



ELSEVIER

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta


Embedding a Latin square with transversal into a projective space [☆]

Lou M. Pretorius^a, Konrad J. Swanepoel^b

^a Department of Mathematics and Applied Mathematics, University of Pretoria, Pretoria 0002, South Africa

^b Department of Mathematics, London School of Economics and Political Science, Houghton Street, WC2A 2AE, London, United Kingdom

ARTICLE INFO

Article history:

Received 20 May 2010

Available online xxxx

Keywords:

Latin square

Desarguesian projective plane

Projective space

Finite geometry

Transversal

MOLS

ABSTRACT

A Latin square of side n defines in a natural way a finite geometry on $3n$ points, with three lines of size n and n^2 lines of size 3. A Latin square of side n with a transversal similarly defines a finite geometry on $3n+1$ points, with three lines of size n , n^2-n lines of size 3, and n concurrent lines of size 4. A collection of k mutually orthogonal Latin squares defines a geometry on kn points, with k lines of size n and n^2 lines of size k . Extending the work of Bruen and Colbourn [A.A. Bruen, C.J. Colbourn, Transversal designs in classical planes and spaces, J. Combin. Theory Ser. A 92 (2000) 88–94], we characterise embeddings of these finite geometries into projective spaces over skew fields.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

1.1. Definitions and notation

A Latin square of side $n \geq 3$ is an $n \times n$ matrix $L = [a_{ij}]$ with entries from a set S of n symbols such that each symbol appears once in each row and once in each column. A transversal of a Latin square $[a_{ij}]$ is a selection of n positions $(i, \sigma(i))$, $i = 1, \dots, n$, no two in the same row and no two in the same column (i.e., σ is a permutation), such that all symbols occur (i.e., $(a_{i, \sigma(i)})_{i=1}^n$ is a permutation of the symbols in S). Two Latin squares $L_1 = [a_{ij}]$ and $L_2 = [b_{ij}]$ are orthogonal if the n^2 ordered pairs (a_{ij}, b_{ij}) , $1 \leq i, j \leq n$, are all distinct. As usual, we abbreviate the term *mutually orthogonal Latin squares*

[☆] This material is based upon work supported by the National Research Foundation. Part of this work was done while Swanepoel was at the Department of Decision Science of the University of South Africa as a research associate.

E-mail addresses: lou.pretorius@up.ac.za (L.M. Pretorius), k.swanepoel@lse.ac.uk (K.J. Swanepoel).

by MOLS. See Section III of the Handbook of Combinatorial Designs [3] for a comprehensive survey on Latin squares.

A triple $(V, \mathcal{P}, \mathcal{B})$ is called a *transversal design* $\text{TD}(k, n)$ of order $n \geq 3$ and block size $k \geq 3$ if V is a set of size kn , \mathcal{P} a partition of V into k subsets of size n , each called a *part*, and \mathcal{B} is a set of k -subsets of V , each called a *block*, such that any two distinct elements of V are contained in either a unique part or a unique block, but not both. This definition agrees with the definition in [2], except that they use the term group instead of part. If $X, Y \in V$ are distinct, we denote the unique part or block that contains them by XY . It is well known that a Latin square of side n is equivalent to a $\text{TD}(3, n)$ by letting one part be the set of row indices, the second part the set of column indices, and the third part the set of symbols. The blocks are then sets of the form $\{i, j, a_{ij}\}$, where i is a row index and j a column index. More generally, a collection of k MOLS is equivalent to a $\text{TD}(k+2, n)$ by duplicating the set of symbols k times. A Latin square with a transversal that has been singled out is equivalent to a $\text{TD}(3, n)$ together with an additional partition \mathcal{T} of the set V into n pairwise disjoint blocks.

