GBRDs with block size three over 2-groups, semi-dihedral groups and nilpotent groups

R. Julian R. Abel Diana Combe

School of Mathematics and Statistics
The University of New South Wales
NSW 2052, Australia

r.j.abel@unsw.edu.au diana@unsw.edu.au

Adrian M. Nelson William D. Palmer

School of Mathematics and Statistics
The University of Sydney NSW 2006, Australia

adriann@maths.usyd.edu.au billp@maths.usyd.edu.au

Mathematics Subject Classifications: 05B05, 20D15.

Submitted: Sep 9, 2009; Accepted: Jan 27, 2011; Published: Feb 14, 2011

Abstract

There are well known necessary conditions for the existence of a generalized Bhaskar Rao design over a group $\mathbb{G}$, with block size $k = 3$. We prove that they are sufficient for nilpotent groups $\mathbb{G}$ of even order, and in particular for 2-groups. In addition, we prove that they are sufficient for semi-dihedral groups.
Key words: Generalized Bhaskar Rao design. 2-groups. Nilpotent groups. Semi-dihedral groups. Normal subgroups. Hall-Paige Conjecture.

1 Introduction

1.1 Definitions and Notation

Throughout this paper $\mathbb{G}$ is a finite group written multiplicatively, $0 \notin \mathbb{G}$ is a zero symbol, and v, b, r, k, λ are positive integers with $v \geq 3$. We denote the cyclic group of order n by $C(n)$. A group is a *p-group*, if the order $|\mathbb{G}| = p^r$ for some prime p and integer r. A group is *elementary abelian* if it is the direct product of cyclic groups of order p for some prime p. A group is *nilpotent* if it is the direct product of P_i where each P_i is a p_i-group for some prime p_i. The *trivial group (or subgroup)* is the group with only one element.

Groups with more than one element are *non-trivial*. A subgroup is a *proper subgroup* if it is strictly smaller than the whole group.

There are several infinite families of groups of particularly importance in this paper. Each of them has a normal, cyclic subgroup of index 2 and this can lead to added complications when using normal subgroup constructions of designs. We recall their definitions here and set up notation in which we parameterize each family by the group order. They are all non-abelian, except for the first one or two groups in each family.

Definition 1. The *dihedral group*, $D(2m)$ of order $2m$.

$$D(2m) = \left\langle a, b : a^m = 1, b^2 = 1, ba = a^{-1}b \right\rangle; \quad m = 1, 2, \ldots$$

Definition 2. The *dicyclic group*, $Q(4m)$ of order $4m$, sometimes called *generalized quaternion*. The group $Q(8)$ is the *quaternion group*, and usually denoted Q.

$$Q(4m) = \left\langle a, b : a^{2m} = 1, b^2 = a^m, ba = a^{-1}b \right\rangle; \quad m = 1, 2, \ldots$$

Definition 3. The *semi-dihedral group*, $SD(8m)$, of order $8m$, sometimes called *quasi-dihedral* or *semi-hedral*.

$$SD(8m) = \left\langle a, b : a^{4m} = 1, b^2 = 1, ba = a^{2m-1}b \right\rangle; \quad m = 1, 2, 3, \ldots$$

1.2 Generalized Bhaskar Rao designs

Definition 4. A *generalized Bhaskar Rao design* $\mathrm{GBRD}(v, b, r, k, \lambda; \mathbb{G})$ is a $v \times b$ array, each entry of which is either 0 or an element of $\mathbb{G}$ such that:

1. each row has r group element entries and each column has k group element entries;
2. for each pair of distinct rows $(x_1, x_2, \ldots, x_b)$ and $(y_1, y_2, \ldots, y_b)$ the list

$$x_i y_i^{-1} : i = 1, 2, \ldots, b, \quad x_i \neq 0, \quad y_i \neq 0,$$

contains each group element exactly $\frac{\lambda}{|\mathbb{G}|}$ times.

The parameters in a $\mathrm{GBRD}(v, b, r, k, \lambda; \mathbb{G})$ are not all independent of each other. Clearly $\lambda \equiv 0 \pmod{|\mathbb{G}|}$, and replacing the group entries by 1 and leaving the others 0, results in an incidence matrix for a $\mathrm{BIBD}(v, b, r, k, \lambda)$, (or an all 1's matrix if $v = k$). It is well known that $r = \frac{\lambda(v-1)}{k-1}$ and $b = \frac{\lambda v(v-1)}{k(k-1)}$. We usually refer to a $\mathrm{GBRD}(v, k, \lambda; \mathbb{G})$, or to a $\mathrm{GBRD}(v, k, t|\mathbb{G}|; \mathbb{G})$.

Sometimes it is convenient to consider a more general form of a GBRD, where k is replaced by a finite set K of positive integers.

Definition 5. A *generalized Bhaskar Rao design* $\mathrm{GBRD}(v, K, \lambda; \mathbb{G})$ is a rectangular array with v rows, each entry of which is either 0 or an element of $\mathbb{G}$ and such that for each column the number of group entries is an element of K and for each pair of distinct rows $(x_1, x_2, \ldots, x_b)$ and $(y_1, y_2, \ldots, y_b)$, where b is the number of columns, the list

$$x_i y_i^{-1} : i = 1, 2, \ldots, b, \quad x_i \neq 0, \quad y_i \neq 0,$$

contains each group element exactly $\frac{\lambda}{|\mathbb{G}|}$ times.

Necessary conditions for the existence of a GBRD$(v, 3, \lambda; \mathbb{G})$ are well known and given, for example, in Abel et al. [2]:

Lemma 6. *The following conditions are necessary for a* GBRD$(v, 3, \lambda; \mathbb{G})$*:*

(i) $\lambda \equiv 0 \pmod{|\mathbb{G}|}$*;*

(ii) $\lambda(v-1) \equiv 0 \pmod 2$*;*

(iii) $\lambda v(v-1) \equiv \begin{cases} 0 \pmod 6 & \text{if } |\mathbb{G}| \text{ is odd} \\ 0 \pmod{24} & \text{if } |\mathbb{G}| \text{ is even;} \end{cases}$

(iv) *If* $v = 3$*, and* $\mathbb{G}$ *has a non-trivial cyclic Sylow* 2*-subgroup, then* $\lambda \equiv 0 \pmod{2|\mathbb{G}|}$.

