Orthogonal 3-GDDs with four groups

P. Dukes

Department of Mathematics 253-37
California Institute of Technology
Pasadena, CA, U.S.A. 91125
dukes@caltech.edu

Abstract

Consider a pair of group divisible designs (GDD) with block size 3, index $\lambda = 1$, and on the same points and groups. They are said to be orthogonal (OGDD) if (i) whenever two blocks, one from each design, intersect in two points, the third points are in different groups; and (ii) two disjoint pairs of points defining intersecting triples in one GDD fail to do so in the other. A question posed by Colbourn and Gibbons, in New Zealand J. Math. **7** (1999), 431–440, asks whether there exists any OGDD with four groups. Despite some nonexistence results, their question is answered in the affirmative here with two computer constructions. Also, two algebraic constructions of related structures help toward some asymptotic existence results.

1 Introduction

A *group divisible design* (GDD) of index λ is a triple $(X, \mathcal{G}, \mathcal{A})$, with $\mathcal{G}$ a partition of the set X into *groups*, $\mathcal{A}$ a collection of subsets (or *blocks*) of X, such that

- every pair of points from the same group is in no block;
- every pair of points from distinct groups meets exactly λ blocks.

Until section 4, $\lambda = 1$ will be assumed. To say the *type* of a GDD is $g_1^{u_1} \cdots g_s^{u_s}$ means there are u_i groups of size g_i for each i, and these are all group sizes. A GDD is *uniform* if all groups have the same size; that is, if it is of type g^u with $gu = |X|$. If all block sizes are in a set K, the notation K-GDD is used. In the case of a triple system, $K = \{3\}$, and uniform group structure g^u, there are the usual necessary conditions:

$$g(u-1) \equiv 0 \pmod 2 \quad \text{and} \quad gu(u-1) \equiv 0 \pmod 3.$$

Let $(X, \mathcal{G}, \mathcal{A}_1)$ and $(X, \mathcal{G}, \mathcal{A}_2)$ be two $\{3\}$-GDDs on the same points and group partition. They are said to be *orthogonal* (denoted OGDD) if

(i) $\{u, v, a\} \in \mathcal{A}_1$ and $\{u, v, b\} \in \mathcal{A}_2$ implies a and b are in different groups;
(ii) $\{u, v, a\}, \{x, y, a\} \in \mathcal{A}_1$ and $\{u, v, w\}, \{x, y, z\} \in \mathcal{A}_2$ implies $w \neq z$.

An OGDD of type 1^v is equivalent to a pair of orthogonal Steiner triple systems (OSTS) of order v. In [3] and [7], OGDDs were used with the standard "filling in holes" construction to prove OSTS(v) exist if and only if $v \equiv 1$ or $3 \pmod 6$, $v \geq 7$ and $v \neq 9$. Since the solution of the OSTS problem, existence of OGDDs, particularly those of uniform type, have generated some interest on their own. The recent paper [2] goes a long way to determining which g and u admit OGDD of type g^u. The theme of that paper can be summarized as follows.

Theorem 1.1. ([2]) *For every positive g, there exists OGDD of type g^u for all but finitely many admissible values of u. For each $u \notin \{4, 6, 9, 14, 22, 26, 34, 38, 58, 94, 142\}$, $u \geq 4$, there exist OGDD of type g^u for all but finitely many admissible values of g.*

An easy consequence of condition (i) above is that an OGDD must have at least four groups, for if u and v are chosen in different groups, then their unique third elements in each GDD must lie in two more distinct groups. Similarly, N mutually orthogonal $\{3\}$-GDDs require at least $N + 2$ groups. Here, the extreme case of OGDDs with exactly four groups is investigated. It is evident from first principles that attention may be restricted to uniform OGDDs.

