BRD(u, k, \lambda)$ to have a subdesign on w points, what we really need is a $\mathrm{BRGDD}_\lambda(k, 1^{u-w}w^1)$ to deal with all but one of the groups, and a type 1^u, (i.e., the BRD itself), for the final group. To give a concrete example of the distinction, we note that if $n \in$

$\{4, 6, 10, 12, 15, 18\}$, or $n > 103$ then there is a $BRGDD_4(5, 1^{10n}3^1)$. See [22, lemmas 112–118]; these BRGDDs are all derived from $GDD(5, 2^{10n}6^1)$. The cases $n = 4$ and 6 are constructed directly. The case $n = 18$ is generated by a $GDD(5, 10^9)$ with five parallel classes constructed by Abel; all the others are produced recursively. So we could take $u = 40$, $w = 3$, $\lambda = 20$, $v = 8$, $k = 5$ say; the point here is that clearly we can't actually have any $BRD(w, k, \lambda)$ since here $w < k$.

Theorem 2.9 (Seberry [28]) *Suppose there exists a $BRD(v, b, r, k, 4t)$, $k \leq 4t$ and $4t$ is the order of a Hadamard matrix and there exist $k-2$ mutually orthogonal latin squares of order k. Then there exists a $BRD(kv, 4tv + k^2b, kr + 4t, k, 4t)$.*

Proof: Use the BRD as the master design, giving points a weight of k, and the TD(k, k) as the ingredient, then fill the groups with a BRD$(k, k, 4t)$ formed from the first k rows of the Hadamard matrix. ∎

Remark 2.10 The original statement of the theorem omitted the condition $k \leq 4t$, although its use is apparent in the original proof, which is essentially the same construction as our proof. The original theorem also called for $k-1$ MOLS; since the order is k, this is a distinction which does not matter for any value of k, although we have stated $k-2$ to match the TD we have used.

Palmer [25] also has some constructions, which when restricted to signing over Z_2, are special cases of Theorem 2.1.

3 Signing Known Designs

The obvious way to construct BRDs is to take the underlying BIBD, and change the signs of the elements of its incidence matrix in some suitable way.

Lemma 3.1 *Suppose we have a partially signed $BIBD(v, k, \lambda)$ incidence matrix of the form $\begin{bmatrix} A \\ B \end{bmatrix}$ such that the rows of A are mutually orthogonal and the rows of B are also mutually orthogonal. Then $C = \begin{bmatrix} A & A \\ B & -B \end{bmatrix}$ is a $BRD(v, k, 2\lambda)$.*

Example 3.2 A BRD$(11, 5, 4)$ exists.

We note that if we change all the signs of any point, or of any block, then we will still preserve the orthogonality (or lack of it) for any pair of points. We take the unique BIBD(11,5,2) and commence to sign it, requiring the first element in each row and column to be $+1$. The signing of the first 5 rows is unique, and we can compatibly sign any one of the remaining rows, (row 6 in the example below), also in a unique way, however no pair of the compatibly signed last six rows is orthogonal, so make make row 6 orthogonal to the first 5, then start again. We have signed the last five rows in an orthogonal fashion, with $a, b \in \{\pm 1\}$; we can also easily check that it is not possible to sign row 6 in a way that makes the last six rows orthogonal. That we should encounter problems is to be expected, since, by Theorem 1.3, we know that we cannot sign a BIBD$(11, 5, 2)$. However since we have the first 6 columns mutually orthogonal, and the similarly the last five, so that we may apply Lemma 3.1 and get a BRD$(11, 5, 4)$.

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & - & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & - & 0 & 0 & - & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & - & 0 & 0 & - & 0 & - & 0 & 1 \\
1 & 0 & 0 & 0 & - & 0 & 0 & - & 0 & - & - \\
0 & 1 & - & 0 & 0 & 0 & 0 & 1 & - & 0 & - \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & - & 1 \\
0 & 0 & 1 & 0 & a & b & \bar{a} & 0 & 0 & 0 & \bar{b} \\
0 & 0 & 1 & \bar{a} & 0 & 0 & a & 1 & 0 & \bar{a} & 0 \\
0 & 0 & 0 & 1 & ab & - & 0 & a & a\bar{b} & 0 & 0
\end{bmatrix}$$

Example 3.3 A construction of an $RTD(8, 8)$ from the multiplication table of a $GF(2^3)$ where the table is indexed by zero an the powers of a root of the primitive equation $x^3 + x + 1 = 0$.

	0	x^0	x^1	x^2	x^3	x^4	x^5	x^6
0	000	000	000	000	000	000	000	000
x^0	000	001	010	100	011	110	111	101
x^1	000	010	100	011	110	111	101	001
x^2	000	100	011	110	111	101	001	010
x^3	000	011	110	111	101	001	010	100
x^4	000	110	111	101	001	010	100	011
x^5	000	111	101	001	010	100	011	110
x^6	000	101	001	010	100	011	110	111

To form the design append the row label to each element. Take each column as a base block, and develop over $Z_2 \times Z_2 \times Z_2$ for the RTD. Each base block generates a parallel class.

Theorem 3.4 *Let m and n be non-negative integers and q a prime with $k \leq q^{m+n+1}$. Then a $BRGDD_{q^{m+1}}(k, (q^n)^k)$ signed over $GF(q)$ exists.*

Proof: We proceed as in Example 3.3 to form the $RTD(q^{m+n+1}, q^{m+n+1})$, but we retain only the first k rows (thus forming a $RTD(k, q^{m+n+1})$). Now we use the first element of the $m+n+1$-tuple to "sign" the tuple with an element of Z_q, and we then ignore the next m elements, and only develop each of the last n elements over Z_q. (Conventionally, for Z_2, we can replace the first element 0 by a plus sign, and the first element 1 by a minus sign). ∎

Corollary 3.5 *The following designs exist:*

i). A $BRGDD_4(8, 2^8)$ and a $BRGDD_4(5, 2^5)$.

ii). A $BRGDD_2(8, 4^8)$ and a $BRGDD_2(5, 4^5)$.

iii). A $BRGDD_2(16, 8^8)$ and a $BRGDD_2(5, 8^5)$.

Theorem 3.6 *Suppose we have a $GDD_\lambda(k, G)$ with groups $G_1, \ldots, G_s$, such that $|G_i|$ is even for all i; then we have a $BRGDD_{4\lambda}(k, H)$ with group list $H = \{|G_i|/2 : 1 \leq i \leq s\}$.*

Proof: Replace the points $a_1, \ldots, a_{2t}$ in G_i by $b_1, \ldots, b_t$, substituting b_j in blocks containing a_{2j}, and substituting $-b_j$ in blocks containing a_{2j-1}. ∎

Remark 3.7 This theorem generalizes to "signings" over $GF(q)$ under the condition that q divides $|G_i|$, and with the initial GDD index of λ being multiplied by q^2 in the BRGDD.

Remark 3.8 An extension of the above, is that if the design was given by base blocks that are developed over the group, assuming now a uniform group size of $|G|$, then we may divide the resulting index by $|G|$.