It is known that, for $v = 3$ and $\lambda = |\mathbb{G}|$, the necessary conditions in Lemma 6 are sufficient for the existence of a GBRD$(v, 3, \lambda; \mathbb{G})$. This is a consequence of the recently proved long standing Hall-Paige conjecture (Evans [10], Wilcox [24], and Wilcox, Evans and Bray [6], New results). The Hall-Paige conjecture [15] concerns complete mappings of finite groups, and states that 'a finite group has a complete mapping if and only if the Sylow 2-subgroup is trivial or non-cyclic'. For any group $\mathbb{G}$, the existence of a GBRD$(v, 3, \lambda; \mathbb{G})$ for $v = 3$ is equivalent to the existence of a complete mapping of the group. For more details about complete mappings, see Evans [11]. For more details of the Hall-Paige conjecture and recent extension to complete mappings of loops (algebraic structures similar to groups but not requiring the product to be associative) see Pula [20].

Abel et al. [2] show the necessary conditions in Lemma 6 are sufficient when $v = 3$ and $\lambda > |\mathbb{G}|$ and that this follows as a consequence of the Hall-Paige conjecture. The necessary conditions in Lemma 6 are known to be sufficient for the existence of a GBRD$(v, 3, \lambda; \mathbb{G})$ for many families of groups $\mathbb{G}$. Abel et al. [2] conjecture that the necessary conditions in Lemma 6 are always sufficient for the existence of a GBRD$(v, 3, \lambda; \mathbb{G})$.

Conjecture 7. *For* $v \geq 3$*, the necessary conditions in Lemma 6 are sufficient for the existence of a* GBRD$(v, 3, \lambda; \mathbb{G})$.

We view Conjecture 7 as a generalization of the Hall-Paige conjecture. It is known that the necessary conditions are sufficient when the group is abelian, and the proof of this developed over some time, involved many people and was completed by Ge et al. [12]. They have been shown to be sufficient for any odd order nilpotent group by Palmer [19], for any dihedral group by Abel et al. [3], and for any sufficiently small group or any dicyclic group by Abel et al. [2]. Most recently Abel et al. [1] have shown them to be sufficient for pq groups and for groups of order ≤ 100 with the possible exception of some non-abelian groups with order $|\mathbb{G}| \in \{32, 36, 48, 54, 60, 64, 72, 96\}$. (The details of the proofs given in [1] for $|\mathbb{G}| \in \{56, 80\}$ are corrected in this paper and given in Section 2.4.) We summarise the evidence for Conjecture 7 in the following theorem:

Theorem 8. *Let* $\mathbb{G}$ *be a finite group, and* $v \geq 3$*, then in each of the following cases, the necessary conditions in Lemma 6 are sufficient for the existence of a* GBRD$(v, 3, \lambda; \mathbb{G})$*:*

(*i*) *For* $v = 3$*;*

(*ii*) *For* $\mathbb{G}$ *abelian, or dihedral, or dicyclic;*

(*iii*) *For* $\mathbb{G}$ *nilpotent of odd order;*

(*iv*) *For* $\mathbb{G}$ *with* $|\mathbb{G}| = pq$ *for* p, q *primes;*

(*v*) *For* $\mathbb{G}$ *with* $|\mathbb{G}| \leq 100$ *with the possible exception of* $|\mathbb{G}| \in \{$ 32, 36, 48, 54, 60, 64, 72, 96$\}$.

The early results on groups of small order, say ≤ 8, necessarily required producing many explicit designs. Proving the existence of GBRDs over cyclic groups of order $2, 4$ and 8 was a major challenge in dealing with cyclic groups in general (and ultimately all abelian groups). The case of the cyclic group of order 2 was difficult, and dealt with by Seberry [21]. The cyclic group of order 4 was dealt with partly by de Launey et al. [8]. The cyclic group of order 8 was considered by Seberry [22]. Some results for GBRDs over cyclic groups of even order were given by Bowler et al. [5]. The completion of the result for groups of order 4 and 8 had to wait until the proof for all abelian groups by Ge et al. [12]. Our aim in this paper was to show that the necessary conditions in Lemma 6 are sufficient for the existence of a GBRD$(v, 3, \lambda; \mathbb{G})$ whenever $\mathbb{G}$ is a nilpotent group of even order, and hence for all nilpotent groups. The main difficulty we faced was to show this for arbitrary 2-groups. In proving our result we also show that the necessary conditions in Lemma 6 are sufficient for any semi-dihedral group. We give explicit designs for $v = 6$ over semi-dihedral groups.

Our work makes extensive use of the known designs for small groups. In addition, the resolution of the Hall-Paige conjecture not only gives the fact that the necessary conditions in Lemma 6 are sufficient in the case where v takes the smallest possible value ($v = 3$), but gives ground level results for using in normal subgroup constructions and lifting results.

For a group $\mathbb{G}$, we say *Conjecture 7 holds* for $\mathbb{G}$ if, for $v \geq 3$, the necessary conditions in Lemma 6 are sufficient for the existence of a GBRD$(v, 3, \lambda; \mathbb{G})$.

1.3 Constructions and lifting lemmas

Definition 9. Let v and λ be positive integers, K be a set of positive integers and X be a set of v elements. A *pairwise balanced design*, or PBD$(v; K; \lambda)$, is a collection of subsets of X, called *blocks*, for which each pair of distinct elements of X appears together in exactly λ blocks and if a block contains exactly k elements of X then k belongs to K. A *balanced incomplete block design*, BIBD(v, k, λ) is a PBD$(v; \{k\}; \lambda)$.

