stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE
(DEPARTMENT OF PURE MATHEMATICS)

ZW 77/79 AUGUSTUS

A.E. BROUWER

A SERIES OF SEPARABLE DESIGNS WITH APPLICATION TO PAIRWISE ORTHOGONAL LATIN SQUARES

Preprint

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O).

1980 Mathematics Subject Classification: 05B05, 05B10, 05B15

A series of separable designs with application to pairwise orthogonal Latin squares *)

by

A.E. Brouwer

ABSTRACT

We observe that a partition of PG($2,q^2$) into Baer subplanes gives rise to certain separable pairwise balanced block designs (with $\lambda = 1$) which in turn can be used to get more mutually orthogonal Latin squares of certain orders than previously known. As a side result we find an embedding of STS(19) in PG(2,11), thus refuting a conjecture of M. Limbos.

KEY WORDS & PHRASES: *mutually orthogonal Latin squares, Baer subplane, difference set.*

---

*) This report will be submitted for publication elsewhere.

It is well known that $PG(2,q^2)$ can be partitioned into Baer subplanes $PG(2,q)$ (see e.g. ROOM & KIRKPATRICK [6]; for more general results see HIRSCHFELD [3]). Let P be the pointset of $PG(2,q^2)$, and let $P = \sum_{i=1}^{q^2-q+1} P_i$ be such a partition. Let $X = \sum_{i=1}^{t} P_i$.

Each line of $PG(2,q^2)$ intersects X in either t or $t+q$ points (for: for each line ℓ there is a unique i such that ℓ intersects P_i in $q+1$ points and P_j with $j \neq i$ in one point), so that we have a pairwise balanced design with $\nu = t(q^2+q+1)$ points, blocksizes t and $t+q$ and $\lambda = 1$. Moreover, this design is separable in the sense of BOSE, SHRIKHANDE & PARKER [1]: the equiblock component consisting of the blocks of size $t+q$ is symmetric: there are exactly $\nu = t(q^2+q+1)$ such blocks, while the equiblock component consisting of the blocks of size t is resolvable into $q^2-q+1-t$ parallel classes, each parallel class consisting of the lines intersecting P_i $(i=t+1,\dots,q^2-q+1)$ in $q+1$ points. Thus we proved:

<u>THEOREM</u>. *Let q be the power of a prime, and $0 < t < q^2-q+1$. Then there exists a pairwise balanced design $B[\{t,q+t\}, 1; t(q^2+q+1)]$ such that it is the union of a symmetric 1-$(\nu,q+t,1)$ design and a resolvable 1-$(\nu,t,1)$ design.*

As a corollary to (a slight improvement of) theorem 4 in BOSE, SHRIKHANDE & PARKER [1] we find the following lower bound for $N(n)$, the maximum number of mutually orthogonal Latin squares of order n.

<u>COROLLARY</u>. *Let q be a prime power, $0 \le t \le q^2-q+1$, $n = t(q^2+q+1)+x$. Let $d_0 = N(x)$, $d_1 = N(t)$, $d_2 = N(t+1)$, $d_3 = N(t+q)$, $d_4 = N(t+q+1)$ (where $N(0) = N(1) = +\infty$).*
Let

$$\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4 \in \{0,1\},$$

and

$$\begin{aligned}
\varepsilon_1 &= 0 \quad \textit{iff} \quad x = q^2-q-t,\\
\varepsilon_2 &= 0 \quad \textit{iff} \quad x = 1,\\
\varepsilon_3 &= 0 \quad \textit{iff} \quad x = q^2,\\
\varepsilon_4 &= 0 \quad \textit{iff} \quad x = t+q+1.
\end{aligned}$$

Then

(i) *if* $x = 0$ *then* $N(n) \geq \min(d_1, d_3)$,

(ii) *if* $x = t+q$ *then* $N(n) \geq \min(d_1-\varepsilon_3, d_3, d_4-1)$,

(iii) *if* $x = q^2-q+1-t$ *then* $N(n) \geq \min(d_0, d_2-\varepsilon_2, d_3-1)$,

(iv) *if* $x = q^2+1$ *then* $N(n) \geq \min(d_0, d_2-\varepsilon_4, d_4-1)$,

(v) *if* $0 < x < q^2-q+1-t$ *then* $N(n) \geq \min(d_0, d_1-\varepsilon_1, d_2-\varepsilon_2, d_3-1)$,

(vi) *if* $t+q < x < q^2+1$ *then* $N(n) \geq \min(d_0, d_1-\varepsilon_3, d_2-\varepsilon_4, d_4-1)$.

A few examples where this method produces better results than previously known:

n	q	t	x	N(n)≥	old lower bound
189	4	9	0	8	7
253	4	12	1	12	10
357	5	11	16	9	7
912+x	7	16	0,1,9,23,27	15,14,8,14,15	12,10,7,7,7
1425	7	25	0	24	15
1509	9	16	53	14	7
1710	8	23	31	21	8
2395	7	42	1	42	15
2862	9	31	41	29	7

This last example is interesting because 2862 has been for a long time the largest n for which $N(n) \geq 7$ was unknown (see BROUWER [2], STINSON [7]). A recent theorem of Wojtas showed $N(2862) \geq 7$, but here we find $N(2862) \geq 29$! [I can prove now $N(n) \geq 7$ for $n > 780$.] Especially for somewhat larger n this method is successful; for instance with $q = 9$ and $t = 31$ we find thirteen improvements in the range $2862 \leq n \leq 2902$.