The following binary operation, associated with a $\text{TD}(3, n)$, is fundamental to our discussion. Let $(V, \mathcal{P}, \mathcal{B})$ be a $\text{TD}(3, n)$ with $\mathcal{P} = \{P_1, P_2, P_3\}$. Fix arbitrary points $1_1 \in P_1$ and $1_2 \in P_2$. By the definition of a $\text{TD}(3, n)$, $1_1 1_2 \cap P_3$ is a singleton, say $\{1_3\}$. We write $1_3 = 1_1 1_2 \cap P_3$ for short. Given any $X, Y \in P_1$, let $X' = 1_2 X \cap P_3$, $Y' = 1_3 Y \cap P_2$, and finally define $X \odot Y := X' Y' \cap P_1$. The equations $A \odot X = B$ and $Y \odot A = B$ both have unique solutions for all $A, B \in P_1$. Furthermore, 1_1 is an identity element. Therefore, (P_1, \odot) is a quasigroup with an identity, i.e., a loop [3, III.2], [11, p. 1].

Let \mathbb{D} be a skew field. Denote its multiplicative group by $\mathbb{D}^* := \mathbb{D} \setminus \{0\}$. Let \mathbb{D}^{d+1} denote the $(d+1)$ -dimensional vector space of $(d+1)$ -tuples of \mathbb{D} . Since \mathbb{D} is not necessarily commutative, there are two ways of multiplying a vector by a scalar. We choose the convention that \mathbb{D}^{d+1} is a *right* vector space. Thus for $\mathbf{x} = (x_1, x_2, \dots, x_{d+1}) \in \mathbb{D}^{d+1}$ and $\alpha \in \mathbb{D}$, the scalar multiple $\mathbf{x}\alpha$ is defined by

$$(x_1, x_2, \dots, x_{d+1})\alpha := (x_1\alpha, x_2\alpha, \dots, x_{d+1}\alpha).$$

We denote the zero vector by $\mathbf{o} = (0, 0, \dots, 0)$.

Let $P^d(\mathbb{D})$ be the d -dimensional projective space over \mathbb{D} . We use homogeneous coordinates $[x_1, \dots, x_{d+1}]$ for a point in $P^d(\mathbb{D})$, or $[x, y, z]$ when $d=2$. Note that, since we started off with a right vector space, the homogeneous equation of a $(d-1)$ -flat or *hyperplane* in $P^d(\mathbb{D})$ has the form

$$\alpha_1 x_1 + \dots + \alpha_{d+1} x_{d+1} = 0, \quad \alpha_i \in \mathbb{D}, \text{ not every } \alpha_i \text{ equals } 0.$$

A *pencil of hyperplanes* is a collection of all hyperplanes that contain a given $(d-2)$ -flat.

An *embedding of the* $\text{TD}(k, n)$ $(V, \mathcal{P}, \mathcal{B})$ *into* $P^d(\mathbb{D})$ is an injection $\varphi: V \rightarrow P^d(\mathbb{D})$ such that $\varphi(P)$ is contained in a hyperplane H_P of $P^d(\mathbb{D})$ for each $P \in \mathcal{P}$, $\varphi(B)$ is contained in a line ℓ_B of $P^d(\mathbb{D})$ for each $B \in \mathcal{B}$, and such that the hyperplanes H_P , $P \in \mathcal{P}$, are distinct, the lines ℓ_B , $B \in \mathcal{B}$, are distinct, and no ℓ_B is contained in an H_P . This definition of embedding coincides with the embeddings in [2]. The requirement that no ℓ_B is contained in an H_P ensures that no points in $\varphi(V)$ can lie on $H_P \cap H_Q$, where $P, Q \in \mathcal{P}$ are distinct.

An *embedding of a Latin square* L into $P^d(\mathbb{D})$ is an embedding of the associated $\text{TD}(3, n)$. An *embedding of a Latin square with a transversal* into $P^d(\mathbb{D})$ is an embedding of the associated $\text{TD}(3, n)$ such that, if the additional partition of V is $\mathcal{T} = \{B_1, \dots, B_n\}$, then the lines $\ell_{B_1}, \dots, \ell_{B_n}$ are concurrent. This point of concurrency is called a *transversal point* of the embedded Latin square, and will be denoted by ∞ . An *embedding of a collection of* k *MOLS* into $P^d(\mathbb{D})$ is an embedding of the associated $\text{TD}(k+2, n)$. In all cases, an embedding is called *proper* if $\varphi(V)$ does not lie on a hyperplane.