This is a very useful construction, because it allows us to get designs with almost no effort from the literature.

Example 3.9 We take as an example a GDD$(5, 2^{61})$ developed over $Z_2 \times Z_{61}$ given in [34], and replace the Z_2 elements (0 by $+1$, 1 by -1) to get the base blocks $(0, 1, 4, 25, -11)$ and $(0, 8, 23, -25, -27)$; multiply these by 1, 13 and 47, (i.e., the cube roots in Z_{61}), to get 6 base blocks which when developed over Z_{61} yield a BRD$(61, 5, 2)$.

Theorem 3.10 *If $v \in \{41, 61, 81\}$, then there is a $BRD(v, 5, 2)$.*

Proof: See [34, Lemmas 2.1 and 2.7]; their constructions of a $GDD(5, 2^v)$ are by base blocks developed over $Z_2 \times Z_v$. ∎

Theorem 3.11 *If $p \equiv 1 \bmod 10$ is a prime and $41 \leq p \leq 1151$, then there is a $GDD(5)$ of type 4^p constructed from a (block-disjoint) base blocks over $GF(4) \times Z_p$.*

Proof: See [6, Table 2.1, Theorem 2.2]. ∎

Corollary 3.12 *If $p \equiv 1 \bmod 10$ is a prime and $41 \leq p \leq 1151$, then there is a $BRGDD_2(5, 2^p)$ of type 2^p.*

Proof: Converting $GF(4)$ into a signed $GF(2)$ increases the index to 4, but we may halve this since we had developed over $GF(4)$ and now only develop over $GF(2)$. ∎

We begin by presenting a standard construction for $AG(2,q)$ where q is a prime power, (see e.g., [20, Theorem 2.1]. Let x be a primitive element for $GF(q)$.

$$\begin{aligned}
\mathcal{P} &= GF(q) \times GF(q) \\
\\
G &= \{(0,0)(0,x^0)(0,x^1)\ldots(0,x^{q-2})\} \bmod (q,-) \\
C &= \{(0,0)(x^0,0)\ldots(x^{q-2},0)\} \bmod (-,q) \\
B_\alpha &= \{(0,0)(x^0,x^\alpha)(x^1,x^{\alpha+1})\ldots(x^q-2,x^{\alpha+q-2})\} \bmod (-,q) \\
\\
\mathcal{B} &= \mathrm{dev}(G) \cup \mathrm{dev}(C) \cup \textstyle\bigcup_{\alpha=0}^{\alpha=q-2} \mathrm{dev}(B_\alpha)
\end{aligned}$$

We now adapt a construction of Wilson's, quoted in [19, Theorem 15.7.4], to produce BRGDDs.

Theorem 3.13 *A $BRGDD_2(q,t^{q+1})$ exists whenever $q = 2t+1$ is an odd prime power.*

Proof: We perform a signed replacement in the above $AG(2,q)$, replacing the second element x^j by x^{j-t} if $t \leq j < 2t$ and giving the point a negative sign, and omitting all points whose second element is zero, and giving the remaining points a positive sign. We also discards all the type $|G|$ blocks, (which contain all the doubleton of the new points), and these now define the groups, so (finite) points are in the same group iff they have the same first element. Let us now examine when the $(++)$ pair (x^a,x^j) with (x^b,x^k) occurs, (assuming $j \neq k$, and $j,k < t$). If this happens in $B_\alpha + d$, then we have

$$\begin{aligned}
x^j &= x^{\alpha+a} + d \\
x^k &= x^{\alpha+b} + d
\end{aligned}$$

so we have

$$\begin{aligned}
x^j - x^k &= x^\alpha(x^a - x^b) \\
d &= x^j - x^{\alpha+a}
\end{aligned}$$

Now, by a similar calculation, (noting that $x^{j+t} = -x^j$ in $GF(q)$), the $(--)$ pair will occur occur in $B_{\alpha+t} + x^t d$, and if $d = -x^{\alpha+c}$ then the missing

element from the deleted zeros, will be $(x^c, 0)$ in both cases. Similarly, we can (using new α and d) find that the $(+-)$ pair occurs when

$$\begin{aligned} x^j + x^k &= x^\alpha(x^a - x^b) \\ d &= x^j - x^{\alpha+a} \end{aligned}$$

and again, the $(-+)$ pair occurs in $B_{\alpha+t} + x^t d$, and again the two blocks have a common missing element. Next, for the pairs with $(0, x^j)$ we have $x^k - x^j = x^{\alpha+b}$, for the $(++)$ pair, and again the $(--)$ pair occurs in $B_{\alpha+t} + x^t d$, and similarly the mixed sign pairs with $x^k + x^j = x^{\alpha+b}$, for the $(-+)$ pair. If we have $j = k$, then it can be checked that we have no same sign solutions in the B_α type blocks, although these can be obtained from $C + x^j$, $C + x^{j+t}$.

To summarise what we have done so far; we removed the parallel class $\mathrm{dev}(G)$ to provide groups, then did a 2 to 1 collapsing of points within a group, (if we ignore the signs for now), which normally inflates the index by 4, but we have shown that the cyclotomic way we collapsed the points allows us to identify doubles of each of the blocks in the design, so we only need increase the index by 2, not 4. More generally, Wilson showed if $q = ef + 1$ is a prime power, we can get a $\mathrm{GDD}_e(k, f^{q+1})$ by collapsing along cyclotomic lines. Furthermore, the signs are properly balanced in each half, so we have a BRGDD, but, so far, we have mixed block sizes, since all the B_α type blocks have lost a point, and the C type blocks remain intact (but C did lose a whole block). Each original point occurred once in $\mathrm{dev}(B_\alpha)$ for each α, so it has each new point twice, once with each sign, so that we can add a group of t (positive) infinite elements to the design, adding ∞_α to $\mathrm{dev}(B_\alpha)$ to get our BRGDD. ∎

Since this is a symmetric design, (i.e., $v = b$), it is also a weighing matrix, which yields the following corollary.

Corollary 3.14 *If p is an odd prime power, a $W((p^2-1)/2, p)$ exists.*

Corollary 3.15 *A $BRGDD_2(5, 2^6)$ exists.*

There is a related result which we wish to mention. We do not know precisely what the relation is, but think it is something that might be studied with profit.

Theorem 3.16 *If $p = ef + 1$, then complements of Desarguesian projective geometries of order p are cyclic e-signable. In particular if $e = 2$, then the circulant weighing matrix $W((p^{n+1} - 1/(p-1), p^n)$ exists for $n > 1$.*

Proof: See [27, Theorem 5.8]. ∎

We next look at difference family constructions. Let $S_1, \ldots, S_n$ be the subsets of V, a finite abelian group of order v written in additive notations, each containing k elements. Write T for the totality of all differences between elements of S_i with repetitions. If T contains each non-zero element of V a fixed number of times, λ say, then the sets $S_1, \ldots, S_n$ are called $n - (v, k, \lambda)$ *supplementary difference sets* (SDS). The parameters of $n - (v, k, \lambda)$ SDS satisfy the condition: $\lambda(v-1) = nk(k-1)$. We also consider one-rotational difference families over a finite Abelian group of order $v-1$, with an additional fixed point, (∞); in this case there are $\rho = \lambda/(k-1)$ sets containing ∞, and the parameters of the $n - (v, k, \lambda)$ SDS satisfy $\lambda v = nk(k-1)$.