Using Singer difference sets we find a few other subsets X of a projective plane such that the cardinality of the intersection of X with a line takes only a few values. Let $\nu = q^2+q+1$, q a prime power and D a difference set (mod ν) for PG(2,q). Let u be a proper divisor of ν. If PG(2,q) has points $0,1,\ldots,\nu-1$ then let X have points $0,m,2m,\ldots,\nu-m$, where $\nu = mu$, so that $|X| = u$. Clearly X together with the intersections $\ell \cap X$ of the lines with X gives us a pairwise balanced design with u points and ν blocks (possibly of size 0 or 1); for each i, $0 \le i < m$ we find u blocks of size $k_i = |X \cap (D-i)|$, so that no more than m distinct block sizes occur.

As an example let us take $q = 11$, $\nu = 133$, $u = 19$, $m = 7$. A difference set is

$$D = \{0,1,3,12,20,34,38,81,88,94,104,109\}.$$

Looking at D (mod 7) we find $k_0 = k_1 = k_5 = 1$, $k_2 = 0$, $k_3 = k_4 = k_6 = 3$, so that we get a Steiner triple system STS(19) on X.
(This result may be of independent interest; no STS(13) is embeddable in a projective plane (KELLY & NWAMKPA [4]), and of the 80 different STS(15) only one (namely PG(3,2)) is embeddable (MONIQUE LIMBOS [5]). In fact Limbos went so far as to conjecture that STS(ν) is never embeddable in a projective plane unless it is a projective space PG(d,2) or an affine space AG(d,3). This system provides a counterexample.)

Since for my application I want all k_i to be (relatively large) prime powers it seems that my chances are best when $m = 3$, $u = \frac{1}{3}\nu$. (Now $q \equiv 1 \pmod 3$.)

PROPOSITION. *Let* $q \equiv 1 \pmod 3$ *be a prime power. Let* $u = \frac{1}{3}(q^2+q+1)$. *Then there exists a separable pairwise balanced design* $B[\{k_0,k_1,k_2\},1;\ u]$, *embeddable in* PG(2,q), *and such that it is the union of three symmetric* $1-(u,k_i,1)$ *designs* $(i = 0,1,2)$.
k_0, k_1 *and* k_2 *are the (unique) solution of*

$$k_0 + k_1 + k_2 = q+1$$
$$k_0^2 + k_1^2 + k_2^2 = q+u.$$

When q *is a square we have*

$$k_0 = \frac{1}{3}(q+1\mp 2\sqrt{q}),$$
$$k_1 = k_2 = \frac{1}{3}(q+1\pm\sqrt{q})$$

where the sign is determined by the requirement $k_i \in \mathbb{N}$.

PROOF. Let $\theta(x) = \sum_{d\in D} x^d$ be the Hall-polynomial of D. The fact that D is a difference set is expressed by $\theta(x) \cdot \theta(x^{-1}) \equiv q + (1+x+\ldots+x^{\nu-1}) \pmod{x^\nu-1}$. Reducing mod x^3-1 we find $\theta(x).\theta(x^{-1}) \equiv q + u(1+x+x^2) \pmod{x^3-1}$. Writing $\theta(x) \equiv k_0 + k_1x + k_2x^2 \pmod{x^3-1}$ yields the equations for k_i. (A solution is found by factoring $q = \theta(\zeta).\theta(\bar{\zeta})$ in $\mathbb{Q}(\zeta)$, where ζ is a primitive cube root of unity.) □

Interesting designs found in this way are for instance

B[{3,4},1;19]	($q = 7$, $k_0,k_1,k_2 = 1,3,4$),
B[{3,5},1;79]	($q = 23$, $m = 7$, intersections 0,3,5),
B[{5,6},1;151]	($q = 32$, $m = 7$, intersections 0,5,6),
B[{4,7,9},1;127]	($q = 19$),
B[{9,13,16},1;469]	($q = 37$).

From the existence of this last design it follows that $N(469) \geq 8$.

Note that when q is a square the set X is a union of Baer subplanes iff $\frac{1}{3}(q-\sqrt{q}+1)$ is an integer. So for $q = 16$ we find $|X| = 91$, $k_0 = 3$, $k_1 = k_2 = 7$, not the union of PG(2,4)'s, but in PG(2,25) we have $|X| = 217$, $k_0 = 12$, $k_1 = k_2 = 7$, the union of seven PG(2,5)'s.

REFERENCES

[1] BOSE, R.C., S.S. SHRIKHANDE & 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] BROUWER, A.E., *The number of mutually orthogonal Latin squares - a table up to order* 10000, Report ZW 123, June 1979, Math. Centrum, Amsterdam.

[3] HIRSCHFELD, J.W.P., *Cyclic projectivities in* PG(n,q), *in* Teorie Combinatorie, Atti dei convegni Lincei 17, Roma 1976, pp.201-211.

[4] KELLY, L.M. & S. NWANKPA, *Affine embeddings of Sylvester-Gallai designs,* J. Combinatorial Theory A 14 (1973) 422-438.

[5] LIMBOS, M., *Projective embeddings of Steiner triple systems,* Lecture in Han-sur-Lesse, June 1979.

[6] ROOM, T.G. & P.B. KIRKPATRICK, *Miniquaternion geometry,* Cambridge, 1971.

[7] STINSON, D.R., *A note on the existence of 7 and 8 mutually orthogonal Latin squares,* Ars Combinatoria 6 (1978) 113-115.

Egeldonk, 790805