From Abel et al. [4] we have the following lemmas:

Lemma 10. *For* $v \geq 3$*,* $v \neq 6$*, there exists a* PBD$(v; \{3, 4, 5, 8\}; 1)$.

Lemma 11. *For* $v \geq 3$*,* $v \neq 6$*,* $v \equiv 0, 1 \pmod 3$ *there exists a* PBD$(v; \{3, 4\}; 1)$.

We use construction theorems which are based on PBDs and subgroup structure.

Theorem 12. *[9] If there exist a* PBD$(v; K; \lambda)$ *and, for each* $h \in K$ *there exists a* GBRD$(h,\ k,\ \mu;\ \mathbb{G})$*, then a* GBRD$(v,\ k,\ \lambda\mu;\ \mathbb{G})$ *exists.*

Theorem 13. *[18] Let* $\mathbb{N}$ *be a normal subgroup of a finite group* $\mathbb{G}$*. Then, if both a* GBRD$(v,\ h,\ \lambda;\ \mathbb{G}/\mathbb{N})$ *and a* GBRD$(h,\ k,\ \mu;\ \mathbb{N})$ *exist, a* GBRD$(v,\ k,\ \lambda\mu;\ \mathbb{G})$ *also exists.*

More generally we have:

Theorem 14. *[7] Let* $\mathbb{N}$ *be a normal subgroup of a finite group* $\mathbb{G}$*. Then, if there exists a* GBRD$(v,\ K,\ \lambda;\ \mathbb{G}/\mathbb{N})$*, and for each* $h \in K$ *there exists a* GBRD$(h,\ k,\ \mu;\ \mathbb{N})$ *exist, then a* GBRD$(v,\ k,\ \lambda\mu;\ \mathbb{G})$ *also exists.*

We have the following lifting lemma:

Lemma 15. *Let* $\mathbb{G}$ *be a group with a normal subgroup* $\mathbb{N}$*. Suppose that*

(*i*) $\mathbb{N}$ *has trivial or non-cyclic Sylow* 2*-subgroup, i.e. a* GBRD$(3, 3, |\mathbb{N}|; \mathbb{N})$ *exists, and*

(*ii*) *if* $|\mathbb{G}| \equiv 0 \pmod 3$ *then* $|\mathbb{G}/\mathbb{N}| \equiv 0 \pmod 3$*, and*

(*iii*) *if* $|\mathbb{G}/\mathbb{N}| \equiv 2 \pmod 4$ *then* $|\mathbb{G}| \equiv 2 \pmod 4$*, and*

(*iv*) *if* $|\mathbb{G}| \equiv 0 \pmod 4$ *then* $|\mathbb{G}/\mathbb{N}| \equiv 0 \pmod 4$*.*

Then, if Conjecture 7 holds for the quotient $\mathbb{G}/\mathbb{N}$*, it also holds for* $\mathbb{G}$*.*

Proof. Suppose $\mathbb{G}$ has a normal subgroup $\mathbb{N}$ satisfying the stated conditions. By (*i*), we have, from the Hall Paige Theorem, that a GBRD(3, 3, $|\mathbb{N}|$; $\mathbb{N}$) exists. Conditions (*ii*), (*iii*) and (*iv*) mean that, for $v \geq 4$, the necessary conditions on v, t in Lemma 6 for the existence of a GBRD(v, 3, $t|\mathbb{G}|$; $\mathbb{G}$) are the same as those for a GBRD(v, 3, $t|\mathbb{G}/\mathbb{N}|$; $\mathbb{G}/\mathbb{N}$). A GBRD(v, 3, $t|\mathbb{G}/\mathbb{N}|$; $\mathbb{G}/\mathbb{N}$) and a GBRD(3, 3, $|\mathbb{N}|$; $\mathbb{N}$) yield a GBRD(v, 3, $t|\mathbb{G}|$; $\mathbb{G}$) by Theorem 13. Therefore, if Conjecture 7 holds for $\mathbb{G}/\mathbb{N}$, it also holds for $\mathbb{G}$. □

Remark 16. (*Correction to* [1].) In [1], a lemma similar to Lemma 15 was given, but condition (*iv*) was accidentally omitted. In fact conditions (*ii*), (*iii*) and (*iv*) when combined reduce to one simpler condition: $\gcd(|\mathbb{G}|, 12) = \gcd(|\mathbb{G}/\mathbb{N}|, 12)$. The omission of condition (*iv*) in [1] affected the proof that Conjecture 7 holds for groups of order 56 or 80. In Section 24 of this paper we address this by showing the more general result that Conjecture 7 holds for any group of order $2^n p$, where $p \geq 5$ is prime and n is the smallest positive integer such that p divides $2^n - 1$.

For 2-groups Lemma 15 simplifies to:

Lemma 17. *Let* $\mathbb{G}$ *be a* 2*-group with a non-trivial, non-cyclic, normal subgroup* $\mathbb{N}$ *such that* $|\mathbb{G}/\mathbb{N}| \geq 4$*. Then, if Conjecture 7 holds for the quotient* $\mathbb{G}/\mathbb{N}$*, it also holds for* $\mathbb{G}$*.*

2 Designs over 2-groups and other families of groups

Firstly we show Conjecture 7 holds for all semi-dihedral groups. Then, in our main result we show that Conjecture 7 holds for all 2-groups. Finally we show that Conjecture 7 holds for all nilpotent groups of even order, and hence for all nilpotent groups.

2.1 Semi-dihedral groups

Recall that for $m = 1, 2, \ldots$ the group $SD(8m) = \langle a, b : a^{4m} = b^2 = 1, ab = ba^{2m-1} \rangle$.

Example 18. For $m = 1, 2, \ldots$ the following $8m$ sets (*base blocks*) can be used to produce a GBRD$(6, 3, 8m; SD(8m))$.

