Latin-Square Geometry: Orthogonal Latin Squares as Skew Lines

# Latin–Square Geometry:

**Orthogonal Latin Squares as Skew Lines** 

## by Steven H. Cullinane

"While the reader may draw many a moral from our tale, I hope that the story is of interest for its own sake.
Moreover, I hope that it may inspire others, participants or observers, to preserve the true and complete record of our mathematical times."
-- From Error-Correcting Codes Through Sphere Packings To Simple Groups, by Thomas M. Thompson, Mathematical Association of America, 1983

"Packing finite projective spaces with disjoint subspaces has for many years been a topic of considerable interest in Galois Geometry. In particular, one studies *partial spreads* in a space PG(3,q), that is, collections of pairwise disjoint lines in PG(3,q): see Hirschfeld [8] for background. A set of *r* mutually skew lines for which any other line meets at least one line of the set will be referred to as a *maximal* partial spread (MPS) of size *r*.

An interesting combinatorial problem (which seems at first sight not at all related to **partial spreads**) is the determination of the pairs (s,t) for which a maximal set of t mutually orthogonal Latin squares of order s exist...."

<u>Some new maximal sets of mutually orthogonal Latin squares</u>, by P. Govaerts, D. Jungnickel, L. Storme, and J. A. Thas, *Designs, Codes, and Cryptography* 29 (1–3), May–June–July 2003, pp. 141–147

Keywords: latin squares, MAXMOLS, partial spread, projective space, polar space

## Mathematics Subject Classification: 05B15, 05B25, 05B40

These authors said, in early 2003, that spreads and orthogonal Latin squares seem "at first sight" unrelated. They of course did not mention my note (shown below) that pointed out such a relationship in December 1978. The earliest sources they cited for such a relationship are Jungnickel in 1984 and 1993.

Here are the details of my 1978 note.

We present two results -- one old, one new -- on the geometry of Latin squares.

## Result A (old):

There exist n-1 mutually orthogonal nxn Latin squares if and only if there exists a finite projective plane with  $n^2 + n + 1$  lines (or, equivalently, an affine plane with  $n^2 + n$  lines).

Result A is well known. See, for instance, chapter 8 of *Discrete Mathematics Using Latin Squares*, C. F. Laywine and G. L. Mullen, Wiley Interscience, 1998, or <u>Bose's [1938] Theorem</u> (pdf).

## Result B (new):

The six 4x4 Latin squares that have orthogonal Latin mates can be embedded in a set of thirty–five 4x4 arrays so that orthogonality in the set of arrays corresponds to skewness in the set of 35 lines of the finite projective space PG(3,2).

Result B is apparently new, and should not be confused with result A. The closest thing to the diagrams of result B in the refereed literature seems to be the use of diagrams on page 774 of *Design Theory, Volume 2*, by T. Beth, D. Jungnickel, and H. Lenz, Cambridge U. Press, 1999, in proving Tarry's theorem on the nonexistence of two mutually orthogonal 6x6 Latin squares.

The research note below shows how result B works. Note particularly that the 35–line projective *space* of result B differs from the 21–line projective *plane* of result A.

Result B is, of course, highly special, being limited to 4x4 squares. This limitation should not prevent its use as an example in popular introductions to discrete mathematics. Indeed, the 4x4 case figured prominently (and exclusively) on the cover and in <u>a two-page article</u> in the August/September 2001 issue of the Mathematical Association of America's "Focus" newsletter.

Naturally, a more general result than B is desirable; hence the problem stated in the 1978 research note below.

## Steven H. Cullinane Orthogonality of Latin squares viewed as skewness of lines. Dec. 1978.

Shown below is a way to embed the six order–4 Latin squares that have orthogonal Latin mates in a set of 35 arrays so that orthogonality in the set of arrays corresponds to skewness in the set of 35 lines of PG(3,2). Each array yields a 3–set of diagrams that show the lines separating complementary 2–subsets of  $\{0,1,2,3\}$ ; each diagram is the symmetric difference of the other two. The 3–sets of diagrams correspond to the lines of PG(3,2). Two arrays are orthogonal iff their 3–sets of diagrams are disjoint, i.e. iff the corresponding lines of PG(3,2) are skew.

This is a new way of viewing orthogonality of Latin squares, quite different from their relationship to projective planes.

PROBLEM: To what extent can this result be generalized?

