Canad. Math. Bull. Vol. **50** (4), 2007 pp. 504–518

Asymptotic Existence of Resolvable Graph Designs

Peter Dukes and Alan C. H. Ling

Abstract. Let $v \geq k \geq 1$ and $\lambda \geq 0$ be integers. A *block design* $\mathrm{BD}(v, k, \lambda)$ is a collection $\mathcal{A}$ of k-subsets of a v-set X in which every unordered pair of elements from X is contained in exactly λ elements of $\mathcal{A}$. More generally, for a fixed simple graph G, a *graph design* $\mathrm{GD}(v, G, \lambda)$ is a collection $\mathcal{A}$ of graphs isomorphic to G with vertices in X such that every unordered pair of elements from X is an edge of exactly λ elements of $\mathcal{A}$. A famous result of Wilson says that for a fixed G and λ, there exists a $\mathrm{GD}(v, G, \lambda)$ for all sufficiently large v satisfying certain necessary conditions. A block (graph) design as above is *resolvable* if $\mathcal{A}$ can be partitioned into partitions of (graphs whose vertex sets partition) X. Lu has shown asymptotic existence in v of resolvable $\mathrm{BD}(v, k, \lambda)$, yet for over twenty years the analogous problem for resolvable $\mathrm{GD}(v, G, \lambda)$ has remained open. In this paper, we settle asymptotic existence of resolvable graph designs.

1 Introduction

Let G be a finite undirected simple graph. A *G-block* (or simply *block*) on a set X is an embedding $G \hookrightarrow X$. For convenience, a G-block may be regarded as either a function from $V(G)$ to X or as a graph isomorphic to G with vertices in X. A *G-decomposition* of a multigraph H is a collection of G-blocks on $X = V(H)$ whose edge sets partition $E(H)$. Let λ be a nonnegative integer. A G-decomposition of λK_v (the multigraph with v vertices and λ edges between every pair of vertices) is also known as a *G-design* of *order* v and *index* λ, or $\mathrm{GD}(v, G, \lambda)$. In such a G-design on X, every unordered pair of distinct points in X appears as an edge of exactly λ blocks. A $\mathrm{GD}(v, K_k, \lambda)$ is usually called a *block design*, or BIBD, or $\mathrm{BD}(v, k, \lambda)$.

A set of G-blocks on X whose vertex sets partition X is called a *resolution class*. A G-decomposition is said to be *resolvable* if its collection of blocks can be partitioned into resolution classes. A resolvable G-decomposition of λK_v is called a resolvable G-design, or $\mathrm{RGD}(v, G, \lambda)$. When G is the complete graph K_k, this is denoted $\mathrm{RBD}(v, k, \lambda)$.

For example, $\mathrm{RBD}(v, 2, 1)$ are *one-factorizations* of the complete graph K_v, and $\mathrm{RBD}(v, 3, 1)$ are the *Kirkman triple systems*. It is well known that each of these objects exists "whenever possible"; refer below to (1.2) and (1.3). We note, however, that the existence of *any* v for which there exists an $\mathrm{RGD}(v, G, \lambda)$ is presently unknown for all but specific families of graphs or trivial indices.

Received by the editors August 10, 2005.

The research of the first author was supported by a University of Victoria Faculty of Science start-up grant. The research of the second author was supported by the Army Research Office (U.S.A) under grant number DAAD 19-01-1-0406 (Ling).

AMS subject classification: Primary: 05B05; secondary: 05C70, 05B10.

Keywords: graph decomposition, resolvable designs.

Suppose G has n vertices, e edges, and degree sequence $d_1, d_2, \dots, d_n$, so that $\sum_i d_i = 2e$. Let $D = \gcd\{d_1, \dots, d_n\}$. By counting in two ways the number of edges of λK_v, and the degree of each vertex in λK_v, it follows that

$$\lambda v(v-1) \equiv 0 \pmod{2e}, \tag{1.1}$$

$$\lambda(v-1) \equiv 0 \pmod{D} \tag{1.2}$$

are necessary conditions for the existence of a GD(v, G, λ). When $e = 0$, we regard these congruences as degenerating to equality, in which case $v = 1$ or $\lambda = 0$.

For a GD(v, G, λ) to have a resolution class, it is, of course, also necessary that

$$v \equiv 0 \pmod{n}. \tag{1.3}$$

Moreover, resolvable G-designs on a set X are *equireplicate*, that is, every point of X appears in the same number $r = \lambda(v-1)n/2e$ of blocks of the design. So a necessary condition for a GD(v, G, λ) to be equireplicate is that there is a (nonnegative) integer combination of degrees, say $\sum t_i d_i = \lambda(v-1)$ such that $\sum t_i = r$, the common number of blocks through any point. In other words, it is necessary that

$$\lambda(v-1) \equiv 0 \pmod{\gamma}, \tag{1.4}$$

where $\gamma = \gamma(G)$ is the least positive integer satisfying

$$\gamma \begin{bmatrix} 1 \\ n/2e \end{bmatrix} \in \operatorname{span}_{\mathbb{Z}} \left\{ \begin{bmatrix} d_i \\ 1 \end{bmatrix} \right\}. \tag{1.5}$$

Note that (1.3) and (1.4) together imply (1.1) and (1.2), since $D \in \operatorname{span}_{\mathbb{Z}}\{d_i\}$.

Given a fixed graph G, we say integers v and λ satisfying (1.3) and (1.4) are *admissible*. It should be mentioned that conditions (1.3) and (1.4) are not in general sufficient for the existence of an RGD(v, G, λ). For instance, let P be the Petersen graph (so $n = 10$, $e = 15$, and $d_i = 3$ for all i). Then with $v = 10$, $\lambda = 1$ is admissible, yet there is no GD$(10, P, 1)$, [1]. Indeed, several exceptions are known even for RBD(v, k, λ); see [3].

Based on the famous work of R. M. Wilson, it is known that if (1.1) and (1.2) are satisfied and v is sufficiently large, then there exists a GD(v, G, λ). The main result of [4] is in fact much more general, showing asymptotic existence (in v) of "edge-colored graph decompositions". Details are given in Section 5, where one important application for our purposes is considered. Another result we use is based on similar techniques and given below for later reference.

Theorem 1.1 *Let $\lambda \in \mathbb{Z}$, $\lambda \geq 0$. Suppose G is a simple graph with n vertices, e edges, and degrees $d_1, d_2, \dots, d_n$. Then there exists an equireplicate* GD(v, G, λ) *for all sufficiently large v satisfying* (1.1) *and* (1.4).

It is also known that RBD(v, k, λ) exist asymptotically in v.

https://doi.org/10.4153/CMB-2007-050-x Published online by Cambridge University Press

Theorem 1.2 ([5]) *Let $\lambda, k \in \mathbb{Z}$ with $\lambda \geq 0$ and $k \geq 1$. There exists* $\mathrm{RBD}(v, k, \lambda)$ *for all sufficiently large v satisfying* (1.3) *and* (1.2) *with $n = k$, $2e = k(k-1)$, and $D = k - 1$.*

In this paper, we prove a common generalization of these results.