Proposition 1.2. *Every OGDD with four groups is uniform.*

Proof: Let X be the pointset with group partition $\mathcal{G} = \{G_1, \ldots, G_4\}$. For $i = 1, 2$, let $\mathcal{A}_i$ be the block set of each GDD, and $\Theta_i : \cup_{j \neq k}(G_j \times G_k) \to X$ be the third element relation defined by $\Theta_i(x, y) = z$ iff $\{x, y, z\} \in \mathcal{A}_i$. Fix $x \in G_1$ and define $A_x = \{y \in G_2 : \Theta_1(x, y) \in G_3\}$. Let $y' \in G_2$. By orthogonality condition (i), $\Theta_2(x, y') \in G_3$ iff $y' \notin A_x$. There is now a well-defined map $f : G_2 \to G_3$ given by $f(y) = \Theta_1(x, y)$ when $y \in A_x$ and $f(y) = \Theta_2(x, y)$ otherwise. Suppose $f(y_1) = f(y_2)$. Then the G_3 third elements of $\{x, y_1\}$ and $\{x, y_2\}$ (in the appropriate GDDs) are equal. Since y_1 and y_2 both belong to G_2, it must be that $y_1 = y_2$ to avoid a contradiction to either $\lambda = 1$ or condition (i). So the mapping f is injective. Therefore, $|G_2| \leq |G_3|$. Since the naming of groups is immaterial, all their sizes are equal. □

Remark. The groups must have even size by the necessary conditions with $u = 4$. Also, it is reported in [2] that $g \geq 6$ is necessary by exhaustive search.

2 Cyclic Automorphisms

A GDD $(X, \mathcal{G}, \mathcal{A})$ of type g^u is *m-cyclic* if X can be written as $\mathbf{Z}_{gu/m} \times \mathbf{Z}_m$, with automorphism $\alpha : (x, i) \mapsto (x + 1, i)$ fixing both $\mathcal{G}$ and $\mathcal{A}$. Usually, x_i is written for (x, i). An orthogonal pair of such $\{3\}$-GDDs is said to be an m-cyclic OGDD. In order for such an object to exist, it is necessary that $m|gu$ and $6|mg(u-1)$. The advantage of designs with automorphisms is that their block sets may be described merely by orbit representatives (or base blocks) for the automorphism. Normally, 1-cyclic designs are simply called *cyclic*, and the subscript 0 is omitted. The cosets of $\{0, u, \ldots, (g-1)u\}$ in $\mathbf{Z}_{gu}$ define the unique group structure for a 1-cyclic $\{3\}$-GDD of type g^u. There are perhaps several distinct group structures possible when $m > 1$. The next result concerns the case when the generating automorphism is transitive (cyclic) within the groups.

Proposition 2.1. *There does not exist m-cyclic OGDD of type g^4 with automorphisms transitive on each group.*

Proof: As in the proof of Proposition 1.2, fix a point x in one group and obtain a bijective map f between the points of two other groups. Let a generating m-cyclic automorphism be α, and suppose it acts transitively on each group. It cannot be the case for $\alpha^n \neq$ identity that both $f(y) = z$ and $f(\alpha^n y) = \alpha^n z$. For otherwise, $\{x, y, z\}$ and $\{\alpha^{-n}x, y, z\}$ are both blocks of the OGDD. This contradicts either $\lambda = 1$ or condition (i) for orthogonality, since x and $\alpha^{-n}x$ are in the same group. View f as a matching in $K_{g,g}$. Label the vertices of each partite set as $\{0, 1, \ldots, g-1\}$ so that the orbit of any point under $\{\alpha^n\}$ in either of the two groups in question is labeled in order (mod g) with increasing n. The matching, say $\{(i, a_i) : 0 \leq i < g\}$, has by the argument above the property that $a_i - i$ achieves every residue (mod g) exactly once. So since g is even, $\sum_i (a_i - i) \equiv g/2 \pmod{g}$. But $\sum_i (a_i - i) \equiv 0$ because of the matching. This is a contradiction. □

Note that the proof of the last two nonexistence claims uses only condition (i) on orthogonality, generally viewed as the weaker constraint. However, it seems natural that this condition is restrictive when there are exactly four groups. Proposition 2.1 really only applies to cyclic, and certain 2-cyclic and 4-cyclic OGDDs. Still, it gives insight into why computational methods had previously failed to produce any OGDD with four groups, as certain potentially helpful automorphisms reducing the search space are lost.