0 1 2 3	1 0 3 2	2 3 0 1	3 2 1 0	0 2 3 1	1 3 2 0	2 0 1 3	3 1 0 2	0 3 1 2	1 2 0 3	2 1 3 0	3 0 2 1	0 2 1 3	1 3 0 2	2 0 3 1	3 1 2 0	0 1 3 2	1 0 2 3	2 3 1 0	3 2 0 1	0 3 2 1	1 2 3 0	2 1 0 3	3 0 1 2	
0 2 2 0	1 3 3 1	1 3 3 1	0 2 2 0	0 2 3 1	0 2 3 1	1 3 2 0	1 3 2 0	0 0 3 3	1 1 2 2	2 2 1 1	3 3 0 0	0 2 3 1	1 3 2 0	0 2 3 1	1 3 2 0	0 3 0 3	1 2 1 2	2 1 2 1	3 0 3 0	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3	
0 0 0 0	1 1 1 1	2 2 2 2	3 3 3 3	0 1 2 3	1 0 3 2	1 0 3 2	0 1 2 3	0 1 1 0	1 0 0 1	2 3 3 2	3 2 2 3	0 2 3 1	1 3 2 0	1 3 2 0	0 2 3 1	0 3 3 0	1 2 2 1	2 1 1 2	3 0 0 3	0 2 1 3	1 3 0 2	1 3 0 2	0 2 1 3	
0 2 2 0	1 3 3 1	2 0 0 2	3 1 1 3	0 0 2 2	1 1 3 3	1 1 3 3	0 0 2 2	0 2 2 0	0 2 2 0	1 3 3 1	1 3 3 1	0 2 2 0	1 3 3 1	0 2 2 0	1 3 3 1	0 2 0 2	1 3 1 3	1 3 1 3	0 2 0 2	0 0 2 2	0 0 2 2	1 1 3 3	1 1 3 3	
0 2 0 2	1 3 1 3	0 2 0 2	1 3 1 3	0 1 2 3	0 1 2 3	1 0 3 2	1 0 3 2	0 0 1 1	1 1 0 0	2 2 3 3	3 3 2 2	0 1 2 3	1 0 3 2	0 1 2 3	1 0 3 2	0 1 0 1	1 0 1 0	2 3 2 3	3 2 3 2	0 2 1 3	0 2 1 3	1 3 0 2	1 3 0 2	
0 0 2 2	1 1 3 3	2 2 0 0	3 3 1 1	0 2 1 3	1 3 0 2	0 2 1 3	1 3 0 2	0 2 0 2	1 3 1 3	2 0 2 0	3 1 3 1	0 2 0 2	0 2 0 2	1 3 1 3	1 3 1 3	0 0 2 2	1 1 3 3	0 0 2 2	1 1 3 3					

View original 1978 note.

#### For related material, see the websites Geometry of the 4x4 Square and Diamond Theory.

The apparent conflict between the 2003 paper by Jungnickel *et al.* and my 1978 note can be resolved as follows:

"The [1954–1964] André/Bruck–Bose construction yields a one–to–one correspondence between spreads of projective space and translation planes (special affine planes). If one feeds a partial spread into this construction, a net results. A net is a point–line geometry which is a natural weakening of an affine plane."

## --- John Bamberg, Symplectic spreads

And it has long been known that affine planes are, as noted above, closely related to orthogonal Latin squares.

In other words, the 1954–1964 André/Bruck–Bose construction is the missing (missing, that is, according to Jungnickel, Thas, *et al.*) link between Latin–square orthogonality and projective–space skewness. Such an orthogonality–skewness link is shown rather more directly and clearly in my 1978 note.

(For details of the André/Bruck-Bose construction, see

Johannes André, Über nicht–Dessarguessche Ebenen mit transitiver Translationsgruppe, *Math Z.* 60, pp. 156–186, 1954, and

R. H. Bruck and R. C. Bose, The construction of translation planes from projective spaces, *J. Algebra* 1, pp. 85–102, 1964.

## The following may also be helpful:

A t-spread of a projective space is a collection of t-dimensional subspaces such that every point is contained in exactly one subspace. So a spread provides a partition of the points of the projective space. A partial t-spread is a collection of pairwise disjoint t-dimensional subspaces. Given a spread S, there is an associated translation plane  $\pi(S)$  derived from the Andre/Bruck-Bose construction (see [6] and [2]). We call a collection C of  $(t + 1) \times (t + 1)$  matrices over GF(q) a t-spread set if it satisfies the following conditions: (1)  $|C| = q^{t+1}$ ; (2) C contains the zero matrix; (3) if A and B are distinct matrices in C, then A - B is invertible. Every t-spread of PG(2t + 1, q) can be represented by a t-spread set (see [6]), as  $S(C) = \{\{(X, XA) \in GF(q^{t+1}) \oplus GF(q^{t+1}) | X \in GF(q^{t+1})\} : A \in C\} \cup Y$  (where  $Y = \{(0, y) : y \in GF(q^{t+1})\}$ ) is a spread if and only if C is a spread set.