Theorem 1.3 *Let $\lambda \in \mathbb{Z}$, $\lambda \geq 0$. Suppose G is a simple graph with n vertices, e edges, and degree sequence $d_1, d_2, \dots, d_n$. Then there exists v_0 such that* $\mathrm{RGD}(v, G, \lambda)$ *exist for all $v \geq v_0$ satisfying* (1.3) *and* (1.4).

The proof of Theorem 1.3 will be done in several steps. In Section 2, we show that given G with n vertices, (resolvable) $\mathrm{GD}(n, G, \lambda)$ exist for all sufficiently large admissible λ. This follows earlier work of Wilson [10]. In Section 3, we use cyclotomy in finite fields and a standard inflation construction for designs to produce equireplicate G-designs of any index λ having arbitrarily many resolution classes. This forms an ingredient for our main construction, given in Section 4. An intricate blend of block design constructions by Wilson [6] and Rees [7] produces a G-design of index λ which is resolvable from one with merely "enough" resolution classes. At that point, our first example of a resolvable G-design with fixed index λ will have been constructed. In Section 5, we apply the method of edge-colored graph decompositions [4] to establish asymptotic existence of special G-decompositions of complete multipartite graphs called G-frames. Section 6 completes the proof by filling examples in the "holes" of G-frames obtained by Wilson's fundamental construction.

In Sections 2 and 5, we will have occasion to use the following well-known result. See [8], for example.

Lemma 1.4 *Given an $m \times n$ rational matrix M and some $\mathbf{c} \in \mathbb{Q}^m$, the equation $M\mathbf{x} = \mathbf{c}$ has an integral solution $\mathbf{x}$ if and only if $\mathbf{y}^\top \mathbf{c}$ is integral whenever $\mathbf{y} \in \mathbb{Q}^m$ is such that $\mathbf{y}^\top M$ is integral.*

We now introduce an important tool for our main construction (Theorem 4.1) and for the recursive methods in Section 6. Let X and Y be sets with $|X| = k$ and $|Y| = m$. The triple $(X, Y, \mathcal{B})$ is called a *transversal design*, abbreviated $\mathrm{TD}(k, m)$, if $\mathcal{B}$ is a set of subsets of $X \times Y$ such that

(i) for any $B \in \mathcal{B}$ and $x \in X$, $|B \cap (\{x\} \times Y)| = 1$,
(ii) any two points $(x, y), (x', y') \in X \times Y$ with $x \neq x'$ are contained in exactly one element of $\mathcal{B}$.

A $\mathrm{TD}(k, m)$ is *resolvable*, abbreviated $\mathrm{RTD}(k, m)$, if $\mathcal{B}$ can be partitioned into partitions of $X \times Y$, each called a *resolution class*. There is a standard finite field construction for $\mathrm{RTD}(k, q)$, where q is a prime power and $k \leq q$. If Y is a finite field of order q, there is such an RTD having the automorphism $(x, y) \mapsto (x, y + 1)$. More generally, the existence of r mutually orthogonal latin squares of order m is equivalent to the existence of a $\mathrm{TD}(r + 2, m)$, which is in turn equivalent to the existence of an $\mathrm{RTD}(r + 1, m)$; see [3] for details. For later use, we state a well-known asymptotic existence result for RTD.

Lemma 1.5 ([2]) *For every $k \in \mathbb{Z}^+$, there exists an* RTD(k, m) *for all but finitely many $m \in \mathbb{Z}^+$.*

2 Existence for Sufficiently Large Index

Let X be an n-set. A *signed multigraph* on X is a mapping $A\colon \binom{X}{2} \to \mathbb{Z}$ from unordered pairs in X to the set of integers. We may view an ordinary graph G with vertex set X as a signed multigraph with $A(T) = 1$ if $T \in \binom{X}{2}$ is an edge of G and $A(T) = 0$ otherwise. Let $\mathcal{S}_n$ denote the symmetric group on X and $\mathbb{Z}[\mathcal{S}_n]$ the group ring of sums of integer multiples of permutations in $\mathcal{S}_n$. We view the collection of all signed multigraphs on X as a module over $\mathbb{Z}[\mathcal{S}_n]$; for $\sigma = \sum c(\pi)\pi \in \mathbb{Z}[\mathcal{S}_n]$ and $A\colon \binom{X}{2} \to \mathbb{Z}$, we have $(\sigma A)(T) = \sigma(A(T)) = \sum_{\pi\in\mathcal{S}_n} c(\pi)A(\pi(T))$.

The following is adapted from a very similar result in [10].

Lemma 2.1 *Let G be a simple graph with n vertices, e edges and* gcd *of degrees D. Suppose neither G nor $\overline{G}$ is a complete bipartite graph $K_{m,n-m}$. If λ is any integer such that $D \mid \lambda(n-1)$ and $2e \mid \lambda n(n-1)$, then there is an element $\sigma \in \mathbb{Z}[\mathcal{S}_n]$ such that $\sigma G = \lambda K_n$.*

Proof If $G = K_n$, we simply take $\sigma = \lambda\pi$ for any integer λ and any $\pi \in \mathcal{S}_n$. If $G = \overline{K_n}$ (and $n \geq 2$), only $\lambda = 0$ is admissible, and there is nothing to prove. For the remainder of the proof, suppose G and $\overline{G}$ both have at least one edge and are neither complete nor complete bipartite. It follows that G has an induced subgraph on 4 vertices which is none of $K_4, K_{1,3}, K_{2,2}, \overline{K_4}, \overline{K_{1,3}}, \overline{K_{2,2}}$. In other words, there exist $T \in \binom{X}{2}$ and disjoint transpositions $\tau_1, \tau_2 \in \mathcal{S}_n$ such that

$$A(T) - A(\tau_1 T) - A(\tau_2 T) + A(\tau_1\tau_2 T) = 1. \tag{2.1}$$

Let $f\colon \binom{X}{2} \to \mathbb{Z}$, be an arbitrary integer weighting and let $f(G)$ denote the sum of weights of all edges of G. In view of Lemma 1.4, it is enough to show that whenever d is some integer dividing $f(\pi G)$ for all $\pi \in \mathcal{S}_n$, then d divides $f(\lambda K_n)$. Computing modulo d,

$$\begin{aligned} 0 &\equiv f(G) - f(\tau_1 G) - f(\tau_2 G) + f(\tau_1\tau_2 G) \\ &= f(T) - f(\tau_1 T) - f(\tau_2 T) + f(\tau_1\tau_2 T), \end{aligned}$$

where the last equality is a consequence of (2.1). Since this holds with G replaced by any ρG, $\rho \in \mathcal{S}_n$, we have $f(\{x, y\}) + f(\{x', y'\}) \equiv f(\{x', y\}) + f(\{x, y'\})$ for any distinct $x, y, x', y' \in X$. It follows that there exist integers ϵ and a_x, $x \in X$, such that $f(\{x, y\}) \equiv a_x + a_y + \epsilon$ for all $x, y \in X$. Then

$$f(\lambda K_n) = \lambda \sum_{\{x,y\}\in\binom{X}{2}} f(\{x, y\}) \equiv \lambda(n-1)\sum_{x\in X} a_x + \frac{\lambda n(n-1)}{2}\epsilon.$$

But, as in [10], $Da_x \equiv Da_y$ for all $x, y \in X$. Since $D \mid \lambda(n-1)$ and $e \mid \lambda n(n-1)/2$,

$$f(\lambda K_n) \equiv \frac{\lambda n(n-1)}{2}(a_x + a_y + \epsilon) \equiv f(G) \equiv 0. \qquad \blacksquare$$

https://doi.org/10.4153/CMB-2007-050-x Published online by Cambridge University Press

Roughly speaking, this provides, for each integer λ, a "signed G-decomposition" of λK_n which is admissible for $v = n$ points. Following [11], it is easy to see that this yields G-designs of order n with sufficiently large admissible index λ. For convenience, define

$$\lambda_{\min} = \frac{\gamma(G)}{\gcd\{\gamma(G), n-1\}}, \tag{2.2}$$

which by (1.4) generates the ideal of admissible λ for n points.

