Multi-letter Youden rectangles from quadratic forms

Peter J. Cameron

School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, UK

Abstract

Some infinite families of *systems of linked symmetric designs* (or SLSDs, for short) were constructed by Cameron and Seidel [3] using quadratic and bilinear forms over $\mathrm{GF}(2)$. The smallest of these systems was used by Preece and Cameron [9] to construct certain designs (which they called *fully-balanced hyper-graeco-latin Youden 'squares'*). The purpose of this paper is to construct an infinite sequence of closely related designs (here called *multi-letter Youden rectangles*) from the SLSDs of Cameron and Seidel. These rectangles are $k \times v$, with $v = 2^{2n}$ and $k = 2^{2n-1} \pm 2^{n-1}$. The paper also provides a non-trivial example of how to translate from the combinatorial view of designs (sets with incidence relations) to the statistical (sets with partitions).

1 Symmetric BIBDs and Youden squares

A symmetric balanced incomplete-block design (SBIBD), or symmetric 2-design, can (like any incidence structure) be represented by a graph (its *incidence graph* or *Levi graph*). The vertex set of the graph Γ is the disjoint union of two sets X_1 and X_2, and each edge has one end in X_1 and the other in X_2. The graph has the properties

- $|X_1| = |X_2| = v$;
- for $\{i, j\} = \{1, 2\}$, any point in X_i has exactly k neighbours in X_j;
- for $\{i, j\} = \{1, 2\}$, any two points in X_i have exactly λ neighbours in X_j.

Any regular bipartite graph has a 1-*factorisation*, a partition of the edge set into k parts or 1-factors of v edges each, where the edges of each 1-factor partition the vertices. (This is a well-known consequence of Hall's Marriage Theorem, given explicitly in this case by Smith and Hartley [12].) The structure given by a SBIBD and a 1-factorisation of its incidence graph is called a *Youden square*. It can be represented in various ways, for example:

- As a set with three partitions: the set C is the set of edges of the graph (or flags in the design); there is a partition $\mathcal{A}$ into k sets of size v given by the 1-factorisation; and there are two partitions $\mathcal{B}_1$ and $\mathcal{B}_2$ into v sets of size k corresponding to the sets X_1 and X_2, where parts in $\mathcal{B}_i$ are labelled by vertices in X_i, the part labelled p consisting of all edges incident with p. Note that the partitions $\mathcal{A}$ and $\mathcal{B}_i$ are *orthogonal* (in the sense that a part of $\mathcal{A}$ and a part of $\mathcal{B}_i$ meet in one point). Also, parts labelled by $p_1 \in X_1$ and $p_2 \in X_2$ meet in at most one point, the intersection being non-empty if and only if p_1 and p_2 are incident. So the original SBIBD (as incidence structure) and the 1-factorisation of its incidence graph can be recovered from the set of partitions. This is the representation used by Bailey [1], and is the most relevant statistically: C is the set of experimental units, and the partitions correspond either to treatments or to "nuisance factors" on C. See [2] for further discussion of this viewpoint.
- As a square array: number the 1-factors from 1 to k and the points of X_1 and X_2 from 1 to v. Then take the $v \times v$ matrix whose (i, j) entry is equal to l if the ith point of X_1 and the jth point of X_2 are incident and the edge joining them belongs to the lth 1-factor, and is blank otherwise. (Replacing all non-blank entries by 1 and blanks by 0 gives the *incidence matrix* of the SBIBD.) This is the representation used by Fisher [4] in presenting Youden's concept, and is probably the reason why they are called "squares", whereas the following representation would suggest "rectangles".
- As a Latin rectangle: with the above numbering, take the $k \times v$ array whose (i, j) entry is l if the lth point of X_2 is joined to the jth point of X_1 by an edge of the ith 1-factor. This is the representation used by Youden [13], and is the one most commonly used in view of its compactness, although it obscures the symmetry between X_1 and X_2.