For $i = 0, 1, 2, \ldots, 2m-1$: $\{(\infty, 1),\ (0, a^i),\ (1, a^{4m-i-1})\}$,
$\{(\infty, 1),\ (0, a^i b),\ (2, a^{4m-i-1}b)\}$, $\{(0, 1),\ (2, a^{2i+2}),\ (3, a^{2m-i-2}b)\}$.
For $i = 0, 2, \ldots, 2m-2$: $\{(0, a^{2m}),\ (1, a^{2i}),\ (4, a^{2m-i-1}b)\}$.
For $i = 1, 3, \ldots, 2m-1$: $\{(0, 1),\ (1, a^{2i}),\ (4, a^{2m-i-1}b)\}$.

We first construct a *group divisible design* (GDD): developing the first coordinates (mod 5), and then multiplying the second coordinates on the right by all elements of $SD(8m)$ gives a $(3, 1)$-GDD of type $(8m)^6$. The required GBRD$(6, 3, 8m; SD(8m))$ has 6 rows, which in this case are labelled as $\infty, 0, 1, 2, 3, 4$. A base block defines an *initial* column in the GBRD as follows: if $\{(s_1, t_1),\ (s_2, t_2),\ (s_3, t_3)\}$ is a base block, then for $i = 1, 2, 3$, we place t_i in row s_i of that initial column. The required GBRD has $40m$ columns; each initial column generates 5 columns, which are obtained by developing the 1st components (or row indices) of the initial columns (mod 5).

Theorem 19. *Let $\mathbb{G} = SD(8m)$ be the semi-dihedral group of order $8m$. Then the necessary conditions given in Lemma 6 are sufficient for the existence of a* GBRD$(v, 3, \lambda; \mathbb{G})$.

Proof. The necessary conditions in Lemma 6 reduce to saying that a GBRD$(v, 3, 8mt; \mathbb{G})$ exists only if $v \equiv 0, 1 \pmod 3$ or $mt \equiv 0 \pmod 3$. To prove these are sufficient, it is sufficient to restrict our argument to the cases $t = 1$ and 3, since for other designs we can take multiple copies of designs with $t = 1$ or 3.

For $v = 3$, the result follows from Theorem $8(i)$, and for $v = 6$, from Example 18. For $v = 4$, we note that $\mathbb{H} = \langle a^2, b \rangle$ is a normal subgroup of $\mathbb{G}$, $\mathbb{H} \cong D(4m)$, and $\mathbb{G}/\mathbb{H} \cong C(2)$. We have a GBRD$(4, 3, 2; C(2))$ and a GBRD$(3, 3, 4m; \mathbb{H})$ by Theorem 8 since $C(2)$ is abelian and $\mathbb{H}$ is dihedral. So the result follows from Theorem 13.

For $v = 5$ or 8, and $|\mathbb{G}| \not\equiv 0 \pmod 3$, we need to prove the result for $t = 3$. Here we first obtain a GBRD$(4, 3, 3|\mathbb{G}|; \mathbb{G})$ which was given in the previous paragraph. We can now apply Theorem 12, since BIBD$(v, 4, 3)$s exist for $v = 5, 8$ (Hanani, [16]).

For $v = 5$ or 8, and $|\mathbb{G}| \equiv 0 \pmod 3$, we need to prove the result for $t = 1$. Here $\mathbb{N} = \langle a^3 \rangle$ is normal in $\mathbb{G}$ and $\mathbb{N} \cong C(4m/3)$. Also, $\mathbb{G}/\mathbb{N} \cong D(6)$. A GBRD$(v, 4, 6; D(6))$ exists for $v = 5, 8$ (see Examples 4 and 5 in Abel et al. [3]). Also, a GBRD$(4, 3, 4m/3; \mathbb{N})$ exists by Theorem 8 since $\mathbb{N}$ is abelian. Hence Theorem 8 gives us a GBRD$(v, 3, |\mathbb{G}|; \mathbb{G})$.

This settles the existence problem for $v \in \{3, 4, 5, 6, 8\}$. For other v, if $v \equiv 0, 1 \pmod 3$, a GBRD$(4, 3, |\mathbb{G}| = 8m; \mathbb{G})$ exists by Lemma 12, since a PBD$(v; \{3, 4\}; 1)$ exists by

Lemma 11. Similarly, if $v \equiv 2 \pmod 3$, a PBD$(v; \{3,4,5,8\}; 1)$, exists by Lemma 10, and Lemma 12 gives us a GBRD$(v, 3, 3|\mathbb{G}| = 24m; SD(8m))$. □

2.2 2-groups

For any group $\mathbb{G}$, the *Frattini subgroup* $\Phi(\mathbb{G})$ is the intersection of its maximal subgroups. The Frattini subgroup is always a proper, normal subgroup, although it is not always non-trivial. When $\mathbb{G}$ is a p-group, the quotient $\mathbb{G}/\Phi(\mathbb{G})$ is elementary abelian, so $\Phi(\mathbb{G})$ is non-trivial unless $\mathbb{G}$ is an elementary abelian p-group.

Theorem 20. *Any 2-group of order at least 16 which is not cyclic, dicyclic, dihedral or semi-dihedral has a non-cyclic normal subgroup of index 4.*

Proof. Let $\mathbb{G}$ be a 2-group and $\Phi(\mathbb{G})$ its Frattini subgroup. By the Burnside Basis Theorem, (see, for example Hall [14], Theorem 12.2.1 or Huppert [17], Satz 3.15), the quotient $\mathbb{G}/\Phi(\mathbb{G})$ is an elementary abelian 2-group, $\mathbb{G}/\Phi(\mathbb{G}) \cong (C(2))^r$, say, and a set of group elements generate $\mathbb{G}$ precisely if their cosets (modulo $\Phi(\mathbb{G})$) generate the quotient group $\mathbb{G}/\Phi(\mathbb{G})$. Since $\mathbb{G}/\Phi(\mathbb{G}) \cong (C(2))^r$, any minimal generating set of $\mathbb{G}$ has r elements. In particular $r = 1$ if and only if $\mathbb{G}$ is cyclic. Note that, because the Frattini subgroup is the intersection of the maximal subgroups of $\mathbb{G}$, there is a one-to-one correspondence between the maximal subgroups of $\mathbb{G}$ and the maximal subgroups of $\mathbb{G}/\Phi(\mathbb{G})$ ($\cong (C(2))^r$). Hence, $\mathbb{G}$ has $2^r - 1$ maximal subgroups.