Lemma 2.2 *Suppose neither G nor $\overline{G}$ is complete bipartite. Then there is an integer λ_0 such that there exists* RGD(n, G, λ) *for all $\lambda \geq \lambda_0$ satisfying $\lambda_{\min} \mid \lambda$.*

Proof For each admissible λ, it follows from Lemma 2.1 that there exists $\sigma_\lambda = \sum_\pi c_\lambda(\pi)\pi \in \mathbb{Z}[\mathcal{S}_n]$ such that $\sigma_\lambda G = \lambda K_n$. Put $\lambda' = 2e(n-2)!$ and let Λ denote the set of admissible integers λ with $-\lambda' \leq \lambda < 0$. Define

$$\lambda_0 = 2e(n-2)! \cdot \max\{-c_\lambda(\pi) : \pi \in \mathcal{S}_n, \lambda \in \Lambda\}.$$

Now let $\lambda \geq \lambda_0$. Write $\lambda = 2e(n-2)!t - \nu$, where t is an integer and $\nu \in \Lambda$. Let $\sigma = \sum_\pi (t - c_\nu(\pi))\pi$. Observe that σ has nonnegative coefficients and $\sigma G = t(\sum_\pi \pi)K_n - \nu K_n = \lambda K_n$. ■

By applying this lemma to the disjoint union of possibly several copies of G, we may drop the restriction of G and $\overline{G}$ not being complete bipartite.

Theorem 2.3 *Let G be any simple graph on n vertices, and let $n' = nk$, where $k \in \mathbb{Z}^+$ is chosen such that $k = 1 + \gamma(G)$ if G or $\overline{G}$ is complete bipartite but not edgeless, and $k = 1$ otherwise. There is an integer λ_0 such that there exists* RGD(n', G, λ) *for all $\lambda \geq \lambda_0$ satisfying $\lambda_{\min} \mid \lambda$.*

Proof The disjoint union G' of k copies of G is never complete bipartite or the complement of a complete bipartite graph. Note that condition (1.4) on λ is the same for G' as for G. So the result follows by Lemma 2.2 applied to G'. ■

To close this section, we note that for any $k \geq 2$, using k copies of G as in Theorem 2.3 provides RGD(nk, G, λ) for some λ. However, there will usually be admissible λ for which the results of this section fail to produce RGD(v, G, λ). In fact, there may be admissible values of λ for v which are not even multiples of $\lambda_{\min}$. The next two sections provide constructions of resolvable graph designs with arbitrary index λ.

https://doi.org/10.4153/CMB-2007-050-x Published online by Cambridge University Press

3 Inflation and Reduction of Index

We will use $\mathbb{F}_q$ to denote a finite field of order q. If $q \equiv 1 \pmod{m}$, then $\mathbb{F}_q$ contains a multiplicative subgroup C_0 of index m. Here, the cosets $C_0, C_1, \dots, C_{m-1}$ of C_0 are assumed to be indexed so that $x \in C_i$ and $y \in C_j$ implies $xy \in C_{i+j}$, where the latter subscript is reduced mod m. These cosets are the *cyclotomic classes* of index m.

The following result has been extensively used in the literature on asymptotic existence of designs.

Lemma 3.1 ([9]) *Let $m, k \geq 2$ be integers. Let μ be any mapping from the unordered pairs in $\{1, \dots, k\}$ to $\{0, 1, \dots, m-1\}$. Suppose q is a prime power with $q > m^{k^2}$ and $q \equiv 1 \pmod{m}$. Then there exist $a_1, \dots, a_k \in \mathbb{F}_q$ such that for $1 \leq i < j \leq k$, $a_i - a_j \in C_{\mu(\{i,j\})}$, where $C_0, C_1, \dots, C_{m-1}$ are the cyclotomic classes of index m in $\mathbb{F}_q$.*

Let $\Gamma_{u,w}$ be the graph with vertex set $X \times Y$, where $|X| = u$, $|Y| = w$, and $\{(x, y), (x', y')\}$ is an edge if and only if $x \neq x'$ and $y \neq y'$. A G-decomposition of $\lambda\Gamma_{u,w}$ is called a *G-grid design* of *type $u \times w$* and *index λ*.

Lemma 3.2 *Let $\lambda \in \mathbb{Z}^+$. Suppose G is a simple graph with n vertices, and suppose there exists* $\mathrm{RGD}(n', G, \lambda^*)$ *for $\lambda^* \equiv 0 \pmod{\lambda}$. Let $l = \lambda^*/\lambda$. For sufficiently large prime powers $q \equiv 1 \pmod{l}$, there exists a resolvable G-grid design of type $n' \times q$ and index λ.*

Proof Let the hypothesized G-design be on points $X = \{x_1, \dots, x_{n'}\}$, with block collection $\mathcal{B}$. Let $S = \{(x, \beta) : x \in \beta \in \mathcal{B}\}$. There are $\lambda^* nn'(n'-1)/2e$ elements in S. Let $\mu\colon \binom{S}{2} \to \{0, 1, \dots, l-1\}$ be defined so that, for each fixed pair (i, j) with $1 \leq i < j \leq n'$, the collection of all $\mu(\{(x_i, \beta), (x_j, \beta)\})$, where β is such that $\{x_i, x_j\} \in E(\beta)$ varies over every element of $\{0, 1, \dots, l-1\}$ exactly λ times. Pick $q \equiv 1 \pmod{l}$ with $C_0, C_1, \dots, C_{l-1}$ as the cyclotomic classes of index l in $\mathbb{F}_q$. By Lemma 3.1, if q is chosen sufficiently large, then there exists a mapping $\phi\colon S \to \mathbb{F}_q$ so that, for all $\beta \in \mathcal{B}$ and $i \leq j$, $\phi((x_i, \beta)) - \phi((x_j, \beta)) \in C_h$, where $h = \mu(\{(x_i, \beta), (x_j, \beta)\})$. It will be convenient to define $a(x, b) + c = (x, ab + c)$ whenever $(x, b) \in X \times \mathbb{F}_q$ and $a, c \in \mathbb{F}_q$. For each block $\beta \in \mathcal{B}$, define $\beta^*(i) = (\beta(i), \phi(\beta(i), \beta))$, an embedding of G in $X \times \mathbb{F}_q$. Given a resolution class $\mathcal{R}$ of $\mathcal{B}$ and any $a \in C_0$, let $\mathcal{R}_a = \{a\beta^* + c : \beta \in \mathcal{R} \text{ and } c \in \mathbb{F}_q\}$. Suppose $a\beta^*(i) + c = a(\beta')^*(i') + c'$ for some $\beta, \beta' \in \mathcal{R}$ and $c, c' \in \mathbb{F}_q$. Then

$$(\beta(i), a\phi(\beta(i), \beta) + c) = (\beta'(i'), a\phi(\beta'(i'), \beta') + c').$$