In the case of a SBIBD arising from a difference set in a group A, we have an action of A on the graph Γ so that the orbits are X_1 and X_2 and the action on each orbit is regular. In this case, A permutes the edges in k orbits each of size v; the orbits form a 1-factorisation.

See Preece [8] for a survey of Youden squares.

2 SLSDs and MYRs

A *system of linked SBIBDs*, or SLSD for short, can be represented by a multipartite graph Γ with r classes $X_1, \ldots, X_r$, satisfying the conditions

- for any distinct indices $i, j \in \{1, \ldots, r\}$, the induced subgraph on $X_i \cup X_j$ is the incidence graph of a SBIBD (with parts X_i and X_j), having parameters (v, k, λ) independent of i and j;
- there exist integers x and y such that, for any distinct indices $i, j, l \in \{1, \ldots, r\}$,

and any vertices $p_i \in X_i$ and $p_j \in X_j$, the number of common neighbours of p_i and p_j in X_l is equal to x if p_i and p_j are adjacent, and to y otherwise.

The designs to be constructed here will be called multi-letter Youden rectangles, or MYRs for short. A *multi-letter Youden rectangle* consists of a set C of vk *cells*, together with a partition $\mathcal{A}$ of C into k sets of size v, and r partitions $\mathcal{B}_1, \ldots, \mathcal{B}_r$ of C into v sets of size k, satisfying the following conditions:

- for $i = 1, \ldots, r$, the partitions $\mathcal{A}$ and $\mathcal{B}_i$ are *orthogonal* (that is, each part of $\mathcal{A}$ meets each part of $\mathcal{B}_i$ in one cell);
- for $i, j = 1, \ldots, r$ with $i \neq j$, each part of $\mathcal{B}_i$ meets each part of $\mathcal{B}_j$ in at most one cell (and we call two such parts *incident* if their intersection is non-empty);
- The sets $\mathcal{B}_1, \ldots, \mathcal{B}_r$, with the incidence relation just defined, form a SLSD.

We can represent the MYR by a $k \times v$ rectangle whose entries are $(r-1)$-tuples, in a similar way to the representation of a Youden square as a Latin rectangle. We number the parts of each partition $\mathcal{B}_i$ from 1 to v, and the parts of $\mathcal{A}$ from 1 to k; then the (i, j) entry of the rectangle is the $(r-1)$-tuple $(x_2, \ldots, x_r)$, where x_l is the number of the part of $\mathcal{B}_l$ containing the cell lying in the ith part of $\mathcal{A}$ and the jth part of $\mathcal{B}_1$. This is the representation used in [9], and explains the name chosen for these designs.

If A_{ij} is the incidence matrix of the incidence structure $(\mathcal{B}_i, \mathcal{B}_j)$, we have $A_{ij}^\top = A_{ji}$, $A_{ij}A_{ji} = (k-\lambda)I + \lambda J$, and $A_{ij}A_{jl} = (x-y)A_{il} + yJ$ for i, j, l distinct, where J is the all-1 matrix. Thus our definition, for $r = 3$, is stronger than the definition of a *Freeman–Youden rectangle* or *balanced superimposition of Youden squares* (see [8,10,11]), which requires the first two matrix equations above but replaces the third by

$$A_{ij}A_{jl}A_{li} + A_{il}A_{lj}A_{ji} = fI + gJ$$

for some f, g. See [1], Section 9, for further comments on this.

Theorem 1 *There exists a multi-letter Youden rectangle with $v = 2^{2n}$, $k = 2^{2n-1} + \varepsilon 2^{n-1}$, and $r = 2^n$, for any $n \geq 2$, where $\varepsilon = \pm 1$.*

The case $n = 2$ of this theorem is proved in [9]. In general, the MYRs will be constructed from some of the SLSDs from [3] in the way that Youden squares are constructed from SBIBDs.

In order to do this, we require an extra condition on the SLSD. A *full clique* in a SLSD is a set of vertices, containing one from each of the sets X_i, whose vertices are pairwise adjacent. (So a full clique contains r vertices.) Not all SLSDs have full cliques, as we shall see.