Assume now that $\mathbb{G}$ is a non-cyclic 2-group of order $2^n \geq 16$, and so $\mathbb{G}/\Phi(\mathbb{G}) \cong (C(2))^r$, for some $2 \leq r \leq n$. Let x_1, x_2, …, x_r form a minimal generating set of $\mathbb{G}$. We consider three cases (*i*) the Frattini subgroup is non-cyclic (*ii*) $r \geq 4$ and finally the remaining cases (*iii*) the Frattini subgroup is cyclic $r \in \{2, 3\}$.

Case (*i*). If $\Phi(\mathbb{G})$ is non-cyclic and $r = 2$, then $\Phi(\mathbb{G})$ is itself a non-cyclic normal subgroup of index 4. If $\Phi(\mathbb{G})$ is non-cyclic and $r > 2$, then $\Phi(\mathbb{G})$ together with x_3, …, x_r, generates a non-cyclic normal subgroup $\mathbb{N} = \langle \Phi(\mathbb{G}), x_3, \ldots, x_r \rangle$ of $\mathbb{G}$. The quotient $\mathbb{G}/\mathbb{N}$ has order 4 and is elementary abelian generated by the cosets $x_1\mathbb{N}$ and $x_2\mathbb{N}$.

Case (*ii*). If $r \geq 4$ then the group $\mathbb{N} = \langle \Phi(\mathbb{G}), x_3, \ldots, x_r \rangle$ is a normal subgroup of $\mathbb{G}$ of index four, regardless of whether or not $\Phi(\mathbb{G})$ is cyclic. This subgroup is non-cyclic because its quotient by its normal subgroup $\Phi(\mathbb{G})$ contains the cosets $x_3\Phi(\mathbb{G})$ and $x_4\Phi(\mathbb{G})$ which generate a non-cyclic subgroup of $\mathbb{G}/\Phi(\mathbb{G})$ isomorphic to $C(2) \times C(2)$.

Case (*iii*). Suppose that $\Phi(\mathbb{G})$ is cyclic and $r = 3$. Then $\mathbb{G}$ has $2^3 - 1 = 7$ maximal subgroups whose intersection $\Phi(\mathbb{G})$ is cyclic of order 2^{n-3}. Since $n \geq 4$, the cyclic 2-group $\Phi(\mathbb{G})$ is non-trivial and so it has a unique subgroup $\mathbb{K}$ say, of index 2. Because $\Phi(\mathbb{G})$ is normal in $\mathbb{G}$, and $\mathbb{K}$ is characteristic in $\Phi(\mathbb{G})$, $\mathbb{K}$ is normal in $\mathbb{G}$. The factor group $\mathbb{G}/\mathbb{K}$ is a 2-group of order 16 with 7 maximal subgroups. Consulting the tables of groups of order 16 in Thomas and Wood [23] we find there are four possibilities for this quotient, and each one has a non-cyclic normal subgroup $\mathbb{N}$ of index 4, with quotient isomorphic to $C(2) \times C(2)$.

- $\langle x : x^4 = 1 \rangle \times \langle y : y^2 = 1 \rangle \times \langle z : z^2 = 1 \rangle = C(4) \times C(2) \times C(2), \quad \mathbb{N} = \langle x^2, z \rangle.$

- $\langle x, y : x^4 = y^2 = 1,\, xy = yx^{-1}\rangle \times \langle z : z^2 = 1\rangle = D(8) \times C(2), \quad \mathbb{N} = \langle x^2, z\rangle$.
- $\langle x, y : x^4 = 1,\, x^2 = y^2,\, xy = yx^{-1}\rangle \times \langle z : z^2 = 1\rangle = Q \times C(2), \quad \mathbb{N} = \langle x^2, z\rangle$.
- $\langle x, y, z : x^4 = y^2 = z^2 = 1,\, xy = yx,\, xz = zx^3y,\, yz = zy\rangle = (C(4) \times C(2)) \rtimes C(2)$, $\mathbb{N} = \langle x^2, y\rangle$.

In each case lifting $\mathbb{N}$ back to $\mathbb{G}$ gives a non-cyclic normal subgroup of $\mathbb{G}$ of index 4, with quotient isomorphic to $C(2) \times C(2)$.

Suppose now that $\Phi(\mathbb{G})$ is cyclic and $r = 2$. In this case $\Phi(\mathbb{G})$ is cyclic of order 2^{n-2}. An element of a cyclic 2-group is either a generator or lies in its unique cyclic subgroup of index two. For 2-groups the Frattini subgroup is generated by the squares in $\mathbb{G}$, $\Phi(\mathbb{G}) = \langle x^2 : x \in \mathbb{G}\rangle$, (see Huppert [17], Satz 3.14). Hence there is an element $x \in \mathbb{G}$ whose square is a generator of $\Phi(\mathbb{G})$, and is hence of order 2^{n-1}. This element generates a cyclic subgroup of $\mathbb{G}$ of index 2. The 2-groups with cyclic subgroup of index 2 are well known, and are listed in Hall [14], Theorem 12.5.1. As $\mathbb{G}$ is non-cyclic and because we are assuming $n \geq 4$, $\mathbb{G}$ is one of the following:

(i) abelian of the form: $\langle x, y : x^{2^{n-1}} = 1, y^2 = 1, xy = yx\rangle = C(2^{n-1}) \times C(2)$;

(ii) modular of the form: $\langle x, y : x^{2^{n-1}} = 1, y^2 = 1, yx = x^{1+2^{n-2}}y\rangle$;

(iii) dicyclic, dihedral or semi-dihedral.