1.2. Overview of the paper

In this paper we give a full description of embeddings of Latin squares, Latin squares with transversals, and MOLS into Desarguesian projective planes and spaces, that is, projective planes and spaces over a skew field. Motzkin [8] made a first attempt at characterising an embedding of a Latin square into a projective plane over a field. A correct description for this case was given by Kelly and Nwankpa [6, Theorems 3.11 and 3.12]. Bruen and Colbourn [2] introduced the above notion of an embedding into $P^d(\mathbb{D})$ also in the case where \mathbb{D} is a field. They gave a detailed description for the 2-dimensional

case, and briefly described an extension to higher dimensions [2, Theorem 5.1]. We give a complete proof of their higher-dimensional result, generalised to skew fields. Our extension to skew fields poses only minor algebraic difficulties. In Section 2 we state without proof the 2-dimensional cases of our results. (They follow from the corresponding higher-dimensional results in Section 5.) In Section 3 we discuss the finite groups that arise as subgroups of \mathbb{D}^* . This is a much richer class of groups than the finite subgroups of fields, which are necessarily cyclic. Section 4 contains some algebraic preparation, and finally in Section 5 we formulate and prove all our higher-dimensional results.

2. Embeddings into Desarguesian projective planes

In this section we formulate the planar case of our results without proof. Although the case where \mathbb{D} is a field is well known, we could not find the non-commutative versions anywhere in the literature.

In Theorem 5 below we show that if a Latin square with transversal is embedded in a Desarguesian projective plane, then the three parts of the corresponding $TD(3, n)$ must lie on concurrent lines. This generalises Case 1 of Theorem 4.1 of Bruen and Colbourn [2] from fields to skew fields. Our original motivation for such a generalisation was to show that the 20-point geometry obtained from the affine plane of order 5 by removing the 5 points of some line, can be embedded into $P^2(\mathbb{D})$ for some skew field \mathbb{D} only if \mathbb{D} has characteristic 5. This result is used in the proof of [9, Lemma 13]. It is sufficient to consider the 16-point geometry in \mathbb{F}_5^2 consisting of three parallel lines together with an additional point. This is an embedding of a Latin square of side 5 with transversal, and Theorem 5 applies.

Let $(V, \mathcal{P}, \mathcal{B})$ be a $TD(3, n)$ that is already embedded in $P^2(\mathbb{D})$, i.e., $V \subseteq P^2(\mathbb{D})$ and there exist three distinct lines h_1, h_2, h_3 of $P^2(\mathbb{D})$ such that $\mathcal{P} = \{V \cap h_1, V \cap h_2, V \cap h_3\}$. We refer to this situation by saying that $(V, \mathcal{P}, \mathcal{B})$ lies on the lines h_1, h_2, h_3 . We now distinguish between whether h_1, h_2, h_3 are concurrent or not.

If the h_i are concurrent, then after choosing $1_1 \in h_1 \cap V$ and $1_2 \in h_2 \cap V$, we may choose homogeneous coordinates such that the point of concurrency of the h_i is $[1, 0, 0]$, $1_1 = [0, 0, 1]$, $1_2 = [0, 1, 1]$ and $1_3 = [0, 1, 0]$. Then the equation of h_1 is $y = 0$, of h_2 is $y = z$ and of h_3 is $z = 0$. The coordinates of the points in V depend on the choices made above. In the next proposition we describe all possible coordinatisations. It extends Proposition 10 of our previous paper [9]. A further extension is found in Proposition 11.