Since $\mathcal{R}$ is a resolution class on X, the first coordinates force $\beta = \beta'$ and $i = i'$. But then the second coordinates force $c = c'$. This shows that each $\mathcal{R}_a$ is a resolution class of blocks on $X \times \mathbb{F}_q$. It is routine to check from the defining property of ϕ that the union of all $\mathcal{R}_a$, where $\mathcal{R}$ is a resolution class of $\mathcal{B}$ and $a \in C_0$, is the block collection of a G-grid design of type $n' \times q$ and index λ. ■

By standard design-theoretic constructions, we may place G-grid designs on the blocks of a resolvable block design and "fill in holes" with other G-designs. This establishes the following.

https://doi.org/10.4153/CMB-2007-050-x Published online by Cambridge University Press

Theorem 3.3 *Let $\lambda \in \mathbb{Z}^+$. Suppose G is a simple graph with n vertices and $e > 0$ edges and that there is an* RGD(n', G, λ^*) *with $\lambda^* \equiv 0 \pmod{\lambda}$. Given any positive integer r and sufficiently large u and q (q a prime power) with*

$$u \equiv n' \pmod{n'(n'-1)}, \quad \lambda(u-1) \equiv 0 \pmod{\gamma}, \tag{3.1}$$

$$q \equiv 1 \pmod{\lambda^*/\lambda}, \quad \lambda(q-1) \equiv 0 \pmod{\gamma}, \quad \lambda q(q-1) \equiv 0 \pmod{2e}, \tag{3.2}$$

there exists an equireplicate GD(uq, G, λ) *with at least r distinct resolution classes.*

Proof Apply Lemmas 2.3 and 3.2 to obtain a resolvable G-grid design, say with block collection $\mathcal{A}$, of type $n' \times q$ and index λ for sufficiently large q satisfying (3.2). Suppose $\mathcal{A}$ partitions into r' resolution classes. By Theorems 1.1 and 1.2 and (3.1), we may take an RBD$(u, n', 1)$, say with block collection $\mathcal{B}$, with u sufficiently large so that (i) $\mathcal{B}$ has at least r/r' resolution classes; and (ii) there exists an equireplicate GD(u, G, λ). For (ii), note that $\lambda u(u-1) \equiv 0 \pmod{2e}$ follows from (3.1) since $2e \mid n\gamma$. Now form a resolvable G-grid design of type $u \times q$ and index λ on points $X \times \mathbb{F}_q$ by replacing every block B of the RBD$(u, n', 1)$ by a copy of $\mathcal{A}$ on $B \times \mathbb{F}_q$. To this block collection, add blocks of an equireplicate GD(u, G, λ) on each $X \times \{a\}$, $a \in \mathbb{F}_q$, and of an equireplicate GD(q, G, λ) on each $\{x\} \times \mathbb{F}_q$, $x \in X$. The result is an equireplicate G-design of order uq having at least $r' \cdot (r/r') = r$ resolution classes. ■

4 The First Examples

For a given graph G, we have so far merely constructed (large) equireplicate G-designs guaranteed to have many resolution classes. Here, we present another finite field construction which results in a (much larger) resolvable G-design, provided a minor requirement holds on the number of resolution classes in the ingredient G-design. This serves as our first example of a resolvable G-design with a given index λ. Our method is adapted from resolvable block design constructions in [6, 7], where the reader is directed for more details.

Theorem 4.1 *Let G be a simple graph with n vertices and $e > 0$ edges. Let $s = \lceil n/e \rceil$. Suppose there exists an equireplicate G-design of order v and index λ with at least $\lambda s + 1$ distinct resolution classes. Let $m = \lambda n(v-1)/2e - \lambda s - 1$ and $L = \mathrm{lcm}\{2es, m\}$. Then for sufficiently large prime powers $q \equiv 1 \pmod{L}$, there exists an* RGD(vq, G, λ).

Proof First, we set up some notation. Take the vertex set of G to be $\{1, \ldots, n\}$. Let the given G-design be on the set X with $|X| = v$ and with blocks $\mathcal{A}$. Regard each $\beta \in \mathcal{A}$ as an injection from $\{1, \ldots, n\}$ to X. For sufficiently large prime powers $q = 2esf + 1$, there exist mappings $\xi_h \colon \{1, \ldots, n\} \to \mathbb{F}_q$ with

$$\bigcup_{h=1}^{s} \{\xi_h(i) - \xi_h(j) : i < j \text{ and } \{i, j\} \in E(G)\}$$

forming a set of representatives for the cyclotomic classes of index es in $\mathbb{F}_q$, and with $\xi_h(i)$, $i \in \{1, \ldots, n\}$, in distinct classes for each h. This follows from Lemma 3.1 and

https://doi.org/10.4153/CMB-2007-050-x Published online by Cambridge University Press

the fact that $n \le es$. We now construct a resolvable G-design of index λ on $X \times \mathbb{F}_q$ in two pieces, mirroring constructions in [6, 7], respectively.

Piece 1: Let Π be a collection of λs different resolution classes in $\mathcal{A}$, and suppose $\theta\colon \Pi \to \{1,\dots,s\}$ is a labeling with $|\theta^{-1}(h)| = \lambda$ for $1 \le h \le s$. Fix $\mathcal{R} \in \Pi$ and suppose $h = \theta(\mathcal{R})$. In what follows, we write ξ for ξ_h as defined above. Let ω be a generator of $\mathbb{F}_q$ and define

$$K = \{\omega^{est}\xi(i) : 1 \le i \le n \text{ and } 0 \le t < f\}.$$

By choice of ξ, we have $|K| = nf$.

For $i \in \{1,\dots,n\}$ and $\beta \in \mathcal{R}$, define $\beta_i\colon \{1,\dots,n\} \to X \times \mathbb{F}_q$ by $\beta_i(j) = (\beta(i), \xi(j))$. Define $\beta^*\colon \{1,\dots,n\} \to X \times \mathbb{F}_q$ by $\beta^*(j) = (\beta(j), \xi(j))$. The β_i and β^* are to be regarded as G-blocks on $X \times \mathbb{F}_q$. For every $c \in \mathbb{F}_q$, put

$$\mathcal{R}_c = \bigcup_{i=1}^{n}\bigcup_{t=0}^{f-1}\{\omega^{est}\xi(i)\beta_i + c : \beta \in \mathcal{R}\} \cup \bigcup_{a\in\mathbb{F}_q^{\times}\setminus K}\{a\beta^* + c : \beta \in \mathcal{R}\}.$$

Note $|\mathcal{R}_c| = (nf + (q - nf))|\mathcal{R}| = vq/n$.