A *full clique cover* is a set of full cliques with the property that every edge is contained in exactly one full clique in the set. (So the number of full cliques in a full clique cover is vk.) A 1-*factor* is a set of v full cliques covering all vertices just once; and a 1-*factorisation* or *resolution* is a partition of the full clique cover into 1-factors. I do not know whether 1-factorisations of full clique covers always exist. However, if there is a group A of automorphisms of the full clique cover whose vertex-orbits are $X_1,\ldots,X_r$ and which acts regularly on each orbit, then the orbits of A on full cliques form a 1-factorisation.

Now, from a resolution of a full clique cover, we construct a MYR as follows:

- the cells are the vk full cliques;
- the partition $\mathcal{A}$ is the resolution of the full clique cover;
- for $i = 1,\ldots,r$, a part of the partition $\mathcal{B}_i$ is the set of full cliques containing a vertex of X_i.

3 Constructing the SBIBDs

This section and the next are based on [3].

Let V be a vector space over the field F. A *bilinear form* on V is a function B from $V \times V$ to F which is linear in each argument. It is *non-degenerate* if no non-zero vector is 'orthogonal' to the whole space, that is, if $B(x,y) = 0$ for all $y \in V$ implies $x = 0$ (and similarly with x and y interchanged).

A *quadratic form* is a function Q from V to F satisfying the two conditions

- $Q(cx) = c^2Q(x)$ for all $c \in F$, $x \in V$;
- the function B defined by

$$B(x,y) = Q(x+y) - Q(x) - Q(y)$$

  for $x,y \in V$, is bilinear.

(We say that B is obtained by *polarising* Q.) If B is non-degenerate, we say that Q is *non-singular*. (The definition of a non-singular quadratic form is broader than this, but the difference will not concern us.)

If the characteristic of F is not 2, then the form B is *symmetric*, that is, $B(x,y) = B(y,x)$, and the quadratic form can be recovered from B by the formula $Q(x) = \frac{1}{2}B(x,x)$.

On the other hand, if the characteristic of F is equal to 2, then we have $B(x,x) = 0$ for all $x \in V$. A form with this property is called *alternating*. Moreover, two

quadratic forms Q and Q' polarise to the same bilinear form if and only if they differ by a *semilinear form*, a function L from V to F satisfying $L(x+y) = L(x)+L(y)$ and $L(cx) = c^2L(x)$ for all $c \in F$, $x,y \in V$. (Note that, if the field is GF(2), then semilinear forms are just linear forms, since $c^2 = c$ for all $c \in F$.)

We also note that a non-degenerate alternating bilinear form can be defined on a vector space of dimension n if and only if n is even.

We now restrict to the case $F = \mathrm{GF}(2)$. Let B be any alternating bilinear form on a $2n$-dimensional vector space over F. The set $Q(B)$ of quadratic forms which polarise to B has 2^{2n} members. If Q is one member of this set, then all others can be obtained by adding linear forms to Q. Suppose that B is non-degenerate. Then any linear form can be written as $L(x) = B(v,x)$ for some vector $v \in V$. So

$$Q(B) = \{Q(x)+B(v,x) : v \in V\} = \{Q(x+v)+Q(v) : v \in V\}.$$

Let $X = \{x \in V : Q(x) = 0\}$ be the set of *zeros* of Q. Then the set of zeros of $Q(x)+B(v,x)$ is obtained by translating X by v, and complementing this set in V if $Q(v) = 1$. So any quadratic form in $Q(B)$ has either N or $2^{2n}-N$ zeros, for some N. It is a standard result (see [3]) that $N = 2^{2n-1}+\varepsilon 2^{n-1}$, where $\varepsilon = \pm 1$. We say that the form Q has *type* ε if it has $2^{2n-1}+\varepsilon 2^{n-1}$ zeros. (The type is essentially the *Arf invariant* of the form; more precisely, the type is $(-1)^\alpha$, where α is the Arf invariant.)