Let  $\mathcal{C}$  be a spread set and let  $\pi = \pi(\mathcal{S}(\mathcal{C}))$ . Then  $\pi$  is a dual translation plane with shears point Y, if and only if  $\mathcal{C}$  is closed under addition. In the finite case, the following are equivalent (see [7, Section 3.1]): (1)  $\pi$  has at least two translation lines; (2) every line of  $\pi$  is a translation line; (3)  $\pi$  is Desarguesian; (4)  $\pi$  is isomorphic to  $PG(2, q^{t+1})$  for some q; (5)  $\mathcal{C}$  is closed under addition and multiplication.

-- From <u>Flocks, ovals, and generalized quadrangles</u> (ps), (Four lectures in Napoli, June 2000), by Maska Law and Tim Penttila)

For further background, here is material on finite geometry from the paper <u>Symplectic spreads</u> (pdf), 15 Sept. 2003, by <u>Simeon Ball</u>, John Bamberg, <u>Michel Lavrauw</u>, and <u>Tim Penttila</u>:

## From <u>Symplectic spreads</u> (pdf):

"First we give an overview of some definitions and theory of finite geometry, together with some results of the past which provide the context and background for our construction.

A projective plane is an incidence structure of points and lines such that:

(PP1) for every pair of distinct points there is a unique line which is incident with both of them;

(PP2) every pair of distinct lines meet in a unique point;

(PP3) there exist four distinct points with no three collinear (no three are incident with a common line).

An affine plane is an incidence structure of points and lines such that:

(AP1) for every pair of distinct points there is a unique line which is incident with both of them;

(AP2) for any non–incident point–line pair p, L, there exists a unique line through p which has no point in common with L;

(AP3) there exist three non-collinear points.

## From <u>Symplectic spreads</u> (pdf):

In a projective or affine plane, a point P is a *centre* for a collineation *phi* if *phi* fixes every line incident with P.

A line *l* is an *axis* of *phi* if *phi* fixes every point on *l*. It is standard knowledge that every non-identity collineation has at most one axis and at most one centre, and it has an axis if and only if it has a centre (see [7, Section 3.1.4]). A collineation which has a centre and axis which are incident with one another, is called an *elation*. A group of collineations *H* is called (P, l)-*transitive* if the subgroup of *H* consisting of those elements which have centre *P* and axis *l*, acts transitively on the non-fixed points of any line through P which is not equal to *l*. For two lines *m* and *l*, we say that *H* is (m, l)-*transitive* if *H* is (P, l)-transitive for all *P* on *m*. Dually, if *P* and *Q* are points, then we say that *H* is (P, Q)-*transitive* if *H* is (P, l)-transitive for every line *l* incident with *Q*. Let *Gamma* be a projective plane and suppose that *Delta* is an affine plane obtained by removing the line  $l_{infinity}$  from *Gamma*. Then *Delta* is a *translation plane* if there exists a  $(l_{infinity}, l_{infinity})$ -transitive group of elations of *Delta*. We call  $l_{infinity}$  the *translation line* of *Delta*. The dual of a translation plane is a *shears plane*, the corresponding point being a *shears point*.

Given a spread S of PG(3,q), the André/Bruck-Bose construction produces a translation plane  $\pi(S)$  of order  $q^2$  as follows: Embed PG(3,q) as a hyperplane of PG(4,q). Define an incidence structure  $\mathcal{A}(S)$  with **points** the points of PG(4,q) not on PG(3,q) and **lines** the planes of PG(4,q) meeting PG(3,q) in a line of S. Then  $\mathcal{A}(S)$  is a translation affine plane of order  $q^2$ . Let  $\pi(S)$  be the projective completion of  $\mathcal{A}(S)$ .

R. H. Bruck in 1951 [4] introduced finite nets. A *net* is a system of points and lines satisfying: (AP2) as before;

(N1) every two points lie on at most one line;

(N2) every point lies on at least two distinct lines.

Note that the definition of a net is the natural weakening of the axioms of an affine plane. Parallelism is an equivalence relation, and in the finite case, the number of parallel classes k is called the *degree* of the net, and the common number n of points on each line is called the *order* of the net. A net is thus equivalent to k - 2 mutually orthogonal  $n \times n$  Latin squares, as shown by Bruck in 1951. See also Bruck's 1963 paper [5] for more on nets. There is an analogue here with the André/Bruck–Bose construction — given a partial spread S, one can construct a net nu(S), but this time the converse fails."