When the signs of some of the elements of S_i are changed such that number of positive and negative differences in T are equal, then $n-(v, k, \lambda)$ SDS is a BRD(v, k, λ). We note that half the differences should be of mixed sign, (including those differences with a fixed element, if present). This fact provides some useful information on the possible signing patterns for a SDS.

Example 3.17 Consider how we might construct a BRD$(6, 3, 4)$ using some SDS. This design has 20 blocks, which suggests we use Z_{v-1} since Z_v would require some short orbits, which complicates things somewhat. (Here it looks like it just complicates things, but it can make the construction impossible, bearing Theorem 1.4 in mind.) Next, we see that we need 4 mixed differences amongst the 8 differences in the 5 finite elements,and also two finite elements of each sign in the base blocks containing ∞, (signing ∞ positively). If we take 2 copies of the one-rotational $2-(6, 3, 2)$ SDS: $(\infty, 0, 1)(0, 2, 4)$, then we only have two options here; either we mix signs on the two infinite blocks, or we don't. In this case both yield solutions:

$$\begin{array}{lllll} (\infty, 0, 1) & (\infty, -0, -1) & (0, 2, -4) & (0, 2, -4) & (\text{mod } 5) \\ (\infty, 0, -1) & (\infty, 0, -1) & (0, -2, 4) & (0, 2, 4) & (\text{mod } 5) \end{array}$$

Later, we will give several examples of signing SDSs into BRDs.

4 BRDs of block size five

Theorem 4.1 *For the existence of a BIBD(v,k,λ), the necessary conditions are :*

i). $\lambda(v-1) \equiv 0 \pmod{k}$

ii). $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$

In the case that $k = 5$, these conditions are sufficient with the exception of the non-existent BIBD$(15,5,2)$.

In the case that $k = 6$ and $\lambda > 1$, these conditions are sufficient with the exception of the non-existent BIBD$(21,6,2)$. In the case that $k = 6$ and $\lambda = 1$, these conditions are sufficient with with possible exception of $BIBD(v,6,1)$ for the 36 values of v in Table 4.1 below, (and where the values there with $v \leq 36$ are definite exceptions).

Proof: For $k = 5$, and $k = 6$ with $\lambda > 1$, see Hanani [20]. For BIBD$(v,6,1)$, the list is an updated version of [5, I.2.5] provided by Abel [2]. ∎

Table 4.1

Possible BIBD$(v,6,1)$ exceptions

(16)	(21)	(36)	46	51	61	81	166	226	231
256	261	286	291	316	321	346	351	376	406
411	436	441	471	496	501	526	561	591	616
646	651	676	771	796	801				

Theorem 4.2 *For the existence of a BRD$(v,5,\lambda)$, the necessary conditions are:*

i). $\lambda(v-1) \equiv 0 \pmod{4}$

ii). $\lambda v(v-1) \equiv 0 \pmod{20}$

iii). $\lambda \equiv 0 \pmod{2}$

Condition (iii) can be replaced by $\lambda v(v-1) \equiv 0 \pmod{40}$. *Furthermore, if $v = 5$ we must have $\lambda \equiv 0 \bmod 4$, with $\lambda > 4$.*

For $BRD(v, 5, \lambda)$, these conditions imply the following:

Table 4.2

λ	condition on v
2	$v \equiv 1$ or 5 mod 20, with $v > 5$
4	$v \equiv 0$ or 1 mod 5
10	$v \equiv 1$ mod 4, with $v > 5$
20	any $v \geq 5$

Lemma 4.3 *A $BRD(5, 5, \lambda)$ exists iff $\lambda \equiv 0$ mod 4 with $\lambda \geq 8$.*

Proof: This essentially is a corollary of Theorems 1.4 and 1.5, noting that Hadamard matrices of order 8 and 12 exist. ∎

Theorem 4.4 *If a $BIBD(v, 5, \lambda)$ exists, then a $BRD(v, 5, 4t\lambda)$ exists for any $t > 1$.*

Proof: Take the BIBD as the master design in WFC, give each point a weight of 1, and use the BRD of Lemma 4.3 as the ingredient design. In this case, this construction just amounts to replacing each block by the BRD$(5, 5, 4t)$ whose point set equals the points of the block. ∎

Remark 4.5 Unfortunately, this general construction gives designs with λ's that are too large; in fact, the only case of use is for $v = 35$, where we failed to find either a BRD$(35, 5, 4)$ or a BRD$(35, 5, 8)$, but via the BIBD$(35, 5, 2)$, have BRD$(35, 5, \lambda)$ for $\lambda = 16, 24$.

Theorem 4.6 *If a $BIBD(v, 6, \lambda)$ exists, then a $BRD(v, 5, 4\lambda)$ exists.*

Proof: Take the BIBD as the master design in WFC, give each point a weight of 1, and use the BRD$(6, 5, 4)$ of Example 1.1 as the ingredient design. In this case, this construction just amounts to replacing each block by the BRD$(6, 5, 4)$ whose point set equals the points of the block. ∎

We will deal now with BRD$(v, 5, 20)$. The necessary conditions do not restrict v except that $v \geq 5$. We will first need a corollary to Theorem 4.6.

Corollary 4.7 *If $v \equiv 0$ or $1 \bmod 3$, and $v \geq 6$, then a $BRD(v, 5, 20)$ exists.*

We next need a preliminary lemma on pairwise balanced designs taken from [7, III.3.2].

Lemma 4.8 *If $v > 34$ or $v = 26$, then a $PBD(v, \{5, 6, 7, 8, 9\}, 1)$ exists.*

Corollary 4.9 *If $v > 34$ or $v = 26$, a $BRD(v, 5, 20)$ exists.*

Proof: Apply theorem 2.1 with the PBD as the master design, with each point of the BIBD receiving weight 1. Use $BRD(v', 5, 20)$ for the ingredient designs, where these are given by Lemma 4.3 for $v' = 5$, by Corollary 4.7 for $v' = 6, 7, 9$ and by Example 7.2 for $v' = 8$. ∎

Theorem 4.10 *If $v \geq 5$ and $v \neq 32$, a $BRD(v, 5, 20)$ exists.*

Proof: By Corollary 4.7, we only have to deal with the 2 mod 3 values in the range 10 through 34 except 26. Constructions for $v = 11$, 14, 17, 20 are given in Examples 3.2, 7.5, 7.8 and 7.9. For $v = 23$: use a BIBD(23,11,5) (from [23, I.1.3]) as the master design with weight 1 in WFC, with a BRD(11,5,4) as ingredient, to get a BRD(23,5,20). For 29, we have a $\mathrm{BRGDD}_2(8, 4^8)$ by Theorem 3.4; removing a group gives a $\mathrm{BRGDD}_2(7, 4^7)$ of type 4^7. Using this as the master in WFC with weight 1 and a BIBD(7,5,10) as ingredient gives a $\mathrm{BRGDD}_{20}(5, 4^7)$ of type 4^7. Fill the groups with an extra point and BRD$(5, 5, 20)$'s. ∎

