Multi-letter Youden rectangles from quadratic forms

Peter J Cameron

School of Mathematical Sciences
Queen Mary, University of London
London E1 4NS, U.K.
p.j.cameron@qmw.ac.uk

BCC18, July 2001

In memory of J. J. Seidel

History

I am completing a story which began (for me) with the paper

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

(This paper, and in particular the object shown on the next slide, grew from a conversation on the bus, on the conference excursion at the British Combinatorial Conference in Aberystwyth, 1973.)

A design

AAA	BBB	CCC	DDD	EEE	FFF	GGG	HHH	III	JJJ	KKK	LLL	MMM	NNN	OOO	PPP
HGB	GHA	FED	EFC	DCF	CDE	BAH	ABG	POJ	OPI	NML	MNK	LKN	KLM	JIP	IJO
KJD	LIC	ILB	JKA	ONH	PMG	MPF	NOE	CBL	DAK	ADJ	BCI	GFP	HEO	EHN	FGM
MIE	NJF	OKG	PLH	IMA	JNB	KOC	LPD	EAM	FBN	GCO	HDP	AEI	BFJ	CGK	DHL
OFL	PEK	MHJ	NGI	KBP	LAO	IDN	JCM	GND	HMC	EPB	FOA	CJH	DIG	ALF	BKE
PCN	ODM	NAP	MBO	LGJ	KHI	JEL	IFK	HKF	GLE	FIH	EJG	DOB	CPA	BMD	ANC
BDC	ACD	DBA	CAB	FHG	EGH	HFE	GEF	JLK	IKL	LJI	KIJ	NPO	MOP	PNM	OMN
CKI	DLJ	AIK	BJL	GOM	HPN	EMO	FNP	KCA	LDB	IAC	JBD	OGE	PHF	MEG	NFH
DMP	CNO	BON	APM	HIL	GJK	FKJ	ELI	LEH	KFG	JGF	IHE	PAD	OBC	NCB	MDA
EBF	FAE	GDH	HCG	AFB	BEA	CHD	DGC	MJN	NIM	OLP	PKO	INJ	JMI	KPL	LOK
FLO	EKP	HJM	GIN	BPK	AOL	DNI	CMJ	NDG	MCH	PBE	OAF	JHC	IGD	LFA	KEB
GPJ	HOI	ENL	FMK	CLN	DKM	AJP	BIO	OHB	PGA	MFD	NEC	KDF	LCE	IBH	JAG
IEM	JFN	KGO	LHP	MAI	NBJ	OCK	PDL	AME	BNF	COG	DPH	EIA	FJB	GKC	HLD
JOH	IPG	LMF	KNE	NKD	MLC	PIB	OJA	BGP	AHO	DEN	CFM	FCL	EDK	HAJ	GBI
LNG	KMH	JPE	IOF	PJC	OID	NLA	MKD	DFO	CEP	BHM	AGN	HBK	GAL	FDI	ECJ
NHK	MGL	PFI	OEJ	JDO	ICP	LBM	KAN	FPC	EOD	HNA	GMB	BLG	AKH	DJE	CIF

What is it?

- Three MOLS.
- In the first six rows, each Latin rectangle is a symmetric $(16,6,2)$ BIBD; the blocks of one design meet the blocks of another in 1 or 3 points; and if we let a column of one rectangle be incident with a column of another if they share one letter, then again we get a symmetric $(16,6,2)$ BIBD. Moreover, these three BIBDs are "linked" in the same way.
- Similarly for the last ten rows.

Viewed otherwise

More symmetrically, we have:

(a) Four sets $S_1, \ldots, S_4$ each of size 16, with an incidence relation beteen each pair, so that (S_i, S_j) forms a $(16, 6, 2)$ BIBD, and the number of elements of S_k incident with s_i and s_j is one if s_i and s_j are incident, 3 otherwise (this is the *linking condition*);

(b) a collection of 96 sets each consisting of four pairwise incident points, (with each incident pair lying in exactly one such set), partitioned into 6 sets of size 16, so that each point occurs once in each part. These 4-sets are cliques in the incidence graph; so we have a *resolvable clique-cover*.

Or again . . .

From a statistician's point of view, the 96 cliques are the plots or experimental units. We have four partitions $\pi_1, \ldots, \pi_4$ of the set $\mathcal{P}$ of plots into 16 sets of 6, and one partition σ into 6 sets of 16, satisfying:

- π_i and σ are orthogonal for all i.
- π_i and π_j form a BIBD for all $i \neq j$.
- π_i, π_j, and π_k satisfy the "linking condition" for all distinct i, j, k.

The rectangle given before is obtained by taking σ as "rows" and π_1 as "columns"; the other three partitions give the three "letters" in the array.

So what's new?

Condition (a) defines a *system of linked square designs* or SLSD. Infinite families of examples were found in my first joint paper:

P. J. Cameron and J. J. Seidel, Quadratic forms over GF(2), *Proc. Kon. Nederl. Akad. Wetensch.* (A) **76** (1973), 1–8.

This paper gives two families, one linear, one non-linear (related to the Kerdock codes).

It has taken me more than 25 years to realise that, for the linear (but not for the non-linear) examples, condition (b) also holds. Thus we obtain an infinite family of objects generalising the one given earlier.

To prove this, one just has to use some easy facts about the automorphism group of the SLSDs.

Details

The BIBDs have parameters $(2^{2m}, 2^{2m-1} \pm 2^{m-1}, 2^{2m-2} \pm 2^{m-1})$ for any $m \geq 2$. The number of sets in the SLSD is 2^m.

To construct them, we identify $\mathrm{GF}(2^m)^2$ with $\mathrm{GF}(2)^{2m}$ by restricting scalars. We take S_λ to be the set of quadratic forms which polarise to the bilinear form $\mathrm{Trace}(\lambda b)$ for all $\lambda \in \mathrm{GF}(2^m)$, where $b((x_1,y_1),(x_2,y_2)) = \det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$. Then for $\lambda \neq \mu$, if $Q_\lambda \in S_\lambda$ and $Q_\mu \in S_\mu$, then $Q_\lambda - Q_\mu$ is non-degenerate; we declare Q_λ and Q_μ incident if $Q_\lambda - Q_\mu$ has type ε, where $\varepsilon = \pm 1$.

The group $2^{2m} : \mathrm{SL}(2, 2^m)$ acts on the configuration. The stabiliser of an incident pair is a dihedral group fixing one element of each set S_λ; using the group, we see that these elements are mutually incident, so they form a clique. Thus we have our clique-cover. Now we partition them into orbits of the translation group to get the resolution.