We show that each $\mathcal{R}_c$ is a resolution class on $X \times \mathbb{F}_q$. It suffices to consider $\mathcal{R}_0$. Suppose first that $\omega^{est}\xi(i)\beta_i(j) = \omega^{est'}\xi(i')(\beta')_{i'}(j')$. Then $\beta(i) = \beta'(i')$, and we must have $\beta = \beta'$, $i = i'$ by virtue of $\mathcal{R}$ being a resolution class. But then $\omega^{est}\xi(j) = \omega^{est'}\xi(j')$, which, since $|K| = nf$, forces $t = t'$ and $j = j'$. Suppose next that $\omega^{est}\xi(i)\beta_i(j) = a(\beta')^*(j')$. Then $\beta(i) = \beta'(j')$, and we must have $\beta = \beta'$, $i = j'$. So $\omega^{est}\xi(j) = a \notin K$, which is absurd. Finally suppose $a\beta^*(j) = a'(\beta')^*(j')$. Then $\beta(j) = \beta'(j')$, and it follows that $\beta = \beta'$, $j = j'$, and $a = a'$.

Now for every $a \in K$, put $\mathcal{R}'_a = \bigcup_{c\in\mathbb{F}_q}\{a\beta^* + c : \beta \in \mathcal{R}\}$. Each $\mathcal{R}'_a$ is also a resolution class, since $a\beta^*(j) + c = a(\beta')^*(j') + c'$ implies $\beta = \beta'$, $j = j'$ as $\mathcal{R}$ is a resolution class. Then $c = c'$ is clear on inspecting the second coordinate.

In total, there are $\lambda s(q + nf)$ resolution classes in Piece 1, with any two points in $X \times \mathbb{F}_q$ of the form (x, a), (x, a') appearing in exactly λ G-blocks, as well as covering any two points of the form $(\beta(j), a)$, $(\beta(j'), a')$, where $\{j, j'\} \in E(G)$ and $\beta \in \mathcal{R} \in \Pi$.

Piece 2: Consider the blocks $\mathcal{P} = \mathcal{A} \setminus \bigcup_{\mathcal{R}\in\Pi}\mathcal{R}$. Let $\mathcal{Q} \subset \mathcal{P}$ be a resolution class. Then every point in X appears in exactly $m = \lambda n(v-1)/2e - \lambda s - 1$ blocks of $\mathcal{P} \setminus \mathcal{Q}$. Fix any $M \subset \mathbb{F}_q \setminus \{0\}$ with $|M| = m$. If $q \equiv 1 \pmod{m}$, the family of sets $\Theta = \bigcup_{a\in\mathbb{F}_q}\{M + a, \{a\}\}$ can be partitioned into $m + 1$ partitions $\Theta_0, \dots, \Theta_m$ of $\mathbb{F}_q$ (where, say, Θ_0 contains $q - m$ singletons and Θ_ℓ contains exactly one singleton for $\ell = 1, \dots, m$.)

For each $x \in X$, let ϕ_x be a bijection from those blocks in $\mathcal{P}$ which contain x onto $M \cup \{0\}$. Now let $(X, \mathbb{F}_q, \mathcal{B})$ be an $\mathrm{RTD}(v, q)$ admitting the automorphism $(x, a) \mapsto (x, a + 1)$. This exists for sufficiently large q by Theorem 1.5. Each $\tau \in \mathcal{B}$ can be viewed as a mapping from X to $\mathbb{F}_q$, where $\tau(x)$ is the unique $c \in \mathbb{F}_q$ with $\tau \cap \mathbb{F}_q = \{c\}$. Given $\beta \in \mathcal{P}$ and $\tau \in \mathcal{B}$, let $[\beta, \tau]\colon \{1,\dots,n\} \to X \times \mathbb{F}_q$ be defined by $[\beta,\tau](i) = (\beta(i), \phi_{\beta(i)}(\beta) + \tau(\beta(i)))$. Fix $z \in X$ and a resolution class $\mathcal{T}$ of $\mathcal{B}$. For each $\ell = 0, \dots, m$, define

$$\mathcal{T}_\ell = \bigcup_{a: a+M \in \Theta_\ell} \{[\beta,\tau] : \beta \in \mathcal{P} \setminus \mathcal{Q} \text{ and } \tau \in \mathcal{T} \text{ with } \tau(z) = a\}$$
$$\cup \bigcup_{a:\{a\} \in \Theta_\ell} \{[\beta,\tau] : \beta \in \mathcal{Q} \text{ and } \tau \in \mathcal{T} \text{ with } \tau(z) = a\}.$$

We show that each $\mathcal{T}_\ell$ is a resolution class on $X \times \mathbb{F}_q$. Assume $[\beta,\tau](i) = [\beta',\tau'](i')$, where $\tau,\tau' \in \mathcal{T}$. Let $x = \beta(i) = \beta'(i')$ and suppose $\phi_x(\beta) = g$, $\phi_x(\beta) = g'$, for some $g, g' \in M \cup \{0\}$. If $g, g' \in M$, then $g + \tau(x) = g' + \tau'(x)$. So $\tau(x) + M$ and $\tau'(x) + M$ intersect. By the automorphism of the RTD, $\tau(z) + M$ and $\tau'(z) + M$ must intersect. But these sets belong to Θ_ℓ, a partition of $\mathbb{F}_q$. It follows that $\tau = \tau'$, $g = g'$, $\beta = \beta'$ and $i = i'$. The conclusion is similar if either g or $g' = 0$.

There are q choices for $\mathcal{T}$ and $m+1$ choices for ℓ. So there are $\lambda qn(v-1)/2e - \lambda sq$ resolution classes in Piece 2, with any two points of the form $(\beta(j), a)$, $(\beta(j'), a')$, where $\{j, j'\} \in E(G)$ and $\beta \in \mathcal{P}$, appearing in a G-block.

Taking Piece 1 and Piece 2 together, there are $\lambda n(vq-1)/2e$ resolution classes consisting of G-blocks covering all pairs of points in $X \times \mathbb{F}_q$, λ times each. It follows that

$$\bigcup_{\mathcal{R} \in \Pi} \Big[\bigcup_{c \in \mathbb{F}_q} \mathcal{R}_c \cup \bigcup_{a \in K} \mathcal{R}'_a \Big] \cup \bigcup_{\mathcal{T}} \bigcup_{\ell=0}^{m} \mathcal{T}_\ell$$

is the set of blocks of a resolvable G-design of index λ on $X \times \mathbb{F}_q$. ■

5 Existence and Applications of *G*-cframes

We must now make a short diversion to introduce and prove results about frames, a key ingredient in the construction of resolvable block designs (see [3]).

A set of G-blocks on X with disjoint vertex sets is called a *partial resolution class*. As is standard in block design terminology, we refer to the maximal independent sets in a complete (λ-fold) multipartite graph as *groups*. A *G-frame* with *group sizes* $g_1, \dots, g_u$ and *index* λ is a G-decomposition of $H = \lambda K_{g_1,\dots,g_u}$ in which the blocks can be partitioned into partial resolution classes, each missing precisely the points of a single group of H. When $g_i = g$ for each $i = 1, \dots, u$, such a G-frame is called *uniform* and has *type* g^u.