Theorem 4.11 *A $BRD(32, 5, 20t)$ exists for all $t > 1$.*

Proof: It suffices to establish this for $\lambda = 40$ and 60. For $\lambda = 40$, a BRD$(31, 4, 2)$ exists [15, Theorem 4.1.1]; adjoin $-\infty$ to one copy of this BRD, and $+\infty$ to another copy; add 9 copies of the blocks of a BRD$(31, 5, 4)$. For $\lambda = 60$, use a BIBD$(32, 6, 15)$ from Theorem 4.1, in Theorem 4.6. ∎

5 BRD$(v, 5, 4)$

The other value that the existence of BIBDs with $k = 6$ helps us with is $\lambda = 4$, but this only covers about one third of the values, and misses most of the smaller, more useful designs (it gives us $v = 31$, 66, 76, 91, etc.). The other small (≤ 45) BRD$(v, 5, 4)$ are $v = 6$ in Example 1.1, $v = 11$ in Example 3.2, $v = 25, 45$ in Theorem 5.1, and $v = 10$, 20, 21, 30, 31, 40, 41 given in Section 7.

The necessary condition for the existence of a $BRD(v, 5, 4)$ is that $v \equiv 0$ or 1 mod 5. The object of this section is to show this condition is sufficient, with the possible exception of 10 values of v, and the definite exception of $v = 5$. In order to do this, we exploit a number of previously constructed designs of various types that are available in the literature.

Theorem 5.1 *Define* $E = \{5, 11, 15, 35, 71, 75, 85, 95, 111, 115, 135, 195, 215, 335\}$. *If* $n \equiv 1, 5 \bmod 10$ *and* $n \notin E$, *then there is a* $GDD(5, 2^n)$.

Proof: See [34, Theorem 1.2]. ∎

Corollary 5.2 *Define* $E = \{5, 11, 15, 35, 71, 75, 85, 95, 111, 115, 135, 195, 215, 335\}$. *If* $v \equiv 1, 5 \bmod 10$ *and* $v \notin E$, *then there is a* $BRD(v, 5, 4)$.

Proof: Essentially this is an application of Theorem 3.6 to Theorem 5.1. ∎

Theorem 5.3 *If* $q \geq 5$, *then there is a* $GDD(5, 20^q)$.

Proof: See [34, Theorem 1.2]. ∎

Corollary 5.4 *If* $q \geq 5$, *then there is a* $BRGDD(5, 10^q)$, *and a* $BRD(v, 5, 4)$ *exists for any* $v \equiv 0, 1 \bmod 10$ *if* $v \geq 50$.

Proof: The BRGDD follows by Theorem 3.6 and the BRD follows from Theorem 2.4. ∎

Remark 5.5 ¿From [3, II.2.73], if $m \geq 5$, and $m \notin \{6, 10, 14, 18, 22\}$, then a $TD(6, m)$ exists, and if $m \neq 10$, then a $TD(5, m)$ exists.

Theorem 5.6 *If a TD*$(5, 2m)$ *exists, then a BRGDD*$_4(5, m^5)$ *exists. If furthermore, a BRD*$(m+w, 5, 4)$ *exist for some* $w \in \{0, 1\}$*, then a BRD*$(10m/2+w, 5, 4)$ *exists.*

Proof: We collapse points using Theorem 3.6 to get the BRGDD, then use Theorem 2.4 to fill the groups in with the aid of w new points. ∎

Corollary 5.7 *A BRGDD*$(46, 5, 4)$ *and a BRGDD*$(146, 5, 4)$ *exist.*

Proof: Let $m = 9$, $w = 1$, or $m = 29$, $w = 1$ in Theorem 5.6. ∎

Theorem 5.8 *If a TD*$(6, m)$ *exists and* $0 \leq n \leq m$*, then a GDD*$(\{5, 6\})$ *of type* m^5n^1 *exists. If furthermore, a BRD*$(2m+w, 5, 4)$ *and a BRD*$(2n+w, 5, 4)$ *both exist for some* $w \in \{0, 1\}$*, then a BRD*$(10m + 2n + w, 5, 4)$ *exists.*

Proof: Truncate one group of the TD to size n to get the GDD. Use this as the master design in Theorem 2.1 with all points getting a weight of 2. Finally, add w new points, and fill in the groups with the BRDs. ∎

Corollary 5.9 *A BRGDD*$(236, 5, 4)$ *exists.*

Proof: Let $m = 23$, $n = 3$, $w = 0$ in Theorem 5.8. ∎

Lemma 5.10 *A BRGDD*$(36, 5, 4)$ *exists.*

Proof: Use a BRGDD$_2(5, 2^6)$ as the master design. In Theorem 2.1, give each point a weight of 3, and use a TD$_2(5, 3)$ from [20, Theorem 3.11] as the ingredient, to get a BRGDD$_4(5, 6^6)$, which can be filled with a BRD$(6, 5, 4)$ by Theorem 2.3. ∎

Theorem 5.11 *Let* $v = 20t + 5$*. If* $v \notin \{45, 225, 345, 465, 645\}$ *(i.e.,* $t \notin E = \{2, 11, 17, 23, 32\}$*), then a RBIBD*$(v, 5, 1)$ *exists.*

Proof: See [6], updated in [4]. ∎

Corollary 5.12 *Let* $n \leq 5t$*, and* $t \notin \{2, 11, 17, 23, 32\}$*, and* $w \in \{0, 1\}$*. If a BRD*$(2n + w, 5, 4)$ *exists, then a BRD*$(40t + 10 + 2n + w, 5, 4)$ *exists.*

Proof: We take the RBIBD$(20t+5, 5, 1)$, and remove a parallel class to provide $4t+1$ groups of size 5, then add new points to n of the remaining parallel classes, to give a GDD$_1(\{5,6\}, 5^{4t+1}n^1)$. We use this as the master design in WFC, and give every point a weight of 2, thus a BRGDD$_4(5, 10^{4t+1}2n^1)$ exists, using ingredient designs from Corollary 3.5 or Example 7.15. We then fill the groups, using w new points and Theorem 2.4. Note that a BRD$(10+w, 5, 4)$ exists by Example 7.3 or 3.2. and for the i-th group, G_i, we add the blocks of a BRD$(|G_i|+w, 5, 4)$ on the points G_i and w; doing this for every group yields the required BRD. ∎

Corollary 5.13 *A $BRD(v, 5, 4)$ exists for $v \in \{195, 335\}$.*

Proof: Take $t = 4$, $n = 12$ and $w = 1$, or $t = 7$, $n = 22$ and $w = 1$ in Corollary 5.12. ∎

We now use this corollary to construct some $BRD(v, 5, 4)$s for the $v \equiv 6 \bmod 10$ cases, noting that we already have BRD$(v, 5, 4)$'s for $v = 6$, 10, 11, 20, 30, 31, 36, 40, 46, 66, 76.

mod 40	n	w	first t	$2n+w$	first v	Later exceptions
6	18	0	4	36	206	(486),(726),(966),(1326)
16	3	0	1	6	56	(96),(456),(696),(936),(1296)
26	28	0	6	56	306	506,746,986,1346
	48	0	10	96	506	(546),(786),(1026),(1386)
36	33	0	7	66	356	(516),(756),(996),(1356)

The parenthesised exceptions are all v for which a BIBD$(v, 6, 1)$ exists. A BIBD$(v, 6, 1)$ also exists for $v = 66$, 76, 106, 126, 156, 186, 196, 276. For these values a BRD$(v, 5, 4)$ exists by Theorem 4.6. We have given two constructions for the 26 mod 40 case, so the exceptions from one can be covered by the other.