It shall be shown now that specifying a 2-cyclic automorphism which is *not* transitive on the groups can, however, produce successful searches. For an OGDD of type g^4, consider the set $X = \mathbf{Z}_{2g} \times \{0, 1\}$, arranged into groups

$$G_j = \{j, j+4, j+8, \ldots, j+4(g/2-1)\} \times \{0, 1\}, \quad j = 0, 1, 2, 3.$$

The implied 2-cyclic automorphism acts in two orbits on each group. By hill-climbing to find one set of base blocks, then backtracking to find a compatible second set of base blocks (a method also used in [2]), the direct constructions below were found.

Example 2.2. Base blocks for OGDDs of type 8^4 and 12^4 with points and groups as above, are given along with an *orthogonality certificate*. This is a list of third elements in the second GDD of all pairs occurring with 0_0 and 0_1 in the first GDD. Orthogonality amounts to each list consisting of distinct elements not from the first group.

OGDD of type 8^4

$\{0_0, 2_1, 9_1\}, \{0_0, 2_0, 5_0\}, \{0_0, 3_1, 13_1\}, \{0_0, 15_1, 1_1\}, \{0_0, 10_0, 9_0\}, \{0_0, 7_1, 6_1\},$
$\{0_0, 10_1, 5_1\}, \{0_0, 11_1, 14_1\};$
$\{0_0, 6_0, 1_0\}, \{0_0, 14_0, 1_1\}, \{0_0, 6_1, 13_0\}, \{0_0, 14_1, 13_1\}, \{0_0, 7_1, 5_1\}, \{0_0, 11_1, 9_0\},$
$\{0_0, 15_1, 10_1\}, \{0_1, 6_1, 9_1\}$

orthogonality certificate:
$0_0 : 15_1, 11_1, 13_0, 14_1, 6_1, 10_0, 15_0, 1_1, 2_0, 9_0, 11_0, 5_1$
$0_1 : 1_0, 14_0, 11_1, 5_0, 15_0, 9_1, 6_0, 15_1, 13_1, 10_1, 2_1, 11_0$

OGDD of type 12^4

$\{0_0, 14_1, 17_0\}, \{0_0, 11_1, 9_1\}, \{0_0, 2_0, 17_1\}, \{0_0, 19_1, 13_0\}, \{0_0, 7_1, 18_1\}, \{0_0, 14_0, 9_0\},$
$\{0_0, 3_1, 1_0\}, \{0_0, 10_1, 13_1\}, \{0_0, 22_1, 21_0\}, \{0_0, 6_0, 5_1\}, \{0_1, 14_1, 5_1\}, \{0_1, 18_1, 1_1\};$
$\{0_0, 10_0, 13_0\}, \{0_0, 18_0, 21_1\}, \{0_0, 22_0, 9_1\}, \{0_0, 2_1, 1_1\}, \{0_0, 23_1, 9_0\}, \{0_0, 19_1, 10_1\},$
$\{0_0, 6_1, 1_0\}, \{0_0, 18_1, 5_0\}, \{0_0, 7_1, 17_1\}, \{0_0, 15_1, 17_0\}, \{0_1, 2_1, 21_1\}, \{0_1, 6_1, 17_1\}$

orthogonality certificate:
$0_0 : 11_0, 22_0, 6_1, 19_0, 5_1, 14_0, 21_1, 1_1, 3_1, 9_1, 18_0, 2_1, 5_0, 15_1, 23_1, 10_0, 15_0, 17_0$
$0_1 : 1_1, 11_0, 17_0, 18_1, 15_0, 22_0, 23_1, 3_1, 9_0, 6_1, 13_0, 22_1, 19_0, 13_1, 2_0, 7_1, 5_0, 10_1$

3 Recursive Methods and Modified GDDs

Let L be a Latin square with associated quasigroup $(Q, \otimes)$, (or simply Q) so that $x_1 \otimes x_2 = x_3$ iff x_3 is in entry (x_1, x_2) of L. The six *conjugates* of Q are Q^σ for $\sigma \in \mathcal{S}_3$, with operation given by $x_{\sigma(1)} \otimes^\sigma x_{\sigma(2)} = x_{\sigma(3)}$ iff $x_1 \otimes x_2 = x_3$. Two quasigroups (Latin squares) for which every conjugate of one is orthogonal to every conjugate of the other form a pair of *conjugate orthogonal quasigroups*, or COQ. It is well known that COQ exist for all but finitely many orders, yet the full spectrum (denoted $\mathcal{COQ}$) of those orders is still unknown. See [7], for example, for more on this subject and the following construction.

