Designs, Codes and Cryptography, 29, 141–147, 2003

Some New Maximal Sets of Mutually Orthogonal Latin Squares

P. GOVAERTS pg@cage.rug.ac.be; http://cage.rug.ac.be/∼pg
Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281, B-9000 Gent, Belgium

D. JUNGNICKEL jungnickel@math.uni-augsburg.de; http://www.math.uni-augsburg.de/opt/
Lehrstuhl für Diskrete Mathematik, Optimierung und Operations Research, Universität Augsburg, D-86135 Augsburg, Germany

L. STORME ls@cage.rug.ac.be; http://cage.rug.ac.be/∼ls
Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281, B-9000 Gent, Belgium

J. A. THAS jat@cage.rug.ac.be; http://cage.rug.ac.be/∼jat
Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281, B-9000 Gent, Belgium

Communicated by: A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel, J. A. Thas

Abstract. Two ways of constructing maximal sets of mutually orthogonal Latin squares are presented.

The first construction uses maximal partial spreads in $PG(3, 4) \setminus PG(3, 2)$ with r lines, where $r \in \{6, 7\}$, to construct transversal-free translation nets of order 16 and degree $r + 3$ and hence maximal sets of $r + 1$ mutually orthogonal Latin squares of order 16. Thus sets of t MAXMOLS(16) are obtained for two previously open cases, namely for $t = 7$ and $t = 8$.

The second one uses the (non)existence of spreads and ovoids of hyperbolic quadrics $Q^+(2m + 1, q)$, and yields infinite classes of $q^{2n-1} - 1$ MAXMOLS(q^{2n}), for $n \geq 2$ and q a power of two, and for $n = 2$ and q a power of three.

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

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

1. Introduction

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; we shall refer to such a set as t MAXMOLS(s). This problem is, for instance, discussed in [2, Chapter X] and in [3, Section IV.27]; see also [12] for a survey. We will be interested in the case $s = 16$. According to the tables in [3] and some subsequent results of Drake et al. [5] and Bedford and Whitaker [1], MAXMOLS(16) are known for $t \in \{1, 2, 3, 4, 11, 15\}$; by Bruck's completion theorem, they cannot exist for $t = 13$ and $t = 14$, cf. [2, Section X.7]. Using MPS's in $PG(3, 4)$, two of the present authors [13] were recently able to construct sets of t MAXMOLS(16) for two previously undecided cases, namely for $t = 9$ and $t = 10$. We shall use a similar approach already suggested in [13] to construct sets of t MAXMOLS(16) for the two further values $t = 7$ and $t = 8$, thus reducing the number of open cases to three; the remaining open cases are $t = 5$, $t = 6$, and $t = 12$.

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).

We will also use results on the (non)existence of spreads and ovoids of the hyperbolic quadric $Q^+(2m + 1, q)$ to construct infinite classes of $q^{2n-1} - 1$ MAXMOLS(q^{2n}), for $n \geq 2$ and q a power of two, and for $n = 2$ and q a power of three. The first example arises for $q = 2$ and $n = 2$, giving us 7 MAXMOLS(16) via a computer free method.

2. Partial Spreads in *PG*(3, 4) \ *PG*(3, 2)

In what follows, we take $PG(3, 2)$ to be the "natural" Baer subgeometry Π_0 of $\Pi = PG(3, 4)$ which is coordinatized by the binary vectors in the vector space $V = V(4, 4)$. We shall denote the corresponding subgroup of order 16 of V by U, and write $GF(4) = \{0, 1, \omega, \omega^2\}$. Then U, ωU and $\omega^2 U$ are three pairwise disjoint subgroups partitioning the quaternary vectors associated with the 15 points of Π_0; hence they may be added to the r subgroups of V associated with any partial spread $\mathcal{S}$ of r lines in $\Pi \setminus \Pi_0$ to give a PCP $\mathcal{P}$ with $r + 3$ components, and one may hope that the associated translation net is transversal-free (and hence the corresponding set of MOLS maximal) provided that $\mathcal{S}$ is maximal.

As already reported in [13], a computer search for maximal partial spreads in $PG(3, 4) \setminus PG(3, 2)$ based on the computer program of [4] for determining the spreads in $PG(3, 4) \setminus PG(3, 2)$ gave the following result:

PROPOSITION 1. *A maximal partial spread of r pairwise skew lines in* $PG(3, 4) \setminus PG(3, 2)$ *exists if and only if* $6 \leq r \leq 10$ *or* $r = 14$.