Lemma 5.14 *If $v \in \{115, 116, 166, 206, 226, 266, 316\}$, then there exists a $PBD(v, \{6, 10, 11, 20, 21, 31, 41\}, 1)$, and consequently a $BRD(v, 5, 4)$ exists.*

Proof: For $v = 116$: delete 5 collinear points of $AG(2, 11)$. For $115 = 6 * 19 + 1$: fill a $TD(6, 19)$ with an extra point. For $v = 166$, 226, 266:

see [6, Lemma 3.2] For $v = 206$: complete the RBIBD$(165, 5, 1)$ to give a $PBD(\{6, 41\}$. For $316 = 10 * 31 + 6$: truncate a group of a $TD(11, 31)$. ∎

The following theorem is the main result of this section.

Theorem 5.15 *If $v \equiv 0, 1 \bmod 5$, then a $BRD(v, 5, 4)$ exists with the definite exception of $v = 5$, and the possible exception of 10 further values of v, the largest of which is 215. These values are given in Table 5.1.*

Table 5.1

Table of v with $BRD(v, 5, 4)$ unconstructed.

(5)	15	16	26	35	75	85	86	95	135	215

We next address the existence of BRD$(v, 5, \lambda)$ for these exceptional values of v with $\lambda > 4$.

Lemma 5.16 *If $v \equiv 0, 1 \bmod 5$ and $v \notin \{10, 11, 15, 16, 20, 35, 40, 50, 51, 80\}$, then a $PBD(v, \{5, 6\}, 1)$ exists.*

Proof: See [7, III.3.17]. ∎

Lemma 5.17 *If $v \equiv 0, 1 \bmod 5$ and $v \notin \{15, 16, 35\}$, then a $BRD(v, 5, 4t)$ exists for all $t > 1$.*

Proof: Since we a $BRD(5, 5, 4t)$ exists for all $t > 1$, and a $BRD(6, 5, 4)$ exists, the result follows from Lemma 5.16, after removing from the exception set there those v for which we have constructed a $BRD(v, 5, 4)$. ∎

Theorem 5.18 *If $v \equiv 0, 1 \bmod 5$, then a $BRD(v, 5, 4t)$ exists for all $t > 1$, with the possible exception of $BRD(15, 5, 12)$, $BRD(35, 5, 8)$, $BRD(35, 5, 12)$, $BRD(35, 5, 28)$.*

Proof: We have a BRD$(v, 5, 20)$ by Theorem 4.10. We have a BRD$(15, 5, 8)$ by Example 7.6. Using the BIBD$(16, 6, t)$ for all $t > 1$, given by Theorem 4.1, we have, by Theorem 4.6, that a BRD$(16, 5, 4t)$ exists for all $t > 1$. Using the BIBD$(35, 5, 2)$ given by Theorem 4.1, and so a BRD$(35, 5, 16)$, and a BRD$(35, 5, 24)$ by Theorem 4.4. ∎

6 BRD$(v, 5, 10)$

In this section, we examine the case of $\lambda = 10$. The key basic construction is Theorem 7.1, where BRD$(v, 5, 10)$ are constructed for all prime powers, $v > 5$, with $v \equiv 1 \bmod 4$.

Lemma 6.1 *There exists a PBD$(v, \{9, 13, 17, 37\}, 1)$, and consequently a BRD$(v, 5, 10)$ exists, for $v \in \{117, 145, 333\}$.*

Proof: For the PBD$(145, \{9, 17\}, 1)$, fill in the groups of a TD$(9, 16)$ with an extra point. For the remaining values, fill in the groups of a TD$(9, n)$. The BRD result follows from Theorem 2.1, with the PBD as the master design, and with all points getting weight 1. ∎

Lemma 6.2 *If $n \in \{5, 6\}$, then:*

i). A BRGDD$_2(5, 4^n)$ exists;

ii). and a BRGDD$_2(5, 8^n)$ exists.

Proof: For either group size, with $n = 5$, we use one of the BRGDDs given in Corollary 3.5 For $n = 6$, take the BRGDD$_2(5, 2^6)$ given in Corollary 3.15 as the master design in Theorem 2.1, and give each point a weight of four, with the ingredient design as a TD$(5, 4)$, or else use the BRGDD$_2(5, 4^6)$ given in Example 7.16. ∎

Lemma 6.3 *A GDD$(5, n^{4t+1})$ exists for $n \in \{5, 15\}$ for all t.*

Proof: See [34]. ∎

Lemma 6.4 *A BRD$(v, 5, 2)$ exists whenever:*

i). $v \equiv 41 \bmod 160$.

ii). $v \equiv 61 \bmod 240$.

iii). $v \equiv 81 \bmod 320$.

Proof: Use the GDD given in Lemma 6.3 as the master design in Theorem 2.1, and give each point in 5-groups weight of 8 or 16, and give each point in 15-groups weight of 4. Use Corollary 3.5 to give the needed ingredient design, and fill this design with BRDs using an additional point and Theorem 2.4, with the filling designs from Theorem 3.10. ∎

Lemma 6.5 *A BRD*$(v, 5, 10)$ *exists for* $v \in \{161, 321, 545\}$.

Proof: For $v = 161$, 321; remove all the blocks through a point, and use these to define groups of a GDD$(5, 4^n)$ for $n = 10$, 20. use this as the master design in WFC, and give each point a weight of 4, then fill the groups using a BRD$(17, 5, 10)$, with an extra point and Theorem 2.4. Similar to Corollary 5.12, remove a parallel class, and add 3 points to a RBIBD$(65, 5, 1)$ to get a GDD$(\{5, 6\}, 5^{13}3^1)$, then give each point a weight of 8 in WFC, use the ingredients of Lemma 6.2 to give a BRGDD$_2(5, 40^{13}24^1)$, and then fill the groups. ∎

Lemma 6.6 *The following BRD*$(v, 5, 10)$ *designs with a BRD*$(u, 5, 10)$ *subdesign exist:*

i). $u \in \{9, 17\}$ *and* $v = 145$.

ii). $u = 9$ *and* $v \in \{41, 49\}$;

iii). $u = 13$ *and* $v \in \{61, 69, 73\}$;

iv). $u = 17$ *and* $v \in \{81, 97\}$.