Suppose $\mathcal{B}$ is a collection of blocks forming a $\mathrm{GD}(v, G, \lambda)$ on the point set X, and $\mathcal{A}$ is a subcollection of $\mathcal{B}$ forming a $\mathrm{GD}(u, G, \lambda)$ on the point set $Y \subset X$. If $\mathcal{B}$ admits a partition into resolution classes on X, say $\mathcal{R}_1, \dots, \mathcal{R}_m$, such that $\mathcal{A} \cap \mathcal{R}_i$ is either empty or a resolution class on Y for $i = 1, \dots, m$, then $\mathcal{A}$ is called a *compatibly resolvable sub-design* of $\mathcal{B}$. A pair of G-decompositions with this property is abbreviated $\mathrm{CRGD}(v, u, G, \lambda)$. Note that the existence of $\mathrm{RGD}(v, G, \lambda)$ implies the existence of $\mathrm{CRGD}(v, 1, G, \lambda)$. The following "group filling" construction is very standard in the literature. See [3], for example.

https://doi.org/10.4153/CMB-2007-050-x Published online by Cambridge University Press

Lemma 5.1 *If there exists*

(i) *a G-frame with group sizes $g_1, \dots, g_u$ and index λ,*
(ii) *a $\mathrm{CRGD}(g_i + h, h, G, \lambda)$ for all $i = 1, \dots, u - 1$, and*
(iii) *an $\mathrm{RGD}(g_u + h, G, \lambda)$,*

then there exists a $\mathrm{CRGD}(g_1 + \cdots + g_u + h, g_u + h, G, \lambda)$.

Suppose in a G-frame of type g^u and index λ that every group is missed exactly m times. Then there are mu partial resolution classes, and each class contains $g(u-1)/n$ blocks. Since there are $\lambda g^2 u(u-1)/2e$ blocks in any such G-frame, we must have $m = \lambda ng/2e$. But furthermore, every point must appear in exactly $m(u-1)$ blocks. So necessary conditions for the existence of a G-frame of type g^u and index λ are

$$g(u-1) \equiv 0 \pmod{n}, \tag{5.1}$$

$$\lambda g(u-1) \equiv 0 \pmod{\gamma}, \tag{5.2}$$

where $\gamma = \gamma(G)$ is as in (1.5).

In the remainder of this section, we prove the existence of various G-frames. First, we show asymptotic existence (in u) of uniform G-frames with u groups.

Theorem 5.2 *Let $\lambda \in \mathbb{Z}$, $\lambda \geq 0$. Suppose G is a graph with n vertices, $e > 0$ edges, and degrees $d_1, \dots, d_n$. Suppose $g \in \mathbb{Z}$ is such that $\lambda ng/2e \in \mathbb{Z}$ and there is a proper g-coloring of the vertices of G. Then there exists u_0 such that G-frames of type g^u and index λ exist whenever $u \geq u_0$ satisfies* (5.1) *and* (5.2).

Proof We use the powerful method of edge-colored graph decompositions in [4], and imitate several of the examples therein. Let $S = \{1, \dots, g\}$. As edge-color set, we use $(S \times S) \cup S$. For consistency, colors will be denoted by (c_1, c_2) or (c). For a mapping $\kappa \colon V(G) \to S$, define G_κ to be the edge-colored directed graph with vertex set $V(G) \cup \{\infty\}$, and edges as follows: for each $\{x, y\} \in E(G)$, there is a (directed) edge from x to y of color $(\kappa(x), \kappa(y))$, and for each $x \in V(G)$ there is an edge from x to ∞ of color $(\kappa(x))$. Let $\mathcal{G}$ be the set of all such G_κ. Let K_u^* denote the edge-colored graph on u vertices with λ edges of each color (c_1, c_2) and m edges of each color (c) directed between every pair of distinct vertices. Observe that a G-frame of type g^u and index 1 is equivalent to a decomposition of K_u^* into edge-colored graphs in $\mathcal{G}$.

Using the notation in [4], $\mu(H)$ denotes the "edge-vector" of H, which in our case is a vector of length $g^2 + g$, indexed by $(S \times S) \cup S$, whose entry in position (c_1, c_2) or (c) is the number of edges of that color in H. For $x \in V(H)$, define $\tau(H, x)$, the "degree-vector" of H, to be the vector of length $2(g^2 + g)$, with entries corresponding to the indegrees and outdegrees of each color at x. According to the main theorem of [4], it suffices to show that the necessary conditions (5.1) and (5.2) imply: (i) $\lambda u(u-1)\mu(K_u^*)$ is an integral linear combination of the $\mu(G_\kappa)$; (ii) $\lambda(u-1)\tau(K_u^*, x)$ is an integral linear combination of the $\tau(G_\kappa, y)$, $y \in V(G_\kappa)$; and (iii) that some positive rational linear combination of the vectors $\mu(G_\kappa)$ equals $\mu(K_u^*)$.

https://doi.org/10.4153/CMB-2007-050-x Published online by Cambridge University Press

(i) We use Lemma 1.4. Suppose $g^2 + g$ rationals X_{ij}, X_i, $i, j \in S$, are chosen such that for all $\kappa\colon V(G) \to S$, (and some modulus)

$$\sum_{i \neq j}\Big(\sum_{\kappa(T)=\{i,j\}} A(T)\Big) X_{ij} + \sum_{i}\Big(\sum_{\kappa(T)=\{i\}} A(T)\Big) X_{ii} + \sum_{i} |\kappa^{-1}(i)| X_i \equiv 0,$$

where $A(T)$ is the $0, 1$-adjacency map for G defined in Section 2. Let $\{x, y\} \in E(G)$. Taking $\kappa^{-1}(j) = \varnothing, \{x\}, \{y\}, \{x, y\}$, and $\kappa^{-1}(i) = V(G) \setminus \kappa^{-1}(j)$ in each case, we get the congruences

$$2eX_{ii} + nX_i \equiv 0, \tag{5.3}$$

$$\deg(x)(X_{ij} + X_{ji}) + (2e - 2\deg(x))X_{ii} + (n-1)X_i + X_j \equiv 0, \tag{5.4}$$

$$\deg(y)(X_{ij} + X_{ji}) + (2e - 2\deg(y))X_{ii} + (n-1)X_i + X_j \equiv 0, \tag{5.5}$$

$$\begin{aligned}(\deg(x) + \deg(y) - 2)(X_{ij} + X_{ji}) + (2e - 2\deg(x) - 2\deg(y) + 2)X_{ii}\\ + 2X_{jj} + (n-2)X_i + 2X_j \equiv 0.\end{aligned} \tag{5.6}$$