In each of the modular and abelian cases the subgroup $\mathbb{N} = \langle x^4, y\rangle$ is a non-cyclic normal subgroup of $\mathbb{G}$ of index 4. Note in the modular case this uses $n \geq 4$, which implies 2^{n-2} is a multiple of 4. In each case $\mathbb{G}/\mathbb{N}$ is isomorphic to $C(4)$.

Therefore, any 2-group of order at least 16 which is not cyclic, dicyclic, dihedral or semi-dihedral has a non-cyclic normal subgroup of index 4. □

Theorem 21. *Let $\mathbb{G}$ be a 2-group. Then the necessary conditions given in Lemma 6 are sufficient for the existence of a* GBRD$(v, 3, \lambda; \mathbb{G})$.

Proof. Let $\mathbb{G}$ be a 2-group. Then if $|\mathbb{G}| \leq 16$ or if the group is abelian (for example cyclic), or dihedral or dicyclic, we apply Theorem 8. If $\mathbb{G}$ is semi-dihedral we apply Theorem 19. Otherwise, let $\mathbb{G}$ be the smallest 2-group of order at least 16 which is not cyclic, dicyclic, dihedral or semi-dihedral, for which it is not determined that Conjecture 7 holds. From Theorem 20, $\mathbb{G}$ has a non-cyclic normal subgroup $\mathbb{N}$ of index 4. Conjecture 7 holds for $\mathbb{G}/\mathbb{N}$ by assumption. Hence, by Lemma 17 we have that Conjecture 7 holds for $\mathbb{G}$. In each case we determine that the necessary conditions given in Lemma 6 are sufficient for the existence of a GBRD$(v, 3, \lambda; \mathbb{G})$. □

2.3 Nilpotent groups

Recall that a *nilpotent* group $\mathbb{G}$ can be expressed as a direct product of the form $\mathbb{G} = \mathbb{G}_{p_1} \times \mathbb{G}_{p_2} \times \cdots \times \mathbb{G}_{p_r}$, where $p_1, p_2, \ldots, p_r$ are primes, and each $\mathbb{G}_{p_i}$ is a p_i-group. We

show that Conjecture 7 holds for nilpotent groups of even order. Since Conjecture 7 is known to hold for nilpotent groups of odd order ([18]), we conclude that it holds for all nilpotent groups.

Theorem 22. *Let $\mathbb{G}$ be a nilpotent group of even order, which is not a 2-group. Then Conjecture 7 holds for $\mathbb{G}$.*

Proof. We have $\mathbb{G} = \mathbb{G}_2 \times \mathbb{G}_3 \times \mathbb{H}$, where $\mathbb{G}_2$ is a non-trivial 2-group, $\mathbb{G}_3$ a 3-group, $\mathbb{H}$ is the product of all the p-group factors of $\mathbb{G}$ for primes $p \neq 2, 3$ and $\mathbb{G}_3 \times \mathbb{H}$ is non-trivial. We consider the three cases (i) $\mathbb{G}_3$ is trivial, (ii) $\mathbb{H}$ is trivial and $\mathbb{G}_3$ is cyclic of order 3 and (iii) $\mathbb{G}_3$ is non-trivial and $\mathbb{G}_3 \times \mathbb{H}$ is not cyclic of order 3.

Case (i). Suppose that $\mathbb{G}_3$ is trivial, so that $\mathbb{G} = \mathbb{G}_2 \times \mathbb{H}$, for $\mathbb{H}$ non-trivial. Then the conditions of Lemma 15 hold for $\mathbb{N} = \mathbb{H}$ and Conjecture 7 holds for $\mathbb{G}/\mathbb{N} = \mathbb{G}_2$ by Theorem 21. Hence Conjecture 7 holds for $\mathbb{G}$.

Case (ii). Suppose that $\mathbb{G} = \mathbb{G}_2 \times \mathbb{G}_3$, with $\mathbb{G}_3$ cyclic of order 3. If $\mathbb{G}_2$ is abelian, $\mathbb{G}$ is abelian and Conjecture 7 holds for $\mathbb{G}$ by Theorem 8. Assume now that $\mathbb{G}_2$ is non-abelian. In particular it is non-cyclic and of order divisible by 4. Then the necessary conditions of Lemma 6 for the existence of a GBRD$(v, 3, \lambda; \mathbb{G})$ reduce to $v \geq 3$ and λ divisible by $|\mathbb{G}|$. Taking t copies of a GBRD$(v, 3, |\mathbb{G}|, \mathbb{G})$ gives a GBRD$(v, 3, t|\mathbb{G}|; \mathbb{G})$. Hence showing Conjecture 7 holds for $\mathbb{G}$ reduces to showing a GBRD$(v, 3, |\mathbb{G}|; \mathbb{G})$ exists for all $v \geq 3$. By Lemma 10 and Theorem 12 it is sufficient to show that a GBRD$(v, 3, |\mathbb{G}|; \mathbb{G})$ exists for $v = 3$, 4, 5, 6 and 8.

We make the observation that for any non-cyclic 2-group $\mathbb{K}$ a GBRD$(v, 3, |\mathbb{K}|; \mathbb{K})$ exists for all $v \equiv 0, 1 \pmod 3$ by Theorem 21.

Suppose $v = 3$, 4 or 6. Set $\mathbb{N} = \mathbb{G}_3 \cong C(3)$. Then a GBRD$(3, 3, |\mathbb{N}|; \mathbb{N})$ exists. The quotient $\mathbb{G}/\mathbb{N} \cong \mathbb{G}_2$. Hence a GBRD$(v, 3, |\mathbb{G}/\mathbb{N}|; \mathbb{G}/\mathbb{N})$ exists by the observation above. Applying Theorem 13 shows a GBRD$(v, 3, |\mathbb{G}|; \mathbb{G})$ exists.