Lemma 3.1. *If there exists OGDD of type g^u and COQ(m) then there exists OGDD of type $(mg)^u$.*

The two computer findings in Example 2.2, together with Lemma 3.1, provide OGDD of type g^4 for almost all g divisible by 8 or 12. By using another type of design, however, a stronger asymptotic result can be achieved.

A *modified group divisible design* (MGDD) of type (u, v) is a set X with two partitions, $\mathcal{G}$ into v holes of size u, and $\mathcal{H}$ into u holes of size v, such that $|G \cap H| = 1$ for all $G \in \mathcal{G}$ and $H \in \mathcal{H}$. Additionally, there is a block set $\mathcal{A}$ so that every pair of points occurs together in a block if and only if it does not appear in a hole of either $\mathcal{G}$ or $\mathcal{H}$. (The term "hole" will be used in place of "group" to avoid confusion later.) Two $\{3\}$-MGDDs on the same points and holes are orthogonal (OMGDD) if: (i') $\{u, v, a\} \in \mathcal{A}_1$ and $\{u, v, b\} \in \mathcal{A}_2$ implies a and b are in different holes of $\mathcal{G}$ *and* of $\mathcal{H}$; as well as orthogonality condition (ii) hold. Loosely speaking, these approximate

OGDDs with four groups. In [2], a useful construction with these designs is given, and the existence of a few small OMGDDs with four holes of one kind is reported.

Lemma 3.2. ([2]) *Suppose there is a K-GDD of order g and group sizes $g_1, \ldots, g_t$. If for some $u \leq t$ there is an OMGDD of type (k, u) for every $k \in K$ and OGDD of type g_i^u for every i, then there is an OGDD of type g^u.*

Lemma 3.3. ([2]) *There exist OMGDD of type $(4, v)$ for $v = 7, 11, 13, 15, 17, 19, 21$.*

An infinite family of OMGDD with four holes (of one kind) will now be constructed from classical triple systems in the finite fields.

Proposition 3.4. *For every prime power $q \equiv 1 \pmod 6$, there exists OMGDD of type $(4, q)$.*

Proof: Let $X = \mathbf{F}_q \times \mathbf{K}$, where $\mathbf{F}_q$ is a field of order $q = 6t+1$ with generator ω and $\mathbf{K} = \{0, \alpha, \beta, \gamma\}$ is the Klein group on four elements. Write $\mathbf{K}^* = \mathbf{K} \setminus \{0\}$. Define the two sets of holes $\{\{a\} \times \mathbf{K} : a \in \mathbf{F}_q\}$ and $\{\mathbf{F}_q \times \{b\} : b \in \mathbf{K}\}$. Clearly, a first hole and a second hole intersect in exactly one element of X. It is well-known (see [5] for example) that the zero-sum base triples $\omega^e\{1, \omega^{2t}, \omega^{4t}\}$, $0 \leq e < t$, when developed additively in the field, form a Steiner triple system. Fix an ordering on each base block. Now for each of these t ordered triples (x, y, z), include

$$\{(x,\alpha),(y,\beta),(z,\gamma)\}, \{(x,\beta),(y,\gamma),(z,\alpha)\}, \{(x,\gamma),(y,\alpha),(z,\beta)\} \in \mathcal{A}_1,$$

and generate these blocks additively over $\mathbf{F}_q \times \mathbf{K}$. Define $\mathcal{A}_2 = -\mathcal{A}_1$ to be the elementwise negative of these blocks. The differences among the zero-sum blocks of each system are $\{\pm(x-y), \pm(y-z), \pm(x-z)\} \times \{\alpha, \beta, \gamma\}$, exhausting all elements of $\mathbf{F}_q^* \times \mathbf{K}^*$. This proves $\mathcal{A}_1$ and $\mathcal{A}_2$ each form a $\{3\}$-MGDD on the given hole partitions. As before, let $\Theta_i(\cdot, \cdot)$ be the third element function for $\mathcal{A}_i$. It is enough to show Θ_2 maps all pairs occurring with $(0,0)$ in $\mathcal{A}_1$ to distinct elements of $\mathbf{F}_q^* \times \mathbf{K}^*$. Note

$$\Theta_2((y-x,\gamma),(z-x,\beta)) = (y+z-x,0) + \Theta_2((-z,\gamma),(-y,\beta)) = (-3x,\alpha),$$

since $x+y+z=0$. The other pairs are similar. But the base triples of the original STS have no repetition among their elements. So $\Theta_2\Theta_1^{-1}(0,0) = (-3H) \times \mathbf{K}^*$, where H is the half-set of (non-zero) field elements in the base triples of the STS. This establishes orthogonality. □