It turns out that every maximal partial spread of 6 or 7 pairwise skew lines in $PG(3, 4) \setminus PG(3, 2)$ gives rise to a transversal-free translation net of order 16 and degree 9 or 10, respectively, as explained above. This follows from an exhaustive computer search. To facilitate this search, we will provide some auxiliary theoretical results which allow us to reduce the complexity of the search considerably. As these results are appropriate modifications of similar results in our previous paper [13], we will leave some details to the reader.

In what follows, we consider any fixed transversal T of the net $\mathcal{D}$ of degree $r + 3$ associated with the PCP $\mathcal{P}$ coming from a given MPS $\mathcal{S}$ of size $r \in \{6, 7\}$ in $\Pi \setminus \Pi_0$. Without loss of generality, we also assume that T contains the origin 0.

We begin with the following simple but useful result which is analogous to Lemma 3.3 of [13]. It concerns the *holes* of the MPS $\mathcal{S}$, i.e., the points of $\Pi \setminus \Pi_0$ which are not covered by a line of $\mathcal{S}$.

LEMMA 2. *The point* $\langle u \rangle$ *of* Π *is a hole for every element* $u \in T \setminus \{0\}$. *Moreover, if* $0, u, v$ *are three elements of* T *for which* $\langle u \rangle$ *and* $\langle v \rangle$ *are distinct points of* Π*, then the "sum"* $\langle u + v \rangle$ *of these two holes is likewise a hole.*

Proof. If $\langle u \rangle$ would be on a line of $\mathcal{S}$ or in Π_0, the corresponding subgroup U would intersect the transversal T in the distinct elements 0 and u, a contradiction. Thus $\langle u \rangle$ is indeed a hole. Now let $\langle u \rangle$ and $\langle v \rangle$ be distinct points of Π, and assume $0, u, v \in T$. We apply the first assertion to the transversal $T + u$ of $\mathcal{D}$, noting $u, 0, u + v \in T + u$, to conclude that $\langle u + v \rangle$ is indeed a hole. ■

Let $u \in T \setminus \{0\}$. We call the hole $\langle u \rangle$ of Π, respectively the point u of T, *thin* if $\langle u \rangle \cap T = \{0, u\}$; *semifat* if $|\langle u \rangle \cap T| = 3$; and *fat* if $\langle u \rangle \subset T$. The major two theoretical steps consist of showing that T more or less "contains" thin points only; this corresponds to Proposition 3.4 in [13]. Indeed, the proof for the following first result proceeds exactly as in [13].

PROPOSITION 3. *There are no fat holes at all. Moreover, there exists at most one semifat hole.*

PROPOSITION 4. *Every point* $u \in T \setminus \{0\}$ *is actually thin provided that* $r = 7$. *If there exists a semifat hole* $\langle u \rangle$, $u \in T \setminus \{0\}$, *for the case* $r = 6$, *then* $\langle u \rangle$ *lies on* 13 *lines each of which contains precisely three further holes.*

Proof. Assume the existence of a semifat point in T, say $0, u, \lambda u \in T$, where $u \neq 0$ and $\lambda \notin \{0, 1\}$. As T has 16 elements, we get 13 vectors $v \in T \setminus \langle u \rangle$. For each choice of v, the points $\langle u\rangle$, $\langle v\rangle$, $\langle u+v\rangle$ and $\langle \lambda u+v\rangle$ are holes (by Lemma 2). By Proposition 3, no point $\langle v\rangle$ can be semifat, and hence we get $3\cdot 13$ points distinct from $\langle u\rangle$ in this way, all of which are holes.

If we assume $r=7$, then there are only 35 holes altogether, so that there must be holes occurring in two different ways, say $0, u, \lambda u, v, v' \in T$, where v' gives a hole on the line L through $\langle u\rangle$ and $\langle v\rangle$. As $\langle v\rangle$ is not semifat and as L cannot consist of holes only, we have

$$\langle v'\rangle \neq \langle u\rangle, \langle v\rangle, \langle \lambda^2 u+v\rangle.$$

Without loss of generality, we may assume $\langle v'\rangle = \langle u+v\rangle$ (otherwise we may replace u by $u'=\lambda u$). Now there are three possibilities to consider. If $v'=u+v$, the transversal $T+\lambda u$ contains the elements 0 and $(u+v)+\lambda u=\lambda^2 u+v$, contradicting our observation that $\langle \lambda^2 u+v\rangle$ cannot be a hole. The case $v'=\lambda(u+v)$ leads to the same contradiction by considering $T+v$ and noting $\langle \lambda(u+v)+v\rangle = \langle \lambda^2 u+v\rangle$. Finally, the case $v'=\lambda^2(u+v)$ is excluded as before by considering $T+u$.