Proposition 1. *Let $(V, \mathcal{P}, \mathcal{B})$ be a $TD(3, n)$ which lies on the concurrent lines h_1, h_2, h_3 of $P^2(\mathbb{D})$. If we choose homogeneous coordinates as above, then there exists a subgroup G of $(\mathbb{D}, +)$ of order n such that*

$$\left. \begin{aligned} h_1 \cap V &= \{[\gamma, 0, 1] \mid \gamma \in G\}, \\ h_2 \cap V &= \{[\gamma, 1, 1] \mid \gamma \in G\}, \\ h_3 \cap V &= \{[-\gamma, 1, 0] \mid \gamma \in G\}. \end{aligned} \right\} \tag{1}$$

The group G depends only on the choice of coordinates. For any two such choices, the two groups G_1 and G_2 so obtained satisfy $G_1 = bG_2a$ for some $a, b \in \mathbb{D}^*$.

Conversely, given any subgroup G of $(\mathbb{D}, +)$ of order n , (1) gives an embedding of a $TD(3, n)$ on the concurrent lines h_1, h_2, h_3 with equations $y = 0, y = z, z = 0$, respectively.

Suppose that a skew field \mathbb{D} contains a finite additive subgroup G . Then \mathbb{D} necessarily has prime characteristic p , and G is isomorphic to the direct sum of finitely many copies of \mathbb{Z}_p , the additive group of the field \mathbb{F}_p with p elements. The next corollary is generalised in Corollary 12.

Corollary 2. *Suppose that a $TD(3, n)$ lies on three lines in $P^2(\mathbb{D})$.*

- *If \mathbb{D} has characteristic 0, the lines are nonconcurrent.*
- *If \mathbb{D} has prime characteristic p and the lines are concurrent, then n is a power of p .*

Now we consider the case where h_1, h_2, h_3 are nonconcurrent. After choosing $1_1 \in h_1 \cap V$ and $1_2 \in h_2 \cap V$, we may choose homogeneous coordinates such that $1_1 = [0, 1, 1]$, and $1_2 = [1, 0, 1]$,

$1_3 = [1, -1, 0]$, and such that h_1 has equation $x = 0$, h_2 equation $y = 0$, and h_3 equation $z = 0$. Again, the coordinates of the points in V depend on the choices made above. The next proposition extends Proposition 12 in the paper [9]. A further extension is found in Proposition 13.

Proposition 3. *Let $(V, \mathcal{P}, \mathcal{B})$ be a $TD(3, n)$ which lies on the nonconcurrent lines h_1, h_2, h_3 of $P^2(\mathbb{D})$. If we choose homogeneous coordinates as above, then there exists a subgroup G of (\mathbb{D}^*, \cdot) of order n such that*

$$\left. \begin{aligned} h_1 \cap V &= \{[0, \gamma, 1] \mid \gamma \in G\}, \\ h_2 \cap V &= \{[\gamma, 0, 1] \mid \gamma \in G\}, \\ h_3 \cap V &= \{[-1, \gamma, 0] \mid \gamma \in G\}. \end{aligned} \right\} \quad (2)$$

The group G depends only on the choice of coordinates. For any two such choices, the two groups G_1 and G_2 so obtained are conjugates, i.e., $G_1 = a^{-1}G_2a$ for some $a \in \mathbb{D}^*$.

Conversely, given any subgroup G of (\mathbb{D}^*, \cdot) of order n , (2) gives an embedding of a $TD(3, n)$ on the nonconcurrent lines h_1, h_2, h_3 with equations $x = 0, y = 0, z = 0$, respectively.

The next corollary, although purely geometric, needs some algebra in its proof (as can be seen in the proof of its higher-dimensional counterpart Corollary 16).

Corollary 4. *If a $TD(3, n)$ can be embedded in three concurrent lines of $P^2(\mathbb{D})$, then it cannot be embedded in three nonconcurrent lines of $P^2(\mathbb{D})$.*

If G is a subgroup of $(\mathbb{D}, +)$ and $a \in \mathbb{D}$, then Ga is also a subgroup of $(\mathbb{D}, +)$, and

$$\mathbb{D}_G := \{a \in \mathbb{D} \mid Ga \subseteq G\}$$

is a subring of \mathbb{D} . If G is nontrivial, for any $g \in G \setminus \{0\}$, \mathbb{D}_G is a subset of $g^{-1}G$, which is isomorphic to G . Consequently, if G is finite, \mathbb{D} has prime characteristic p , say, and then G is a p -group, and $(\mathbb{D}_G, +)$ is also a p -group. (When G is finite, \mathbb{D}_G is in fact a subfield of \mathbb{D} .)