Proof: the case $v = 145$ follows from Lemma 6.1. For $v = 5(u-1)+1$, use a BRGDD$_2(5, 4^5)$ as the master design, and give each point a weight of $w = (v-1)/20$, and use a TD$_5(5, w)$ as the ingredient design, then fill with the aid of one additional point. The subdesign is the last filling design. For $v = 6(u-1)+1$, use a BRGDD$_2(5, 2^6)$ as the master design, and give each point a weight of $w = (v-1)/12$, and use a TD$_5(5, w)$ as the ingredient design, then fill with the aid of one additional point. The subdesign is the last filling design. For the BRD$(69, 5, 10)$; this is constructed using Theorem 6.7 below, by filling the groups of a BRGDD$_{10}(5, 12^5 8^1)$ with an additional point. we can take one of these filling designs as the subdesign. ∎

Theorem 6.7 *Suppose a BRD*$(4m+1,5,1)$ *and a BRD*$(4n+1,5,1)$ *both exist, and* $t = 5m+n$, *with* $0 \le n \le m$; *then there exists a BRD*$(4t+1,5,10)$.

Proof: Truncate one group of a $\mathrm{TD}_5(6,m)$ to size n, and use this as the master design in Theorem 2.1, giving points weight 4. This TD exists for all m by [20, Theorem 3.11]. Use the BRGDDs of Lemma 6.2 as the ingredient designs to get a $\mathrm{BRGDD}_{10}(5,(4m)^5(4n)^1)$, and fill this design with BRDs using an additional point and Theorem 2.4. ∎

Corollary 6.8 *A BRD*$(4t+1,5,10)$ *exists for* $t \in \{44,46,50,53,76,86\}$.

Proof: For this variant of Theorem 6.7, we fill the designs with the aid of u additional points, where we have a $\mathrm{BRD}(4m+u,5,10)$ containing a $\mathrm{BRD}(u,5,10)$ subdesign, and a $\mathrm{BRD}(4n+u,5,10)$ design exists. We take $m = 8$ with $u = 9$, $m = 12$ with $u = 13$, $m = 14$ with $u = 13$, or $m = 16$ with $u = 17$ to get the above constructions, where the BRDs with subdesigns follow from Lemma 6.6. ∎

Theorem 6.9 *If* $v = 4t+1 > 445$, *then a BRD*$(v,5,10)$ *exists. For smaller* v, *there are at most 12 possible exceptions, as given in Table 6.1, with* $v = 5$ *being a definite exception.*

Table 6.1

t	(1)	5	8	11	14	16	19	21	26	61
$4t+1$	(5)	21	33	45	57	65	77	85	105	245

t	101	111
$4t+1$	405	445

Proof: The existence of $\mathrm{BRD}(v,5,10)$ is established by application of Theorem 6.7, using the construction of Theorem 7.1 to deal with prime power cases, and with the help of Lemmas 6.1, 6.5 and Corollary 6.8. (The non-existence result for $v = 5$ was given in Lemma 4.3). For the larger values of $t > 111$, take $n \in \{15,36,7,18,9\}$ in Theorem 6.7, and let $v = 4t+1$ with $t = 5m+n$; if m is not valid, then try using $m+1$ and $n-5$. This deals

with all values of $t \geq 108$, except for $t \equiv 1 \bmod 5$. For these values we may use $n \in \{6, 31\}$, and deal with all values of $5m + n > 111$, except 136, which is covered by Corollary 6.8. The smaller values of t, (i.e., $t \leq 111$), can be easily checked. ∎

7 Construction of BRDs

In this section we will give examples of Bhaskar Rao designs constructed from SDS's, some of which have been used in proofs of sections 4 and 5. We first look at some simple non-existence results for signed SDS via counting arguments, and start by examining possible parameter sets of interest.

Table 7.1

v	b	r	k	λ	$\lvert G\rvert$	ρ	Number of finite pairs in SDS
$20t+1$	$2tv$	$10t$	5	2	v	0	$20t$
$20t+5$	$(4t+1)(10t+2)$	$10t+2$	5	2	?	?	?
$10t$	$2tv$	$10t-1$	5	4	v	0	$20t$
$10t+1$	$2tv$	$10t$	5	4	v	0	$20t$
$10t+5$	$(2t+1)(v-1)$	$10t+4$	5	4	$v-1$	1	$20t+6$
$10t+6$	$(2t+1)v$	$10t+5$	5	4	v	0	$20t+10$
$4t+1$	$2tv$	$10t$	5	10	v	0	$20t$
$t+1$	tv	$5t$	5	20	v	0	$10t$
$t+1$	$(t+1)(v-1)$	$5t$	5	20	$v-1$	5	$10t-10$

Now we consider the ρ blocks containing a fixed element (which we will consider to be of constant sign); suppose there are x_i blocks containing i positive elements with ∞. Suppose these ρ blocks contribute M mixed sign pairs in total. Then:

$$\begin{aligned} \rho(k-1)/2 &= \sum ix_i \\ M &= \sum i(k-1-i)x_i \end{aligned}$$

Now adding these gives $M + 2\rho = \sum i(k-i)x_i$, and since k is odd, $i(k-i)$ is always even, so M is even, whatever (valid) pattern of signing we pick. Also, for blocks that do not have a fixed point, we have $i(k-i)$ which is always even, so we must always have an even number of mixed sign pairs, and thus the total number of finite pairs in the SDS must be a multiple of 4. This eliminates $(v, 5, 4)$ SDS for $v \equiv 1$ or 5 mod 10, (at least using full orbits over Z_v or Z_{v-1}) for these cases (and all their odd multiples), and determines that for $(v, 5, 20)$ we should look at Z_{v-1} if v is even, and Z_v if v is odd. Also, $(20t + 5, 5, 2)$ is not an option with these groups.

We next consider a signed SDS for BRD$(4t + 1, 5, 10)$ in the case that $4t + 1 = q$ is a prime power. Let x be a primitive element for $GF(q)$.

$$\begin{aligned} \mathcal{P} &= GF(q) \\ \\ B_\alpha &= \{0, -x^\alpha, x^{\alpha+2t}, bx^\alpha, -bx^{\alpha+2t}\} \pmod q \\ C_\alpha &= \{0, x^\alpha + 1, x^{\alpha+2t+1}, bx^{\alpha+1}, -bx^{\alpha+2t+1}\} \pmod q \\ \\ &= \qquad \text{for } \alpha = 0, 2, 4, \ldots, 2t-2 \end{aligned}$$

The signed differences arising from B_0 and C_0 are:

± 1	$+-$	$\pm b$	$+-$	$\pm(b+1)$	$++$	$\pm(b-1)$	$--$	± 2	$-$	$\pm 2b$	$-$
$\pm x$	$++$	$\pm bx$	$+-$	$\pm(b+1)x$	$+-$	$\pm(b-1)x$	$+-$	$\pm 2x$	$+$	$\pm 2bx$	$-$