Remark. This is a variant of *opposite orthogonal* STS, introduced in [6]. Such objects enjoy the property that their zero-sum base blocks are disjoint. For this reason, a concrete algebraic presentation was chosen here even though the proof can be modified to use *any* OSTS pair, even of non-prime-power order.

Theorem 3.5. *There exist OGDD of type g^4 for all but finitely many $g \equiv 0 \pmod 4$.*

Proof: This is similar to Corollary 8.2 of [2]. Let K denote the set of v for which an OMGDD of type $(4, v)$ exists. For a fixed u, the spectrum of OMGDD with type (u, v) is PBD-closed in v. Let K' be the elements of K which are 1 greater than $\mathcal{COQ}$ multiples of 8 or 12. Observe that from Lemma 3.3 (or for fewer exceptions, Proposition 3.4) that the closure of K' contains all sufficiently large 1 (mod 4) integers. So there exists g_0 such that $g > g_0$ and $g \equiv 0 \pmod 4$ implies the existence of an OMGDD of type $(4, g+1)$. Delete one point from a nontrivial K'-PBD on $g+1$ points. The result is a K'-GDD having group sizes in $8 \cdot \mathcal{COQ} \cup 12 \cdot \mathcal{COQ}$. Lemmas 3.1 and 3.2 applied with the OGDDs of type 8^4 and 12^4 given earlier yields an OGDD of type g^4. □

The existence problem remains open for type g^4, where $g \equiv 2 \pmod 4$, and also for g among the possible exceptions from Theorem 3.5, the smallest being $g = 16$. A single example of an OGDD with four groups of size $g \equiv 2 \pmod 4$ would settle asymptotic existence, however. A computer construction of this kind seems to be difficult due to Proposition 2.1 and the fact that $g/2$ is odd. The author would like to thank Peter Gibbons for attempting hill-climbs to types 10^4 and 18^4.

Conjecture 3.6. *There exists OGDD of type g^4 for all but finitely many even g.*

4 Unseparated OGDDs

Here, asymptotic existence is established for a somewhat weaker structure with $\lambda = 2$. To this end, a symmetrization of orthogonality condition (ii) must be introduced. An OGDD with block sets $\mathcal{A}_1$ and $\mathcal{A}_2$ is *skew-orthogonal* (abbreviated SOGDD) if

(iii) $\{u, v, a\}, \{x, y, w\} \in \mathcal{A}_1$ and $\{u, v, z\}, \{x, y, a\} \in \mathcal{A}_2$ implies $w \neq z$.
(Note $u = x$ is a possibility.)

Consider now a $\{3\}$-GDD with $\lambda = 2$. Suppose whenever $\{u, v, a\}, \{u, v, b\}$ are blocks, a and b are in different groups. Also, suppose it avoids the configuration of triples $\{u, v, a\}$, $\{u, v, b\}$, $\{x, y, a\}$, $\{x, y, b\}$ for $\{u, v\} \neq \{x, y\}$. The design will then be called an *unseparated* OGDD. If an unseparated OGDD were decomposable into a pair of GDDs with index $\lambda = 1$, that pair would be skew-orthogonal. See [4] for more on skew-orthogonal triple systems. The following result sheds light on why $g \equiv 2 \pmod 4$ is the difficult case for existence of OGDDs with four groups of size g.