Add (5.3) and (5.6) and subtract (5.4) and (5.5) to get, for all $i, j \in S$,

$$2(X_{ij} + X_{ji}) \equiv 2(X_{ii} + X_{jj}). \tag{5.7}$$

Subtracting (5.4) from (5.3), we have

$$\deg(x)(X_{ij} + X_{ji}) + X_j \equiv 2\deg(x)X_{ii} + X_i. \tag{5.8}$$

By swapping i and j in (5.8), we see

$$2\deg(x)X_{ii} + 2X_i \equiv 2\deg(x)X_{jj} + 2X_j. \tag{5.9}$$

If γ is odd, then $2\gamma \mid \lambda g u(u-1)$. So by (5.9) and (1.5),

$$\lambda g u(u-1)X_{ii} + mu(u-1)X_i \equiv \lambda g u(u-1)X_{jj} + mu(u-1)X_j. \tag{5.10}$$

If γ is even, multiply (5.7) by $\gamma/2$ and combine with (5.8) to get $\gamma X_{ii} + X_i \equiv \gamma X_{jj} + X_j$. By (1.5), we again have (5.10). It follows from (5.3) that

$$\begin{aligned}u(u-1)\Big(\lambda \sum_{i,j\in S} X_{ij} + m\sum_{i} X_i\Big) &\equiv u(u-1)\sum_{i\in S}(\lambda g X_{ii} + mX_i)\\ &\equiv \lambda g^2 u(u-1)X_{11} + mgu(u-1)X_1 \equiv 0.\end{aligned}$$

(ii) We use Lemma 1.4. Suppose $2g^2 + 2g$ rationals X_{ij}, Y_{ij}, X_i, Y_i, $i, j \in S$, are chosen such that, for all $\kappa\colon V(G) \to S$ and all $x \in V(G)$ with $\kappa(x) = j$,

$$\sum_{i=1}^{g} |N(x) \cap \kappa^{-1}(i)|(X_{ij} + Y_{ji}) + X_j \equiv 0, \quad \text{and} \quad \sum_{i=1}^{g} |\kappa^{-1}(i)| Y_i \equiv 0.$$

https://doi.org/10.4153/CMB-2007-050-x Published online by Cambridge University Press

Put $Z_{ij} = X_{ij} + Y_{ji}$. Again, let $\{x, y\} \in E(G)$. The colorings with $\kappa^{-1}(j) = \varnothing$, $\{x\}$, $\{x, y\}$, and $\kappa^{-1}(i) = V(G) \setminus \kappa^{-1}(j)$ give the congruences

$$\deg(x)Z_{ii} + X_i \equiv 0, \tag{5.11}$$

$$\deg(x)Z_{ij} + X_j \equiv 0, \tag{5.12}$$

$$(\deg(x) - 1)Z_{ij} + Z_{jj} + X_j \equiv 0. \tag{5.13}$$

Subtracting (5.13) from (5.12) gives $Z_{ij} \equiv Z_{jj}$ for all $i, j \in S$. By (5.2) and (5.11),

$$(u-1)(\lambda g Z_{ii} + mX_i) \equiv 0.$$

The congruences at vertex ∞ reduce to $nY_i \equiv 0$ and $Y_i \equiv Y_j$ for all i, j. Therefore,

$$\begin{aligned}(u-1)\Big(\sum_{i,j} \lambda Z_{ij} + m\sum_i X_i + m\sum_i Y_j\Big)\\ \equiv (u-1)\sum_i(\lambda g Z_{ii} + mX_i) + mg(u-1)Y_1 \equiv 0.\end{aligned}$$

(iii) As in (i), use variables X_{ij} and X_i, where $i, j \in S$. The sum of all possible $\mu(G_\kappa)$ is of the form $\mathbf{u}_1 = (P\mathbf{j}, Q\mathbf{j}, R\mathbf{j})$, where $m(g-1)P + mQ = \lambda g R$, and $\mathbf{j}$ is the all ones vector of appropriate length. If $\kappa'(V(G)) = \{i\}$, then $\mu(G_{\kappa'})$ has 0 in all entries, except for $2e$ in the entry indexed by X_{ii} and n in the entry indexed by X_i. So the sum of all $\mu(G_{\kappa'})$, $|\kappa'(V(G))| = 1$, is of the form $\mathbf{u}_2 = A(\mathbf{0}, \lambda g\mathbf{j}, m\mathbf{j})$ for some positive $A \in \mathbb{Q}$. At the other extreme, if κ'' is a proper g-coloring of G, then $\mu(G_{\kappa''})$ has entries summing to $2e$ among X_{ij} positions for $i \neq j$, and entries summing to n among X_i positions. Summing over all permutations of this coloring, one has the vector $\mathbf{u}_3 = B(\lambda g\mathbf{j}, \mathbf{0}, m\mathbf{j})$ for some positive $B \in \mathbb{Q}$. Now a nonnegative multiple of either $\mathbf{u}_2$ (if $P \geq Q$) or $\mathbf{u}_3$ (if $P \leq Q$) added to $\mathbf{u}_1$ gives a positive linear combination of the required form. ■

We remark that the hypothesis of G admitting a proper g-coloring is perhaps unnecessary, but provides a tidy proof of a sufficient result for our purposes.

We close this section with a variant of Wilson's fundamental construction, which produces non-uniform G-frames from uniform ones. See [3] for a proof and discussion of the case $G = K_k$.

Lemma 5.3 *Suppose there exist an* $\mathrm{RTD}(u+2, q)$ *and G-frames of types g^u, g^{u+1} and g^{u+2} and index λ. Let $p_1, p_2 \in \mathbb{Z}$ with $0 \leq p_1, p_2 \leq q$. Then there exists a G-frame with index λ having precisely u groups of size qg, one group of size $p_1 g$, and one group of size $p_2 g$.*

6 Recursion

Here, we fix a positive integer λ and a simple graph G, and concern ourselves with admissible orders v for this λ and G. The index of any G-design or G-frame is here assumed to be λ. By Theorem 4.1, there exists a resolvable G-design of order v' for some particular $v' > n$. Our asymptotic construction will use this order v' as a basis.

https://doi.org/10.4153/CMB-2007-050-x Published online by Cambridge University Press

Lemma 6.1 *There exists* $k_0 \equiv 0 \pmod{n}$ *such that for all* $k \geq k_0$ *with* $k \equiv 0 \pmod{n}$*, there exists a* $\mathrm{CRGD}(k(v'-1)+v', v', G, \lambda)$.

Proof Since v' is admissible, (5.1) and (5.2) are satisfied for $g = v'-1$ and $u = k+1$ for any $k \equiv 0 \pmod{n}$. By Theorem 5.2, there exists a G-frame of type $(v'-1)^{k+1}$ for sufficiently large $k \equiv 0 \pmod{n}$. The claim follows directly from Lemma 5.1 with $h = 1$. ■

For two sets of integers X, Y, define XY as the set of all products of an element of X with an element of Y. Write $X \equiv Y \pmod{M}$ if the corresponding sets of least nonnegative representatives modulo M are equal. When M is understood, let $\langle \alpha \rangle$ denote the subgroup of $\mathbb{Z}/M\mathbb{Z}$ generated by α. We now call upon a result of elementary number theory.