.....

### References for <u>Symplectic spreads</u> (pdf):

[1] A. A. Albert. On the collineation groups associated with twisted fields. In *Calcutta Math. Soc. Golden Jubilee Commemoration Vol. (1958/59), Part II*, pages 485–497. Calcutta Math. Soc., Calcutta, 1958/1959.

[2] Johannes André. Über nicht–Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.*, 60: 156–186, 1954.

[3] L. Bader, W. M. Kantor, and G. Lunardon. Symplectic spreads from twisted fields. *Boll. Un. Mat. Ital. A*(7), 8(3): 383–389, 1994.

[4] R. H. Bruck. Finite nets. I. Numerical invariants. Canadian J. Math., 3: 94–107, 1951.

[5] R. H. Bruck. Finite nets. II. Uniqueness and imbedding. Pacific J. Math., 13: 421–457, 1963.

[6] R. H. Bruck and R. C. Bose. The construction of translation planes from projective spaces. *J. Algebra*, 1: 85–102, 1964.

[7] P. Dembowski. *Finite geometries*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Springer–Verlag, Berlin, 1968.

[8] U. Dempwolff. Translation planes of order 27. Des. Codes Cryptogr., 4(2): 105–121, 1994.

[9] Christoph Hering. Eine nicht-desarguessche zweifach transitive affine Ebene der Ordnung 27. *Abh. Math. Sem. Univ. Hamburg*, 34: 203–208, 1969/ 1970.

[10] William M. Kantor. Commutative semifields and symplectic spreads. To appear in J. Algebra.

[11] William M. Kantor. Strongly regular graphs defined by spreads. Israel J. Math., 41(4): 298–312, 1982.

[12] T. G. Ostrom. Replaceable nets, net collineations, and net extensions. *Canad. J. Math.*, 18: 666–672, 1966.

[13] Chihiro Suetake. A new class of translation planes of order  $q^3$ . Osaka J. Math., 22(4): 773–786, 1985.

[14] Fam Khyu T'ep. Irreducible J-decompositions of the Lie algebras  $A_p^{n-1}$ . *Mat. Zametki*, 49(5): 128–134, 159, 1991.

[15] J. A. Thas. Ovoids and spreads of finite classical polar spaces. *Geom. Dedicata*, 10(1–4): 135–143, 1981.

[16] J. A. Thas. Old and new results on spreads and ovoids of finite classical polar spaces. In *Combinatorics* '90 (*Gaeta, 1990*), volume 52 of *Ann. Discrete Math.*, pages 529–544. North–Holland, Amsterdam, 1992.

[17] J. A. Thas. Ovoids, spreads and m-systems of finite classical polar spaces. In *Surveys in combinatorics*, 2001 (Sussex), volume 288 of *London Math. Soc. Lecture Note Ser.*, pages 241–267. Cambridge Univ. Press, Cambridge, 2001.

See also further details from the paper cited in the epigraph--

### From <u>Some new maximal sets of</u> <u>mutually orthogonal Latin squares</u>:

"Let us briefly sketch the connection between partial spreads in PG(3,q) and sets of mutually orthogonal Latin squares of order  $q^2$ . Any *r* mutually skew lines in PG(3,q) may be viewed as a collection of *r pairwise disjoint* subgroups of order  $q^2$  in the additive group of the vector space V = V(4,q) (meaning, of course, that any two of these subgroups intersect trivially). This is a particular example of a so-called *partial congruence partition* (PCP) and therefore leads to a (translation) net of order  $s = q^2$  and degree *r* by taking the vectors in *V* as points and all the translates of the specified *r* subgroups as lines, cf. [9] or [2]. If the given partial spread is actually maximal, one may hope that the associated net is likewise maximal, resulting in t = r - 2 MAXMOLS(*s*),  $s = q^2$ . This approach has been used successfully by Jungnickel [10, 11]. However, in general, the associated net may well be extendable; it is easily seen that this happens if and only if the net admits a *transversal*, i.e., a set of *s* points meeting every line of the net in a unique point.

In the present note, we will use maximal partial spreads of size r in  $PG(3,4)\setminus PG(3,2)$  to construct transversal–free translation nets of degree r + 3; this approach will give our new examples of MAXMOLS(16)."

#### References for <u>Some new maximal sets of</u> <u>mutually orthogonal Latin squares</u>:

1. D. Bedford and R. M. Whitaker, New and old values for maximal MOLS (*n*), *Ars Comb.*, Vol. 54 (2000), pp. 255–258.

2. T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, 2nd ed. Cambridge University Press (1999).

3. C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton (1996).

4. E. Cornelis and H. Vernaeve, Spreads in  $PG(3,4)\setminus PG(3,2)$ . Project for the computer algebra course, *Computational Group Theory*, Ghent University (2000).