Now the set X of zeros of Q is a difference set in the additive group of the vector space V, and so gives rise to a symmetric BIBD, whose points are the vectors in V and whose blocks are the translates of X; as we have seen, these are the zero sets of the quadratic forms in $Q(B)$, complemented in the case of forms of type opposite to that of Q.

This design has a more symmetrical description, as follows. (The proof that this is the same is an exercise, or is given in [3].) Let B_1 and B_2 be two alternating bilinear forms on V, whose difference $B_1 - B_2$ is non-degenerate. Then the points and blocks of the SBIBD are the sets $Q(B_1)$ and $Q(B_2)$ respectively; a point Q_1 and block Q_2 are incident in the design D_ε if and only if the form $Q_1 - Q_2$ (which is non-singular) has type ε.

The design D_ε has $v = 2^{2n}$, $k = 2^{2n-1}+\varepsilon 2^{n-1}$ and $\lambda = 2^{2n-2}+\varepsilon 2^{n-1}$.

4 Constructing the SLSDs

As in the previous section, let V be a vector space of dimension $2n$ over the field $F = \mathrm{GF}(2)$. A set $\mathcal{B}$ of alternating bilinear forms is said to be a *non-degenerate set*

if, for any $B_1, B_2 \in \mathcal{B}$, the form $B_1 - B_2$ is non-degenerate. Given a non-degenerate set $\mathcal{B}$ and a value $\varepsilon = \pm 1$, we define a SLSD $S_\varepsilon(\mathcal{B})$ as follows: the elements are the quadratic forms in the sets $Q(B)$ for $B \in \mathcal{B}$; forms $Q_i \in Q(B_i)$ and $Q_j \in Q(B_j)$ are incident if $Q_i - Q_j$ has type ε. It follows from the description in the preceding section that the first condition in the definition of a SLSD is satisfied; see [3] for a proof that the second condition holds too.

There are two known constructions for non-degenerate sets of bilinear forms. The second of these is essentially due to Kerdock [5], and produces sets of cardinality $v/2 = 2^{2n-1}$; this is the maximum possible cardinality (see Section 7). However, the Kerdock sets do not have full clique covers in general.

The other construction produces sets of cardinality $\sqrt{v} = 2^n$; it is these which we shall use. They are additively closed sets of the maximum possible size (see Section 7).

Let $K = \mathrm{GF}(2^n)$. There is a F-linear map from K onto F, the *trace map*, given by

$$\mathrm{Tr}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}.$$

(Note that $x^{2^n} = x$ for all $x \in K$.)

Let V be a 2-dimensional vector space over K. By restricting scalars from K to F, V becomes a $2n$-dimensional vector space over F. If b is an alternating bilinear form on V as K-space, then $B = \mathrm{Tr}(b)$ is an alternating bilinear form on V as F-space; and B is non-degenerate if and only if b is. Similarly, the traces of the quadratic forms (on the K-space V) polarising to b are precisely the quadratic forms (on the F-space V) polarising to B.

Now take b to be any non-degenerate alternating bilinear form on the K-space V (for example, take $b((x_1,x_2),(y_1,y_2)) = x_1y_2 - x_2y_1$). Then αb is also a non-degenerate alternating bilinear form, for any non-zero $\alpha \in K$. We have

$$\mathrm{Tr}(\alpha_1 b) - \mathrm{Tr}(\alpha_2 b) = \mathrm{Tr}((\alpha_1 - \alpha_2)b)$$

for $\alpha_1 \neq \alpha_2$. So the 2^n forms

$$\{\mathrm{Tr}(\alpha b) : \alpha \in K\}$$

comprise a non-degenerate set of cardinality 2^n, and so give rise to a SLSD with $r = 2^n$.

5 Constructing the MYRs

We must now produce the full clique cover and its 1-factorisation. The argument uses a little group theory.