Theorem 5. *If a Latin square of side $n \geq 3$ with transversal is embedded as a $TD(3, n)$ in three lines h_i of $P^2(\mathbb{D})$ with transversal point ∞ , then the h_i are concurrent. If homogeneous coordinates are chosen as in Proposition 1, then the transversal point $\infty = [\gamma, a, 1]$, where $\gamma \in G, a \in \mathbb{D}_G \setminus \{0, 1\}$, and G is the subgroup of $(\mathbb{D}, +)$ associated to the embedding. Conversely, any point with these coordinates is a transversal point.*

In particular, a transversal point lies on a line with equation $y = az$ for some $a \in \mathbb{D}_G \setminus \{0, 1\}$. A Latin square embedded in three concurrent lines with associated group G has a transversal if and only if $|\mathbb{D}_G| \geq 3$.

The above theorem is generalised in Theorem 15.

The next theorem gives a description of the embedding of mutually orthogonal Latin squares.

Theorem 6. *Let $(V, \mathcal{P}, \mathcal{B})$ be a $TD(k, n)$, $n \geq 3, k \geq 4$ with an embedding into $P^2(\mathbb{D})$ on lines h_1, h_2, \dots, h_k . Then the lines h_1, \dots, h_k are concurrent. If coordinates are chosen such that h_1, h_2, h_3 have coordinates as in Proposition 1, then there exist distinct $a_4, \dots, a_k \in \mathbb{D}_G \setminus \{0, 1\}$ such that*

$$h_i \cap V = \{[\gamma, a_i, 1] \mid \gamma \in G\}, \quad i = 4, \dots, k,$$

where G is a subgroup of $(\mathbb{D}, +)$ of order n . Furthermore, n is a prime power p^m , G is isomorphic to \mathbb{Z}_p^m , $|\mathbb{D}_G| = p^t$ for some $t \leq m$, and $k \leq |\mathbb{D}_G| + 1$.

In particular, if a Latin square with transversal can be embedded into $P^2(\mathbb{D})$, then the Latin square can be extended to a $TD(|\mathbb{D}_G| + 1, n)$ with an embedding that extends the original embedding.

This theorem is generalised in Theorem 17.

3. The finite multiplicative subgroups of skew fields

It is well known that any finite multiplicative subgroup of a field is cyclic. This is in marked contrast to (non-commutative) skew fields where a much greater variety of finite multiplicative groups appear. Completing earlier work of Herstein [5], the finite multiplicative subgroups of skew fields have been characterised by Amitsur [1]. This classification is involved (see the end of this section for a partial formulation) and we only give a few representative examples.

As already observed by Herstein [5], if \mathbb{D} has prime characteristic, any finite subgroup G of \mathbb{D}^* generates a subring which is a finite-dimensional vector space over the prime field of \mathbb{D} , and therefore a subfield of \mathbb{D} . By Wedderburn's theorem, it follows that the subring is commutative, and it follows that G is cyclic. Herstein similarly proved that if G is an abelian subgroup of \mathbb{D}^* (with \mathbb{D} of arbitrary characteristic) then G is cyclic.

The interesting case is therefore when \mathbb{D} is a non-commutative skew field of characteristic 0 and G a nonabelian subgroup of \mathbb{D}^* . The smallest such G is the quaternion group of order 8: $G = \{\pm 1, \pm i, \pm j, \pm k\}$, which is a subset of the quaternions \mathbb{H} . By Proposition 3 this gives a TD(3, 8) of 24 points in $P^2(\mathbb{H})$. Since G is nonabelian, Proposition 3 again gives that this TD(3, 8) cannot be embedded in $P^2(\mathbb{F})$, where \mathbb{F} is a field. By Corollary 4 it can also not be embedded on three concurrent lines of a projective plane over any division ring.