5. D. A. Drake, G. H. J. van Rees and W. D. Wallis, Maximal sets of mutually orthogonal Latin squares, *Discr. Math.*, Vol. 194 (1999), pp. 87–94.

6. R. H. Dye, Partitions and their stabilizers for line complexes and quadrics, *Ann. Mat. Pura Appl.*, Vol. 114, No. 4 (1977), pp. 173–194.

7. The GAP Group, *GAP -- Groups, Algorithms, and Programming, Version 4.1* http://www-gap.dcs.st-and.ac.uk/~gap (1998).

8. J. W. P. Hirschfeld, Finite Projective Spaces of Three Dimensions, Oxford University Press (1985).

9. D. Jungnickel, Existence results for translation nets, in (P. J. Cameron, J. W. P. Hirschfeld and D. R. Hughes, eds.) *Finite Geometries and Designs*, Cambridge University Press (1981), pp. 172–196.

10. D. Jungnickel, Maximal partial spreads and translation nets of small deficiency, *J. Algebra*, Vol. 90 (1984), pp. 119–132.

11. D. Jungnickel, Maximal partial spreads and transversal-free translation nets, *J. Combin. Theory Ser. A*, Vol. 62 (1993), pp. 66–92.

12. D. Jungnickel, Maximal sets of mutually orthogonal Latin squares, in (S. Cohen and H. Niederreiter, eds.) *Finite Fields and Applications*, Cambridge University Press (1996), pp. 129–153.

13. D. Jungnickel and L. Storme, Maximal partial spreads in PG(3,4) and maximal sets of mutually orthogonal Latin squares of order 16, *Discr. Math.*, Vol. 26 (2003), pp. 361–372.

14. W. M. Kantor, Ovoids and translation planes, Canad. J. Math., Vol. 34 (1982), pp. 1195–1207.

15. K. Mellinger, A note on line-Baer subspace partitions of PG(3,4). J. Geom., Vol. 72 (2001), pp. 128–131.

16. T. Penttila, Personal communication, December 14 (2001).

17. E. E. Shult, Nonexistence of ovoids in Omega<sup>+</sup>(10, 3), *J. Combin. Theory Ser. A*, Vol. 51 (1989), pp. 250–257.

18. J. A. Thas, Polar spaces, generalized hexagons and perfect codes, *J. Combin. Theory Ser. A*, Vol. 29 (1980), pp. 87–93.

19. J. A. Thas, Ovoids and spreads of finite classical polar spaces, *Geom. Dedicata*, Vol. 10 (1981), pp. 135–144.

20. J. A. Thas, Ovoids, spreads and *m*-systems of finite classical polar spaces, in (J. W. P. Hirschfeld, ed.), *Surveys in combinatorics*, 2001, Cambridge University Press (2001), pp. 241–267

# Further sources of material on latin–square orthogonality and projective skewness

## **Godsil on Spreads**

For the use of the term "partial spreads" to mean sets of affine parallel classes (as interpreted within graph theory), see

<u>Partial spreads</u> (ps), a note by Chris Godsil:

"Let Z be a complete graph on  $n^2$  vertices. A *parallel class* in Z is a spanning subgraph isomorphic to  $nK_n$ . We say two parallel classes  $S_1$  and  $S_2$  are *orthogonal* if they have no edges in common.... A *partial spread* is a set of pairwise orthogonal parallel classes."

This informal note has no references. The way the note uses the terms "partial spread" and "orthogonal" is directly related to my 1978 note. Historians of mathematics can determine whether Godsil is the first to use these terms with these meanings.

Background for Godsil's note:

<u>Strongly Regular Graphs</u> (ps), by Peter J. Cameron (draft of a survey article), and two references cited by Cameron:

- C. D. Godsil, Algebraic Combinatorics, Chapman & Hall/CRC Press, 1993, and
- R. C. Bose, Strongly regular graphs, partial geometries, and partially balanced designs, *Pacific J. Math.* 13 (1963), 389–419.

# **Mellinger on Spreads**

Various <u>publications of Keith E. Mellinger</u> (2001–2004) detail the close relationship between finite translation planes and spreads.

# **Book on Translation Planes and Spreads**

See <u>Foundations of Translation Planes</u> (2001), by M. Biliotti, V. Jha, and N. L. Johnson, for an extensive treatment of how spreads and translation planes are related.

Page last maintained Feb. 6, 2005; created Nov. 1, 2001.