The unbalanced elements are $\pm x$ and $\pm(b+1)$, both with $(++)$, and $\pm(b-1)$ and ± 2, both with $(--)$. (If b is square, $\pm 2x$ will be balanced by $\pm 2bx$, and by $\pm 2b$ otherwise). We can usually achieve balance by a careful choice of b; solutions were found for all prime powers through 125, (except 5 of course). It is easy to see that a solution must exist, at least for $q = 4t + 1 > 5$: if ± 2 is a square, we require that $b + 1$ be a square, and $b - 1$ not be a square, so $b^2 - 1$ is not a square; there are t values of b for which $b^2 - 1$ is not a square (see [19, p. 178]), so either we have what we want, or else we have a value b' such that $b' + 1$ is not a square, and $b' - 1$ is; in this case $b = -b'$ is our solution. Alternatively, if ± 2 is not a square, then it will cancel out the $\pm x$ signs, and we need $b - 1$ and $b + 1$ to be of the same quadratic character, (i.e., $b^2 - 1$ is a square), so that they will cancel each other out; there are $t - 1$ such values of b^2, and so $2t - 2$ possible values of b; (and no solutions for $v = 5$). Note that $b = \pm 1$ is not counted in any of this, since $b^2 - 1 = 0$ then, so we do not have to worry about having distinct elements in the block.

Theorem 7.1 *If $v = 4t + 1 > 5$ is a prime power, then a BRD$(v, 5, 10)$ exists.*

We now give explicit solutions for the smaller prime powers:

Table 7.2

q	x (++)	b	$\log(b-1)$ (−−)	$\log(b)$	$\log(b+1)$ (++)	$\log(2)$ (−−)
9	$x^2 = 2x + 1$	$x + 1$	1	7	6	4
13	2	2	0	1	8	1
17	3	8	11	10	2	14
25	$x^2 = 4x + 3$	$x + 1$	1	17	14	6
29	2	5	2	22	6	1
37	2	2	0	1	26	1
41	6	4	15	12	22	26
49	$x^2 = 6x + 4$	$x + 3$	11	26	12	16
53	2	4	17	2	47	1
61	2	2	0	1	6	1
73	5	8	33	24	12	8
81	$x^4 = 2x^3 + 1$	$x + 1$	1	77	68	40
89	3	4	1	32	70	16
97	5	8	31	6	44	34
101	2	5	2	24	70	1
109	6	4	52	6	76	57
113	3	6	83	8	36	12
121	$x^2 = 10x + 4$	$x + 1$	1	71	68	36
125	$x^3 = 4x^2 + 3$	$x + 1$	1	29	99	93

We now give some explicit SDS's for small v.

Example 7.2 There exists a BRD$(8, 5, 20)$ consisting of the following base blocks:

$[0, 1, 2, -3, 4]; [0, 1, 2, 4, -5]; [0, 1, 2, 4, -6]; [\infty, 0, -1, -2, -4];$
$[\infty, -0, 1, 2, 4]; [\infty, -0, -1, 2, 4]; [\infty, -0, 1, -2, 4]; [\infty, -0, 1, 2, -4] \pmod 7$

Example 7.3 There exists a BRD(10,18,9,5,4).
$[-00, 01, 02, 11, 22]; [\infty, 01, 02, -11, -22] \pmod{(3,3)}$

Example 7.4 There exists a BRD$(13, 5, 10)$ constructed from the double of a BIBD$(13, 5, 5)$ taken from [1, IV.10.9]. The base blocks are:

$[0, 1, 2, -4, -8]; [0, -1, 2, -4, -8]; [0, 1, -3, 6, -12];$
$[0, -1, 3, 6, 12]; [0, 2, 5, 6, -10]; [0, 2, 5, -6, 10] \pmod{13}$

Example 7.5 There exists a BRD$(14, 5, 20)$ consisting of the blocks of the BRD$(13, 5, 10)$ constructed in Example 7.4 above, augmented with the following base blocks:

$[\infty, -1, -2, 4, 8]; [\infty, -3, -6, 11, 12]; [\infty, -5, 7, 9, -10]; [\infty, -0, 1, -3, 9];$
$[-0, 1, 2, 4, 8]; [0, 3, 6, 11, 12]; [0, -5, 7, 9, -10]; [\infty, -0, 1, 3, -9] \pmod{13}$

Example 7.6 A BRD$(15, 5, 8)$ was found from $6-(15, 5, 4)$ SDS taken from Hall [19, p. 410]. The base blocks of the BRD$(15, 5, 8)$ are:

$[-\infty, 0, -1, 2, -7]; [-\infty, 0, 1, -2, -7]; [0, -1, -4, 9, -11];$
$[0, 1, -4, 9, -11]; [0, 1, 4, -10, -12]; [-0, -1, -4, -10, -12] \pmod{14}$

Example 7.7 A BRD$(16, 5, 8)$ exists by Theorem 4.6. An alternative construction is given by the following $6-(16, 5, 8)$ SDS. The base blocks of the BRD$(16, 5, 8)$ are:

$[0, -1, 2, 4, -7]; [0, -1, -2, 4, 7]; [0, -1, 5, 8, -10];$
$[0, 1, 5, -8, 10]; [0, 1, 3, 7, -11]; [0, 1, 3, -7, 11] \pmod{16}.$

Example 7.8 There exists a BRD$(17, 5, 10)$ constructed from the double of a $4-(17, 5, 5)$ SDS. The base blocks of BRD$(17, 5, 10)$ are:

$[0, 1, 4, -13, -16]; [0, 1, -4, 13, -16]; [0, 3, 5, -12, -14]; [0, 3, -5, 12, -14];$
$[0, 2, 8, 9, -15]; [0, 2, 8, -9, 15]; [0, 6, 7, 10, -11]; [0, 6, 7, -10, 11] \pmod{17}.$

Example 7.9 BRD$(20, 5, 4)$ was constructed from the following base blocks:

$[-1, -5, 6, -10, -12]; [4, -7, -8, -13, -16];$
$[9, 11, 15, -17, -18]; [\infty, 0, -2, 3, -14] \pmod{19}.$

Example 7.10 A BRD$(21, 5, 4)$ adapted from Assaf's GDD in [34, Lemma 2.2]:
$[0, 2, 5, 11, -4]; [0, -1, -3, -7, -12];$
$[0, 1, 8, -16, -19]; [0, 4, -9, -10, -17] \pmod{21}$

Example 7.11 BRD$(30, 5, 4)$ was found from a $6-(30, 5, 4)$ SDS, the base blocks of BRD$(30, 5, 4)$ are:

$[-0, 1, 8, 10, 13]; [-0, -4, -15, -21, 26]; [-0, -1, 10, 14, \infty];$
$[-0, 3, 4, -11, 23]; [0, -2, 16, -17, 26]; [-0, 4, 6, 11, 27] \pmod{29}$

Example 7.12 A BRD$(31, 5, 4)$ exists by Theorem 4.6. Using a difference set construction for a BIBD$(31, 6, 1)$ (i.e., $[1, 5, 11, 24, 25, 27]$) yields the following $6-(31, 5, 4)$ SDS:

$[1, 5, -11, -24, -25]; [1, -5, 11, -24, -27]; [-1, 5, 11, -25, -27];$
$[1, 5, 24, 25, -27]; [1, 11, 24, -25, 27]; [5, 11, -24, 25, 27] \pmod{31}.$