Coxeter [4] classified the finite multiplicative subgroups of the quaternions \mathbb{H} . Those that are not commutative, hence not conjugate to a subgroup of the nonzero complex numbers \mathbb{C}^* , are conjugate to one of the following:

- (1) The *binary dihedral group*

$$D_n^* = \{e^{ik\pi/n}, e^{ik\pi/n}j \mid 0 \leq k < 2n\}$$

of order $4n$ for any $n \geq 2$ (with the quaternion group being the case $n = 2$) giving a TD(3, $4n$),

- (2) the *binary tetrahedral group* consisting of the 24 units of the Hurwitz integers

$$T^* = \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k) \right\}$$

giving a TD(3, 24),

- (3) the *binary octahedral group* O^* of order 48:

$$O^* := T^* \cup \left\{ \frac{1}{\sqrt{2}}(\pm a \pm b) \mid a, b \in \{1, i, j, k\}, a \neq b \right\}$$

giving a TD(3, 48),

- (4) and the *binary icosahedral group* I^* of order 120:

$$I^* := T^* \cup \left\{ \frac{1}{2}(\pm \pi_2 \pm \varphi^{-1} \pi_3 \pm \varphi \pi_4) \mid \begin{array}{l} \pi = \pi_1 \pi_2 \pi_3 \pi_4 \text{ is an even} \\ \text{permutation of } \{1, i, j, k\} \end{array} \right\},$$

where $\varphi = (1 + \sqrt{5})/2$, giving a TD(3, 120).

Amitsur found another class of groups (called D-groups in [1]) that occur as multiplicative subgroups of division rings. They are of the form

$$G_{m,n,r} := \langle a, b \mid a^m = b^n = 1, bab^{-1} = a^r \rangle,$$

where m, n, r satisfy a complicated collection of relations [1, Theorems 4 and 5]. In particular, $r^n \equiv 1 \pmod{m}$ ensures that $|G_{m,n,r}| = mn$. The smallest nonabelian multiplicative subgroup of odd order turns out to be $G_{7,9,2}$ of order 63. As demonstrated by Lam [7], this group occurs in the following skew field. Let ζ be a primitive 21st root of unity. Introduce a new symbol b that satisfies $b^3 = \zeta^7$ and $b\zeta = \zeta^{16}b$. Then the \mathbb{Q} -algebra

$$\mathbb{D} = \{ \alpha + \beta b + \gamma b^2 \mid \alpha, \beta, \gamma \in \mathbb{Q}(\zeta) \}$$

turns out to be a division algebra, so that it is in particular, a skew field. Note that since $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(21) = 12$, the dimension of \mathbb{D} over \mathbb{Q} is 36. If we set $a = \zeta^3$, then the subgroup of \mathbb{D}^* generated by a and b is $G_{7,9,2}$. See Lam [7] for further details, as well as the next largest example $G_{13,9,9}$ of a nonabelian multiplicative subgroup, which is of order 117.

Amitsur [1, Theorem 7] proved that all non-cyclic multiplicative subgroups of division rings must be either of the form $G_{m,n,r}$ where m, n, r satisfy certain properties, or $T^* \times G_{m,n,r}$ where m, n, r satisfy certain properties, or O^* or I^* .

4. Some elementary algebraic lemmas

Lemma 7. *In a skew field of characteristic p , no element can have multiplicative order p .*

Proof. Let x be an element of multiplicative order p , i.e. $x^p = 1$, $x \neq 1$. Then by the binomial theorem modulo p applied to the commuting elements x and -1 ,

$$0 = x^p - 1 = (x - 1)^p \neq 0,$$

a contradiction. (Note that this argument also works for $p = 2$.) \square

Lemma 8. *Let G be a finite nontrivial subgroup of (\mathbb{D}^*, \cdot) , where \mathbb{D} is a skew field. Then $\sum_{g \in G} g = 0$.*