Proposition 4.1. *An unseparated OGDD of type g^4 is equivalent to four quasigroups (Latin squares) Q_j, $1 \leq j \leq 4$, of order g with the following orthogonality relations on their conjugates:*

$$Q_1 \perp Q_2, \quad Q_1^{(23)} \perp Q_3, \quad Q_1^{(123)} \perp Q_4,$$

$$Q_2^{(23)} \perp Q_3^{(23)}, \quad Q_2^{(123)} \perp Q_4^{(23)}, \quad Q_3^{(123)} \perp Q_4^{(123)}.$$

Proof: Let X be a set with $|X| = g$. Represent points of the GDD as (x, i), $x \in X$, $i = 1, 2, 3, 4$ so that the groups are $X \times \{i\}$. For any $a, b \in X$, there is a unique $c \in X$ such that $\{(a, 1), (b, 2), (c, 3)\}$ is a triple. Define a quasigroup operation on X by $a \oplus_1 b = c$. Similarly define $\oplus_2$, $\oplus_3$ and $\oplus_4$ for triples (ordered by group number) in $X \times \{1, 2, 4\}$, $X \times \{1, 3, 4\}$ and $X \times \{2, 3, 4\}$, respectively. Let Q_j be the quasigroup $(X, \oplus_j)$. The avoided configuration for the unseparated OGDD translates precisely into the required orthogonality relations. This construction is clearly reversible. □

Corollary 4.2. *There does not exist SOGDD of type* 6^4.

Proof: Such an SOGDD gives rise to an unseparated OGDD by uniting block sets. By the proposition, this would result in a pair of orthogonal Latin squares of order 6, which is impossible. □

Theorem 4.3. *Unseparated OGDD of type* g^4 *exist for all but finitely many* g.

Proof: Set $Q_2 = Q_1^{(12)}$ and $Q_4 = Q_3^{(12)}$ in Proposition 4.1. It is certainly sufficient additionally that every conjugate of Q_1 be orthogonal to every conjugate of Q_3. So it suffices to prove asymptotic existence of COQ(g) with the extra property that the pair of quasigroups are each orthogonal to their own (12)-conjugates. Now if g is a prime power, there exist idempotent quasigroups over the finite field of order g given by the operations $x \otimes_\lambda y = \lambda x + (1 - \lambda)y$, $\lambda \neq 0, 1$. It is routine to verify that $\kappa \neq \lambda$ implies $\otimes_\kappa$ and $\otimes_\lambda$ are orthogonal. As with the work on COQs found in [7], it follows easily that in any large enough finite field, idempotent COQs with the desired extra property exist. The Bose-Parker-Shrikhande construction [1] preserves the orthogonality of a Latin square with its transpose. Thus the theorem follows. □

Unfortunately, it is not clear when, for g even, such a design is decomposable. Using a computer, the author generated many unseparated OGDDs as in Theorem 4.3 by using different affine maps in finite fields of characteristic two. None were found to decompose into an SOGDD pair, however. So there remain no examples known of SOGDD with four groups. It should be noted that a "mostly" decomposable index two design of this kind exists asymptotically for g odd. Simply combine block sets of a skew OMGDD of type $(4, g)$ from Proposition 3.4 and fill in all the size four holes with complete (twofold) triple systems on four points.

Acknowledgments

The OGDD of type 12^4 was a somewhat difficult search found on a Pentium Pro based Beowulf Cluster at Caltech's Center for Advanced Computing Research. An NSERC postgraduate scholarship helped support this work as well.

References

[1] R. C. Bose, S. S. Shrikhande, and E. T. Parker, *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture,* Canad. J. Math. **12** (1960), 189–203.

[2] C. J. Colbourn and P. B. Gibbons, *Uniform orthogonal group divisible designs with block size three,* New Zealand J. Math. **7** (1999), 431–440.

[3] C. J. Colbourn, P. B. Gibbons, R. Mathon, R. C. Mullin and A. Rosa, *The spectrum of orthogonal Steiner triple systems*, Canad. J. Math. **46(2)** (1994), 239–252.

[4] P. Dukes and E. Mendelsohn, *Skew-orthogonal Steiner triple systems,* J. Combin. Des. **7** (1999), 431–440.

[5] R. C. Mullin and E. Nemeth, *On furnishing Room squares*, J. Combin. Theory **7** (1969), 266–272.

[6] S. Schreiber, *Cyclical Steiner triple systems orthogonal to their opposites,* Discrete Math. **77** (1989), 281–284.

[7] D. R. Stinson and L. Zhu, *Orthogonal Steiner triple systems of order* $6t + 3$, Ars Combin. **31** (1991), 33–64.

(Received 31/7/2001)