For $r=6$, we do not obtain a contradiction if we assume the existence of a semifat point, as there will be altogether 40 holes in this case. But then the same reasoning as before immediately gives the structural restriction stated in the assertion (the 13 lines are the lines joining $\langle u\rangle$ to $\langle v\rangle$, with $v\in T\setminus\langle u\rangle$). ■

3. The Computer Searches

To perform the computer searches, we used GAP [7]. As already announced, the searches established the following result.

THEOREM 5. *Every maximal partial spread of* 6 *or* 7 *pairwise skew lines in* $PG(3,4)\setminus PG(3,2)$ *gives rise to a transversal-free translation net of order* 16 *and degree* 9 *or* 10*, respectively.*

In order to establish Theorem 5, we have used the setup of the preceding section. In particular, the restrictions in Proposition 4 considerably simplify the exhaustive search for a possible transversal T of the translation net $\mathcal{D}$ constructed from an MPS $\mathcal{S}$ in $PG(3,4)\setminus PG(3,2)$.

By Proposition 4, T gives rise to fifteen thin points of Π provided that $r=7$. The computer searches of [4] and [13] show that there is (up to equivalence under $P\Gamma L(4,4)$) only one maximal partial spread of size $r=6$ in $PG(3,4)\setminus PG(3,2)$. It is a simple matter to check that the 40 holes determined by this MPS do not form a configuration as described in Proposition 4; thus T gives rise to fifteen thin points of Π also for $r=6$.

There is (up to equivalence under $P\Gamma L(4,4)$) exactly one maximal partial spread of size $r=7$ in $PG(3,4)\setminus PG(3,2)$. We checked this MPS and the one for $r=6$; in both cases, the corresponding net turned out not to admit a transversal (containing 0 and fifteen thin points). This establishes Theorem 5. As an immediate consequence, we obtain the desired new examples of MAXMOLS(16):

COROLLARY 6. *There exist t MAXMOLS*(16) *for* $t=7$ *and* $t=8$.

We conclude this section with two remarks. As explained in Section 2, any MPS of $PG(3,4) \setminus PG(3,2)$ with size r yields a PCP $\mathcal{P}$ with $r+3$ components in the additive group of the vector space $V = V(4,4)$. We may of course view this group as the additive group of $V(8,2)$, and hence $\mathcal{P}$ can be considered as a partial 3-spread $\mathcal{T}$ in $PG(7,2)$. In view of Theorem 5, the associated translation net is transversal-free for $r \in \{6,7\}$; thus $\mathcal{T}$ is maximal in these cases.

We know of the existence of maximal partial 3-spreads of size 9 in $PG(7,2)$. Namely, the hyperbolic quadric $Q^+(7,2)$ in $PG(7,2)$ has a spread consisting of nine 3-dimensional subspaces [6,18,19]. This spread of $Q^+(7,2)$ is maximal since an arbitrary 3-dimensional space in $PG(7,2)$ intersects a hyperbolic quadric non-trivially.

On the other hand, the existence of a maximal partial 3-spread in $PG(7,2)$ of size 10 was not known. We summarize these observations in the following proposition.

PROPOSITION 7. *There exist maximal partial* 3*-spreads of sizes* 9 *and* 10 *in* $PG(7,2)$.

Our second remark concerns a failed attempt to find 12 MAXMOLS(16) by a similar approach. It is known to be possible to find three pairwise disjoint Baer subgeometries in $PG(3,4)$, actually even to partition $PG(3,4)$ into three Baer subgeometries and eight lines. By a computer result of Penttila [16], there are precisely two such partitions up to equivalence, see also Mellinger [15]. Motivated by this fact, we decided to look for maximal partial spreads in $\Pi \setminus (B_1 \cup B_2 \cup B_3)$, where the B_i are three pairwise disjoint Baer subgeometries in $\Pi = PG(3,4)$. Clearly the first Baer subspace B_1 may always be assumed to be the standard $PG(3,2)$. Also B_2 can be chosen as a fixed Baer subspace skew to B_1, [15]. So, the difference in the tuples (B_1, B_2, B_3) that need to be investigated, occurs only in the third position; for the third Baer subspace B_3 there are precisely three choices.