The explicit form of b given in the last section is the determinant of the matrix $\begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$. It follows from this that the *special linear group* $\mathrm{SL}(2,2^n)$ of 2×2 matrices of determinant 1 over K preserves b, and hence each of the forms $\mathrm{Tr}(\alpha b)$. Thus the product $A\cdot\mathrm{SL}(2,2^n)$, where A is the additive group of V, acts on the SLSD, fixing each of the sets $X_1,\ldots,X_r$. (In fact it acts doubly transitively on each X_i.)

The subgroup fixing a point p_i of X_i is a complement to A in this product, and so is isomorphic to $\mathrm{SL}(2,2^n)$; it is transitive on the remaining points of X_i and has two orbits on X_j for all $j\neq i$, namely, the points incident and non-incident to p_i. If $p_j\in X_j$ is a point incident with p_i, then the stabiliser of p_i and p_j is a dihedral group of order $2(2^n-\varepsilon)$. Now all such dihedral groups in our group $A\cdot\mathrm{SL}(2,2^n)$ are conjugate (they are the normalisers of Sylow p-subgroups, where p is a prime divisor of $2^n-\varepsilon$); so this subgroup fixes one point p_l in each set X_l. Moreover, these points p_l are pairwise incident. For, if p_l and p_m were not incident, their stabiliser would be a dihedral group of order $2(2^n+\varepsilon)$; but this number does not divide $2(2^n-\varepsilon)$.

Now the set of all these points p_l is a full clique. It is the unique full clique containing p_i and p_j which is stabilised by a dihedral group of order $2(2^n-\varepsilon)$. So we have constructed a full clique cover.

Now the orbits of the group A on these full cliques form the required 1-factorisation, as we described earlier.

6 Further remarks

(1) The obvious outstanding problem is to determine the maximum value of r for a MYR with given v and k. I conjecture that the examples here are maximal in this sense. Noda [7] showed that, for SLSDs with the parameters of those used here, the maximum value of r is $v/2$ (this value being attained by the system derived from the Kerdock set).

(2) Preece and Vowden [11] remark that the 6×16 MYR is "fatally flawed statistically", since the fourth factor is confounded with the other three. Does this phenomenon hold more widely?

(3) Following Bailey's remarks in [1], Section 10, another problem is to decide whether any of these designs are optimal, or indeed whether the combinatorial properties specified here imply optimality, as they do when $r=2$ ([1],

Corollary 7.1.2).

The first two points are related. In the case of the 6×16 MYR, the parameter x is equal to 1. This means that, if $p_1 \in X_1$ and $p_2 \in X_2$ are adjacent in the multipartite graph, then there is a unique $p_3 \in X_3$ adjacent to both. Similarly there is a unique $p_4 \in X_4$ adjacent to both; and p_3 and p_4 must themselves be adjacent, or the construction would not work. (Indeed, there are two non-singular sets of four alternating bilinear forms on $\mathrm{GF}(2)^4$, up to translation and linear transformation; the set we construct is of one type, and all 4-subsets of the eight-element Kerdock set are of the other type. In the second type, the vertices p_3 and p_4 above fail to be adjacent, so no full cliques exist.)

Now the point p_1 lies in six full cliques; there are $6 \cdot 5 = 30$ full cliques sharing their second vertex with one of these, and the same number sharing each of the other vertices. Our above remarks show that there are no overlaps between these sets. Since $6 + 3 \cdot 30 = 96$, we see both that there cannot be another factor, and that the last factor is effectively determined by the others.

This argument does not apply for any other parameter set in this series.

Finally, we remark that if we take the MYRs with $\varepsilon = \pm 1$ and change the numbering of the 1-factors in one of them so that all the 1-factors are numbered from 1 to v, we have a resolvable full clique cover of the complete multipartite graph with r parts of size v. This is clearly equivalent to $r-1$ mutually orthogonal Latin squares of order v. In other words, if we take the representations of the two MYRs as Latin rectangles, and place one rectangle under the other, we obtain mutually orthogonal Latin squares. The case $v = 16$ is given in this form in [9].