Lemma 6.2 *Suppose* $X \equiv 1 + \langle \alpha \rangle$ *and* $Y \equiv 1 + \langle \beta \rangle \pmod{M}$*. Then* $XY \equiv 1 + \langle \gcd\{\alpha, \beta\} \rangle \pmod{M}$.

Since the set of all $v - 1 \in \mathbb{Z}$ satisfying (1.4) is an ideal, the admissible orders are periodic modulo $M = n(v'-1)$. We now observe that the constructions of Sections 3 and 4 yield examples in all admissible congruence classes mod M.

Theorem 6.3 *Let* $M = n(v'-1)$*. For every admissible order* t *for* λ *and* G*,* $0 \leq t < M$*, there exists an* $\mathrm{RGD}(w, G, \lambda)$ *with* $w > M$ *and* $w \equiv t \pmod{M}$.

Proof First, note that we may choose the prime power of Theorem 4.1 to be $1 \pmod{M}$. So it suffices to show that there is an equireplicate $\mathrm{GD}(w, G, \lambda)$ with arbitrarily many resolution classes and $w \equiv t \pmod{M}$.

Let n' be chosen as in Theorem 2.3. Since $n' | v'$, we have $\gcd\{n', M\} = n$. Define X' to be the set of possible u in Theorem 3.3. Let

$$X = 1 + \left\langle \mathrm{lcm}\left\{ n'-1, \frac{\gamma}{\gcd\{\lambda, \gamma\}} \right\} \right\rangle$$

and observe that by (3.1), $X' \equiv X \cap n\mathbb{Z} \pmod{M}$. By Theorem 2.3, there exists an $\mathrm{RGD}(n', G, \lambda^*)$ for $\lambda^* = p\,\mathrm{lcm}\{\lambda_{\min}, \lambda\}$, where $p > M$ is some prime. Define Y' to be the set of possible primes $q > n$ (for this λ^*) in Theorem 3.3. By Dirichlet's Theorem and (3.2), $Y' \supseteq Y$, where

$$Y \equiv 1 + \left\langle \mathrm{lcm}\left\{ \frac{2e}{\gcd\{2e, \lambda\}}, \frac{\gamma}{\gcd\{\gamma, \lambda\}}, \frac{p\,\lambda_{\min}}{\gcd\{\lambda_{\min}, \lambda\}} \right\} \right\rangle \pmod{M}.$$

By Lemma 6.2 and some calculations, $XY \equiv 1 + \langle \alpha \rangle \pmod{M}$, where

https://doi.org/10.4153/CMB-2007-050-x Published online by Cambridge University Press

$$\alpha = \operatorname{lcm}\left\{ \frac{\gamma}{\gcd\{\gamma,\lambda\}}, \gcd\left\{ n'-1, \frac{2e}{\gcd\{2e,\lambda\}} \right\}, \gcd\left\{ n'-1, \frac{\lambda_{\min}}{\gcd\{\lambda_{\min},\lambda\}} \right\} \right\}.$$

By (1.4) and (2.2), $2e|n\gamma$ and $\lambda_{\min}|\gamma$. So the second and third factors in the lcm expression for α divide the first. Since every element in Y' is relatively prime to n,

$$X'Y' \equiv \left(1 + \left\langle \frac{\gamma}{\gcd\{\gamma,\lambda\}} \right\rangle\right) \cap n\mathbb{Z} \pmod{M},$$

covering all representatives of admissible orders mod M. ■

Proof of Theorem 1.3 Take an admissible order t for λ and G, with $0 \le t < M$. Let $w \equiv t \pmod{M}$ be as in Theorem 6.3. We must show that there exists an RGD$(cM + w, G, \lambda)$ for sufficiently large integers c.

Write $w = w' + v'$. Let $g = \gcd(M, w')$. Since both M and w' are divisible by n and γ, Theorem 5.2 guarantees G-frames of type g^u, g^{u+1}, and g^{u+2} and index λ, for some u. Let $k_0 \in \mathbb{Z}$ be as in Lemma 6.1 and $k_1 \in \mathbb{Z}$ be large enough so that by Lemma 1.5 there exists an RTD$(u + 2, k(v' - 1)/g)$ for all $k \ge k_1$. Suppose $l \ge \max\{k_0, k_1\}/n$ and $l' \ge k_0/n$ with $k = nl$ and $k' = nl'$. By Lemma 5.3 there exists a G-frame with exactly u groups of size $k(v' - 1)$, one group of size $k'(v' - 1)$, and one group of size w'. Also, there exist a CRGD$(k(v'-1)+v', v', G, \lambda)$, a CRGD$(k'(v'-1)+v', v', G, \lambda)$ and an RGD$(w' + v', G, \lambda)$. So Lemma 5.1 results in a resolvable G-design of order $(ku+k')(v' - 1) + w' + v' = (lu+l')M + w$ and index λ. The proof is now complete, since any sufficiently large integer c is of the form $lu + l'$, where l, l' are as above. ■

Acknowledgements The authors would like to thank E. R. Lamken and R. M. Wilson for helpful discussions on this topic.

References

[1] P. Adams, D. E. Bryant, and A. Khodkar, *The spectrum problem for λ-fold Petersen graph designs.* J. Combin. Math. Combin. Comput. **34**(2000), 159–176.

[2] S. Chowla, P. Erdős, and E. G. Strauss, *On the maximal number of pairwise orthogonal Latin squres of a given order.* Canad. J. Math. **12**(1960), 204–208.

[3] S. Furino, Y. Miao, and J. Yin, *Frames and Resolvable Designs. Uses, Constructions, and Existence.* CRC Press, Boca Raton, FL, 1996.

[4] E. R. Lamken and R. M. Wilson, *Decompositions of edge-colored complete graphs.* J. Combin. Theory Ser. A **89**(2000), no. 2, 149–200.

[5] J. X. Lu, *An existence theory for resolvable balanced incomplete block designs.* (Chinese) Acta Math. Sinica **27**(1984), no. 4, 458–468.

[6] D. K. Ray-Chaudhuri and R. M. Wilson, *The existence of resolvable block designs.* In: Survey of Combinatorial Theory. North-Holland, Amsterdam, 1971, pp. 361–375.

[7] R. Rees, *Two new direct product-type constructions for resolvable group-divisible designs.* J. Combin. Des. **1**(1993), no. 1, 15–26.

[8] A. Schrijver, *Theory of Linear and Integer Programming.* John Wiley & Sons, Chichester, 1986.

[9] R. M. Wilson, *Cyclotomy and difference families in elementary abelian groups.* J. Number Theory **4**(1972), 17–47.

[10] ———, *Decompositions of complete graphs into subgraphs isomorphic to a given graph.* In: Congressus Numerantium XV, Utilitas Math. Winnipeg, MB. 1976, pp. 647–659.
[11] ———*The necessary conditions for t-designs are sufficient for something.* Congressus Numerantium IV, Utilitas Math. Winnipeg, MB. 1973, pp. 207–215.

Department of Mathematics and Statistics
University of Victoria
Victoria, BC
V8W 3P4
e-mail: dukes@math.uvic.ca

Department of Computer Science,
University of Vermont
Burlington, VT 05405
U.s.A.
e-mail: aling@emba.uvm.edu