Example 7.13 BRD$(40, 5, 4)$ was found from a $8-(40, 5, 4)$ SDS containing the base blocks:

$[\infty, 0, 3, -9, -27]; [2, -5, -13, -26, -32]; [-1, 4, -20, -29, -36];$
$[-8, 16, 25, -30, -35]; [10, -11, -12, -14, -22]; [-7, 15, -17, -31, -33];$
$[6, 21, 28, -34, -38]; [18, 19, -23, 24, -37] \pmod{39}.$

Example 7.14 A BRD$(41, 5, 2)$ adapted from [34, Lemma 2.1].
$[-0, 1, 3, 7, -34]; [-0, 5, -16, -30, -29];$
$[-0, -8, 23, 2, 20]; [-0, 1, 19, 4, 28] \pmod{41}$

Example 7.15 A BRGDD$_4(5, 2^6)$ exists. Let $\{i, i+6\}$ be the groups.
$[-0, 1, 2, 4, 9]; [0, 1, -2, -4, 9] \pmod{12}$

Example 7.16 A BRGDD$_2(5, 4^6)$ exists. Points agreeing in their first two elements are in the same group. (Design adapted from [24, III.1.37]).
$[000, 012, -020, -101, -112]; [000, 010, -021, 100, 113];$
$[000, 011, 102, 112, -121]; [000, 013, -103, -111, 123] \pmod{(-, 3, 4)}$

Acknowledgement

The authors would like to thank Mr. Fabian Migrini for writing one of the computer programs to sign SDS's. The authors also wish to thank the referees for improving the exposition of the paper and clarifying one result.

References

[1] R.J.R. Abel, Difference families, in: *The CRC Handbook of Combinatorial Designs* (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, FL, 1996, 270–287.

[2] R.J.R. Abel, Personal communication, Nov. 1997.

[3] R.J.R. Abel, A.E. Brouwer, C.J. Colbourn and J.H. Dinitz, Mutually orthogonal Latin squares, in: *The CRC Handbook of Combinatorial Designs* (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, FL, 1996, 111–142.

[4] R.J.R. Abel, G. Ge, M. Greig and L. Zhu, Resolvable Balanced Incomplete Block Designs with a Block Size of 5, (submitted) 1998.

[5] R.J.R. Abel and M. Greig, BIBDs with small block sizes, in: *The CRC Handbook of Combinatorial Designs* (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, FL, 1996, 41–47.

[6] R.J.R. Abel and M. Greig, Some new RBIBDs with block size 5 and PBDs with block sizes $\equiv 1 \bmod 5$, *Australasian J. Comb.* **15** (1997) 177–202.

[7] F.E. Bennett, H-D.O.F. Gronau, A.C.H. Ling and R.C. Mullin, PBD-closure, in: *The CRC Handbook of Combinatorial Designs* (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, FL, 1996, 203–213.

[8] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, UK, 1985.

[9] M. Bhaskar Rao, Group divisible family of PBIB designs, *J. Indian Stat. Assoc.* **4** (1966), 14–28.

[10] M. Bhaskar Rao, Balanced orthogonal designs and their applications in the construction of some BIB and group divisible designs. *Sankhyā Ser. A* **32** (1970) 439–448.

[11] G.R. Chaudhry and J. Seberry, On the (10, 5, λ)-Family of Bhaskar Rao Designs, *Bull. Inst of Combin. and its Applications* **23** (1998) 83–87.

[12] W. de Launey, (0,G)-Designs and Applications, Ph.D. thesis, University of Sydney (1987).

[13] W. de Launey and D.G. Sarvate, Non-existence of certain GBRDs, *Ars Combin.* **18** (1983) 5–20.

[14] W. de Launey, Bhaskar Rao designs, in: *The CRC Handbook of Combinatorial Designs* (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, FL, 1996, 241–246.

[15] W. de Launey and J. Seberry, On Bhaskar Rao designs of block size four, *Proceedings of the Seminar on Combinatorics and Applications, Indian Stat. Institute* (1982) 311–316.

[16] W. de Launey and J. Seberry, On generalized Bhaskar Rao designs of block size four, *Congr. Numer.* **41** (1984) 229–294.

[17] A. Dey and C.K. Midha, Generalized balanced matrices and their applications, *Utilitas Math.* **10** (1976) 139–149.

[18] P.B. Gibbons and R. Mathon, Construction methods for Bhaskar Rao and related designs, *J. Austral. Math. Soc. (Series A)* **42** (1987) 5–30; *ibid.* **43** 420.

[19] M. Hall, Jr., *Combinatorial Theory, (2nd ed.),* John Wiley and Sons, New York, 1986.

[20] H. Hanani, Balanced incomplete block designs and related designs, *Disc. Math.* **11** (1975), 255–369.

[21] C. Lam and J. Seberry, Generalized Bhaskar Rao designs, *J. Stat. Plann. and Inference* **10** (1984) 83–95.

[22] C.H.A. Ling, Pairwise balanced designs and related codes, Ph.D. thesis, University of Waterloo (1997).

[23] R. Mathon and A. Rosa, 2-(v, k, λ) designs of small order, in: *The CRC Handbook of Combinatorial Designs* (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, FL, 1996, 3–41.

[24] R.C. Mullin and H-D.O.F. Gronau, PBDs: recursive constructions, in: *The CRC Handbook of Combinatorial Designs* (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, FL, 1996, 193–203.

[25] W.D. Palmer, Partial generalized Bhaskar Rao designs over Abelian groups, *Australasian J. Comb.* **6** (1992) 257–266.

[26] W. Palmer and J. Seberry, Bhaskar Rao designs over small groups, *Ars Combin.* **26A** (1988) 125–148.

[27] D.P. Rajkundlia, Some techniques for constructing infinite families of BIBD's, *Disc. Math.* **44** (1983), 61–96.

[28] J. Seberry, Regular group divisible designs and Bhaskar Rao designs with block size three, *J. Stat. Plann. and Inference* **10** (1984) 69–82.

[29] J. Seberry, Generalized Bhaskar Rao designs of block size three, *J. Stat. Plann. and Inference* **11** (1985) 273–279.

[30] S.J. Singh, Some Bhaskar Rao designs and applications for $k = 3, \lambda = 2$, *University of Indore J. Science* **7** (1982) 8–15.

[31] D.J. Street, Bhaskar Rao designs from cyclotomy, *J. Austral. Math. Soc.* **29** (1980) 425–430.

[32] D.J. Street and C.A. Rodger, Some results on Bhaskar Rao designs, Combin. Math. VII, *Lecture Notes in Math.* **829** (1980) 238–245.

[33] R. Vyas, Some Bhaskar Rao designs and applications for $k = 3, \lambda = 4$, *University of Indore J. Science* **7** (1982) 16–25.

[34] J. Yin, A.C.H. Ling, C.J. Colbourn and R.J.R. Abel, The existence of uniform 5−GDDs, *J. Comb. Designs* **5** (1997) 275–299.