In the case $v = 5, 8$ set $\mathbb{N} = \mathbb{G}_2$. From the observation above, we know that a GBRD$(4, 3, |\mathbb{N}|; \mathbb{N})$ exists. The quotient $\mathbb{G}/\mathbb{N} \cong \mathbb{G}_3$ is cyclic of order 3. So by Ge et al [13] there exists a GBRD$(v, 4, |\mathbb{G}/\mathbb{N}|; \mathbb{G}/\mathbb{N})$ for all $v \geq 4$ with $v \equiv 0, 1 \pmod 4$; and hence, in particular, for $v = 5, 8$. So for $v = 5$ or 8 an application of Theorem 13 shows a GBRD$(v, 3, |\mathbb{G}|; \mathbb{G})$ exists.

Case (iii). $\mathbb{G} = \mathbb{G}_2 \times \mathbb{G}_3 \times \mathbb{H}$ with $\mathbb{G}_3$ a non-trivial 3-group and $\mathbb{G}_3 \times \mathbb{H}$ not cyclic of order 3. Let $\mathbb{M}$ be a maximal subgroup of $\mathbb{G}_3$. Then $\mathbb{M}$ is normal in $\mathbb{G}_3$ and $\mathbb{G}_3/\mathbb{M}$ is cyclic of order 3. Consequently $\mathbb{N} = \mathbb{M} \times \mathbb{H}$ is normal in $\mathbb{G}$ and Conjecture 7 holds for $\mathbb{G}/\mathbb{N} \cong \mathbb{G}_2 \times \mathbb{G}_3/\mathbb{M}$, as proved above. The conditions of Lemma 15 hold for $\mathbb{N} = \mathbb{M} \times \mathbb{H}$. Hence Conjecture 7 holds for $\mathbb{G}$. □

Combining Theorems 21 and 22, and the result for nilpotent groups of odd order ([18]), we have that Conjecture 7 holds for all nilpotent groups:

Theorem 23. *Let $\mathbb{G}$ be a nilpotent group. Then the necessary conditions given in Lemma 6 are sufficient for the existence of a* GBRD$(v, 3, \lambda; \mathbb{G})$.

2.4 Groups of orders 56 and 80

In [1], a proof that Conjecture 7 holds for all groups with order 56 or 80 was given, but this proof needs to be revised, since it made use of Lemma 15 with one necessary condition missing (see Remark 16). Here we prove the more general result:

Theorem 24. *Let $\mathbb{G}$ be a group of order $2^n p$, where $p \geq 5$ is prime and n is the smallest positive integer such that p divides $2^n - 1$. Then the necessary conditions given in Lemma 6 are sufficient for existence of a* GBRD$(v, 3, \lambda; \mathbb{G})$.

Proof. By the third Sylow theorem, the number of Sylow p-subgroups is congruent to 1 modulo p. The assumed conditions on n, p imply there are 1 or 2^n such subgroups. If there is only one such subgroup, then it is necessarily normal. In this case we can apply Lemma 15 with $\mathbb{N}$ this subgroup. Suppose now that $\mathbb{G}$ has 2^n Sylow p-subgroups. These subgroups are each cyclic of order p, and so the intersection of any two is the identity. Hence, as any element of order p generates one of these subgroups, there are $2^n(p-1)$ elements of order p. The remaining 2^n elements must make up a Sylow 2-subgroup $\mathbb{N}$ of $\mathbb{G}$. Since this Sylow 2-subgroup must be unique, $\mathbb{N}$ is therefore normal in $\mathbb{G}$. The action by conjugation of the elements of order p (on $\mathbb{N}$) must be non-trivial (because if any of the elements of order p had trivial action then we would have $\mathbb{G} \cong \mathbb{N} \times C(p)$ which has only one Sylow p-subgroup, in contradiction with the assumption that there are 2^n such subgroups). Hence $\mathbb{N}$ must have non-trivial automorphisms of odd order p. In particular, because the automorphism group of the cyclic group of order 2^n is of order 2^{n-1}, the Sylow 2-subgroup group $\mathbb{N}$ of $\mathbb{G}$ is not cyclic. Thus the necessary conditions in Lemma 6 reduce to saying a GBRD$(v, 3, 2^n pt; \mathbb{G})$ can exist only if $v \equiv 0$ or 1 (mod 3) or $t \equiv 0$ (mod 3). To prove these conditions are sufficient, we only need to deal with the cases $t = 1$ and 3, since for other designs we can take multiple copies of designs with $t = 1$ or 3.

First we show the existence of a GBRD$(v, 3, 2^n p; \mathbb{G})$ for $v = 3, 4$ and 6. Then by Lemma 11 and Theorem 12, a GBRD$(v, 3, 2^n p; \mathbb{G})$ exists for all $v \equiv 0$ or 1 (mod 3). Next, we show the existence of a GBRD$(v, 3, 3(2^n p); \mathbb{G})$ for $v = 5$ and 8. Then by Lemma 10 and Theorem 12, a GBRD$(v, 3, 3(2^n p); \mathbb{G})$ exists for all v.

When $v = 3$, 4 or 6, then, unless $p < v$ (i.e. $p = 5$ and $v = 6$) there exists a GBRD(v, v, p; $C(p)$) (for example, take the first v rows of the multiplication table of the finite field of order p). Also, since the normal Sylow 2-subgroup $\mathbb{N}$ is non-cyclic, a GBRD$(v, 3, 2^n; \mathbb{N})$ exists by Theorem 21. Together with Theorem 13 this gives us a GBRD$(v, 3, 2^n p; \mathbb{G})$.

When $v = 6$ and $p = 5$ we have $n = 4$ and $2^n p = 80$. A GBRD$(v, \{3, 6\}, 5; C(5))$ is given in the next paragraph, and a GBRD$(k, 3, 16; \mathbb{N})$ exists for $k = 3, 6$ [2]. Together with Theorem 14 this gives us a GBRD$(v, 3, 80; \mathbb{G})$.