Now there exist maximal partial spreads of five mutually skew lines in $\Pi \setminus (B_1 \cup B_2 \cup B_3)$. Such an MPS $\mathcal{S}$ gives rise to a translation net $\mathcal{D}$ of order 16 and degree 14, by extending the PCP associated with $\mathcal{S}$ with nine new components, three for each of the Baer subspaces B_i (similar to the approach explained at the beginning of Section 2). We had hoped that one might find a transversal-free translation net $\mathcal{D}$ and hence a corresponding set of 12 MAXMOLS(16) in this way, but unfortunately in all cases $\mathcal{D}$ turned out to have a transversal $PG(3,2)$ (and thus to extend to an affine translation plane of order 16).

4. Infinite Classes of MAXMOLS Arising from Spreads of $Q^+(4n-1, q)$

Consider the hyperbolic quadric $Q^+(2m+1,q)$ in $PG(2m+1,q)$. A *spread* of this quadric is a set of q^m+1 pairwise disjoint generators, that is, a set of q^m+1 pairwise disjoint m-spaces on $Q^+(2m+1,q)$. An *ovoid* of this quadric is a set of q^m+1 points on the quadric such that no generator contains two of them.

It is known that for m even, the quadric $Q^+(2m+1,q)$ has no spread. For a survey on (non)existence of spreads and ovoids we refer to [20].

THEOREM 8. *Suppose that* $Q^+(4n-1,q)$ *has a spread and that* $Q^+(4n+1,q)$ *does not have an ovoid. Then there exist* $q^{2n-1}-1$ *MAXMOLS*(q^{2n}).

Proof. Start with a spread $\mathcal{S}$ of $Q^+(4n-1, q)$ in $PG(4n-1, q)$. Embed $PG(4n-1, q)$ in $PG(4n, q)$ and consider the net whose points are the affine points of $PG(4n, q)$ and whose lines are the sets of affine points of $(2n)$-spaces in $PG(4n, q)$ that intersect $PG(4n-1, q)$ in an element of $\mathcal{S}$.

With this net corresponds a set of $q^{2n-1}-1$ MOLS(q^{2n}). It suffices to show that the net is transversal-free to prove that these MOLS are in fact MAXMOLS. Suppose, by way of contradiction, that it admits a transversal T. Then T consists of q^{2n} points of $PG(4n, q) \setminus PG(4n-1, q)$.

If P_1 and P_2 are points of T, then P_1P_2 intersects $PG(4n-1, q)$ in a point outside $Q^+(4n-1, q)$. Indeed, otherwise this line would intersect $PG(4n-1, q)$ in a point of an element of $\mathcal{S}$, say S, and the transversal T would contain at least two points of the line $\langle P_1, S\rangle \setminus PG(4n-1, q)$ of the net.

Now in the dual space of $PG(4n, q)$, $PG(4n-1, q)$ becomes a point P, the elements of $\mathcal{S}$ become $(2n)$-spaces through P, and $Q^+(4n-1, q)$ becomes a cone with vertex P and base a quadric $Q^+(4n-1, q)$. The point P_1 (P_2) becomes a $(4n-1)$-space π_1 (π_2) not through P and the line P_1P_2 becomes a $(4n-2)$-space that intersects the cone in a nonsingular quadric $Q(4n-2, q)$.

Embed the cone in a nonsingular $Q^+(4n+1, q)$ in $PG(4n+1, q)$ and apply the polarity of $Q^+(4n+1, q)$. This polarity maps π_i onto a bisecant to $Q^+(4n+1, q)$ through P, $i = 1, 2$. Call the second point of $Q^+(4n+1, q)$ on this line P_i'. Then $\langle P_1', P_2', P\rangle$ intersects $Q^+(4n+1, q)$ in a nonsingular conic, since π_1 and π_2 intersect in a space that has a nonsingular intersection with $Q^+(4n+1, q)$.

Therefore the $q^{2n}+1$ points $P, P_1', P_2', \ldots$ form an ovoid of $Q^+(4n+1, q)$, a contradiction. ∎

COROLLARY 9. *There exist $q^{2n-1}-1$ MAXMOLS(q^{2n}) for $n \geq 2$ and q even, and for $n = 2$ and q a power of three.*

Proof. For these values for n and q it is known that $Q^+(4n-1, q)$ has a spread, see Dye [6] and Thas [18,19], and that $Q^+(4n+1, q)$ does not have an ovoid, see Kantor [14] and Shult [17]. ∎

Remark 10. For $q = 2$ and $n = 2$, we obtain 7 MAXMOLS(16). Hence, in addition to Corollary 6, also a computer free construction of 7 MAXMOLS(16) is presented.

Acknowledgment

Some of the research for this note was done while Dieter Jungnickel visited Ghent University; he gratefully acknowledges the hospitality extended to him.

References

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 $\Omega^{+}(10, 3)$, *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.