7 Appendix: two bounds

The two non-singular sets mentioned above are both of maximum size in some sense. The first part of the following result is well known.

Theorem 2 *Let $\mathcal{B}$ be a non-degenerate set of alternating bilinear forms on a $2n$-dimensional vector space V over* $\mathrm{GF}(2)$.

(a) $|\mathcal{B}| \leq 2^{2n-1}$.
(b) If $\mathcal{B}$ is additively closed, then $|\mathcal{B}| \leq 2^n$.

PROOF. Choosing a basis $\{e_1, \ldots, e_{2n}\}$ for V, a bilinear form B is represented by a matrix $M(B) = (B(e_i, e_j))$. If B is alternating, the matrix is skew-symmetric with zero diagonal; if B is nondegenerate, the matrix is non-singular.

If $\mathcal{B}$ is a nondegenerate set, then all the matrices $M(B)$ for $B \in \mathcal{B}$ have distinct first rows, since the difference of any two of them is non-singular. There are only 2^{2n-1} possible first rows, since the first entry is necessarily zero. This proves (a).

Now suppose that $\mathcal{B}$ is additively closed, so that it too is a vector space over $\mathrm{GF}(2)$. Recall that the determinant of a skew-symmetric matrix is the square of a polynomial in the matrix entries called the *Pfaffian* (see [6], p. 373). Now the Pfaffian is a form of degree n on the vector space $\mathcal{B}$ which vanishes only at the origin. By the Chevalley–Warning theorem ([6], p. 140), we have $\dim B \leq n$, and so $|\mathcal{B}| \leq 2^n$.

Acknowledgements

I am grateful to R. A. Bailey and D. A. Preece for explanations, comments, and access to their reprint collections.

References

[1] R. A. Bailey, Resolved designs viewed as sets of partitions, in *Combinatorial Designs and their Applications* (ed. F. C. Holroyd, K. A. S. Quinn, C. Rowley and B. S. Webb), Chapman & Hall/CRC Press Research Notes in Mathematics **403**, CRC Press, Boca Raton, 1999, pp. 17–47.

[2] R. A. Bailey, Orthogonal partitions in designed experiments, *Designs, Codes and Cryptography* **8** (1996), 45–77.

[3] P. J. Cameron and J. J. Seidel, Quadratic forms over $\mathrm{GF}(2)$, *Proc. Kon. Nederl. Akad. Wetensch.* (A) **76** (1973), 1–8.

[4] R. A. Fisher, The mathematics of experimentation, *Nature* **142** (1938), 442–443, reprinted in *Collected Papers of R. A. Fisher* (ed. J. H. Bennett), vol. 4, University of Adelaide, Adelaide, 1974, pp. 155–158.

[5] A. M. Kerdock, A class of low-rate nonlinear binary codes, *Information and Control* **20** (1972), 182–187.

[6] S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965.

[7] R. Noda, On homogeneous systems of linked symmetric designs, *Math. Z.* **138** (1974), 15–20.

[8] D. A. Preece, Fifty years of Youden squares: a review, *Bull. Inst. Math. Appl.* **26** (1990), 65–75.

[9] D. A. Preece and P. J. Cameron, Some new fully-balanced Graeco-Latin Youden 'squares', *Utilitas Math.* **8** (1975), 193–204.

[10] D. A. Preece and N. C. K. Phillips, A new type of Freeman–Youden rectangle, *J. Combinatorial Mathematics and Combinatorial Computing* **25** (1997), 65–78.

[11] D. A. Preece and B. J. Vowden, Some series of cyclic balanced hyper-Graeco-Latin superimpositions of three Youden squares, *Discrete Math.* **197/198** (1999), 671–682.

[12] C. A. B. Smith and H. O. Hartley, The construction of Youden squares, *J. Royal Statist. Soc.* (B) **10** (1948), 262–263.

[13] W. J. Youden, Use of incomplete block replications in estimating tobacco-mosaic virus, *Contrib. Boyce Thompson Inst.* **9** (1937), 41–48.