A GBRD$(6, \{3, 6\}, 5; C(5))$ can be obtained in a manner similar to the one in Example 18, from five base blocks over $(\mathbb{Z}_5 \cup \{\infty\}) \times \mathbb{Z}_5$: $\{\infty_0, 0_0, 1_0, 2_0, 3_0, 4_0\}$, $\{\infty_0, 0_3, 1_2\}$, $\{\infty_0, 0_1, 2_4\}$, $\{0_0, 1_3, 2_4\}$, $\{0_0, 1_2, 3_3\}$. The corresponding GBRD has six rows, labelled as $\infty, 0, 1, 2, 3, 4$. Each base block defines an *initial* column in the GBRD as follows: if $\{(s_1, t_1), (s_2, t_2), \ldots, (s_m, t_m)\}$ is a base block, then for $i = 1, 2, \ldots, m$, we place t_i in row s_i of that initial column. The required GBRD has 21 columns; the initial column

with six entries generates just one column, and the others generate five columns each, by developing the first components (or row indices) of the initial columns modulo 5.

For $v = 5, 8$, a GBRD$(v, 4, 3p; C(p))$ exists. One can be obtained by Theorem 13, using a BIBD$(v, 4, 3)$ (which exists by Hanani [16]) and a GBRD(4, 4, p; $C(p)$). A GBRD(4, 3, 2^n; $\mathbb{N}$) exists by Theorem 21 since $\mathbb{N}$ is a non-cyclic 2-group. Hence a GBRD$(v, 3, 3(2^n p); \mathbb{G})$ exists by Theorem 13. □

2.5 Summary of new and old evidence for Conjecture 7

Theorem 25. *Let $\mathbb{G}$ be a finite group and $v \geq 3$. Then, in each of the following cases, the necessary conditions for the existence of a* GBRD$(v, 3, \lambda; \mathbb{G})$ *given in Lemma 6 are sufficient:*

(*i*) *For $v = 3$;*

(*ii*) *For $\mathbb{G}$ nilpotent (and in particular for abelian groups, and p-groups);*

(*iii*) *For $\mathbb{G}$ dihedral, dicyclic or semi-dihedral;*

(*iv*) *For $\mathbb{G}$ with $|\mathbb{G}| = pq$ for p, q primes;*

(*v*) *For $\mathbb{G}$ with $|\mathbb{G}| \leq 100$ with the possible exception of $|\mathbb{G}| \in \{36, 48, 54, 60, 72, 96\}$.*

References

[1] R.J.R. Abel, D. Combe, A.M. Nelson and W.D. Palmer, GBRDs over groups of order ≤ 100 or of order pq with p, q primes, *Discrete. Math.* **310** (2010), 1080–1088.

[2] R.J.R. Abel, D. Combe, G. Price and W.D. Palmer, Existence of Generalised Bhaskar Rao Designs with block size 3, *Discrete. Math.* **309** (2009), 4069–4078.

[3] R.J.R. Abel, D. Combe and W.D. Palmer, Bhaskar Rao designs and the dihedral groups, *J. Combin. Theory Ser. A* **106** (2004), 145–157.

[4] R.J.R. Abel, F.E. Bennett and M. Greig, PBD-closure, pp 247–254 in: *The CRC Handbook of Combinatorial Designs* (C.J. Colbourn and J.H. Dinitz, Eds), CRC Press, Boca Raton, FL, Second Edition, 2007.

[5] A. Bowler, K. Quinn and J. Seberry, Generalized Bhaskar Rao designs with elements from cyclic groups of even order, *Australas. J. Combin.* **3** (1991), 5–13.

[6] *The CRC Handbook of Combinatorial Designs* (C.J. Colbourn and J.H. Dinitz, Eds), CRC Press, Boca Raton, FL, Second Edition, 2007. New results can be found at http://www.emba.uvm.edu/dinitz/part6.newresults.html.

[7] D. Combe, W.D. Palmer, and W.R. Unger, *Bhaskar Rao designs and the alternating group* A_4, Australas. J. Combin. **24**, 275–283, 2001.

[8] W. de Launey, D.G. Sarvate and J. Seberry, Generalized Bhaskar Rao designs of block size 3 over Z_4, *Ars Combin.* **19A** (1985), 273–285.

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

[10] A.B. Evans, The admissibility of sporadic simple groups, *J. Algebra* **321** (2009), 105–116.

[11] A.B. Evans, *Orthomorphism Graphs of Groups*, Springer-Verlag, 1992.

[12] G. Ge, M. Greig, J. Seberry and R. Seberry, Generalized Bhaskar Rao designs with block size 3 over finite abelian groups, *Graphs Combin.* **23** (2007), no 3, 271–290.

[13] G. Ge, C.W.H. Lam, Bhaskar Rao designs of block size 4, *Discrete Math.* **268** (2003), 293–298.

[14] Marshall Hall, *The Theory of Groups*, (1959), Macmillan, New York.

[15] Marshall Hall and L.J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **5** (1955), 541–549.

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

[17] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.

[18] W.D. Palmer, A composition theorem for generalized Bhaskar Rao designs, *Australas. J. Combin.* **6** (1992), 221–228.

[19] W.D. Palmer, Partial generalized Bhaskar Rao designs, Ph.D. Thesis, University of Sydney, 1993.

[20] K. Pula, Products of all elements in a loop and a framework for non-associative analogues of the Hall-Paige conjecture, *Electron. J. Combin.*, **16(1)**, (2009) #R57.

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

[22] J. Seberry, Bhaskar Rao designs of block size three over groups of order 8 , Technical Report **CC88/4**, Department of Computer Science, University of New South Wales. (1988).

[23] A.D. Thomas and G.V. Wood, *Group Tables*, Shiva Publishing Limited, 1980.

[24] S. Wilcox, Reduction of the Hall-Paige conjecture to sporadic simple groups, *J. Algebra* **321** (2009), 1407–1428.