Proof. Consider an arbitrary $g_0 \in G$. Then

$$\sum_{g \in G} g = \sum_{g \in G} g_0 g = g_0 \left(\sum_{g \in G} g \right),$$

thus

$$(1 - g_0) \sum_{g \in G} g = 0.$$

Therefore, either $\sum_{g \in G} g = 0$ or $G = \{1\}$. \square

Lemma 9. *Let G be a finite subgroup of (\mathbb{D}^*, \cdot) , where \mathbb{D} is a skew field. Then the order of G , considered as an element of \mathbb{D} , is nonzero:*

$$\underbrace{1 + 1 + \cdots + 1}_{|G| \text{ times}} \neq 0.$$

Proof. Suppose $|G|1 = 0$ in \mathbb{D} . Then \mathbb{D} has prime characteristic p , say, and p divides $|G|$. By a theorem of Cauchy [10, Theorem 4.2], G has an element of order p , which contradicts Lemma 7. \square

Lemma 10. *Let G be a finite subgroup of (\mathbb{D}^*, \cdot) , where \mathbb{D} is a skew field. Suppose that $G + a = Gb$ for some $a, b \in \mathbb{D}$. Then either $a = 0$ or $G = \{1\}$.*

Proof. Suppose G is nontrivial. Then

$$\begin{aligned} 0 &= \sum_{g \in G} g \quad (\text{Lemma 8}) \\ &= \sum_{g \in G} (-a + gb) = -|G|a + \left(\sum_{g \in G} g \right) b \\ &= -|G|a \quad (\text{again Lemma 8}). \end{aligned}$$

By Lemma 9, $a = 0$. \square

5. Higher dimensions

Before we generalise Propositions 1 and 3, we establish the following notation. Let $(V, \mathcal{P}, \mathcal{B})$ be a $TD(3, n)$ embedded in $P^d(\mathbb{D})$. Thus $V \subseteq P^d(\mathbb{D})$ and there exist three distinct hyperplanes H_1, H_2, H_3 of $P^d(\mathbb{D})$ such that $\mathcal{P} = \{V \cap H_1, V \cap H_2, V \cap H_3\}$. We refer to this situation by saying that $(V, \mathcal{P}, \mathcal{B})$ lies on the hyperplanes H_1, H_2, H_3 . We now distinguish between the cases where the dimension of $H_1 \cap H_2 \cap H_3$ is $d - 2$ or $d - 3$.

If $\dim(H_1 \cap H_2 \cap H_3) = d - 2$, then after choosing $1_1 \in H_1 \cap V$ and $1_2 \in H_2 \cap V$, we may choose homogeneous coordinates such that $H_1 \cap H_2 \cap H_3 = \{\mathbf{x}, 0, 0 \mid \mathbf{x} \in \mathbb{D}^{d-1}\}$, $1_1 = [\mathbf{o}, 0, 1]$, $1_2 = [\mathbf{o}, 1, 1]$ and $1_3 = [\mathbf{o}, 1, 0]$. (Recall that \mathbf{o} is the $(d - 1)$ -dimensional zero vector.) Then H_1 has the equation $x_d = 0$, H_2 the equation $x_d = x_{d+1}$, and H_3 the equation $x_{d+1} = 0$. The coordinates of the points in V depend on the choices made above. The next proposition describes all possible coordinatisations.

Proposition 11. *Let $(V, \mathcal{P}, \mathcal{B})$ be a $TD(3, n)$ which lies on the hyperplanes H_1, H_2, H_3 of $P^d(\mathbb{D})$ such that $\dim(H_1 \cap H_2 \cap H_3) = d - 2$. If we choose homogeneous coordinates as above, then there exists a subgroup G of $(\mathbb{D}^{d-1}, +)$ of order n such that*

$$\left. \begin{aligned} H_1 \cap V &= \{[\boldsymbol{\gamma}, 0, 1] \mid \boldsymbol{\gamma} \in G\}, \\ H_2 \cap V &= \{[\boldsymbol{\gamma}, 1, 1] \mid \boldsymbol{\gamma} \in G\}, \\ H_3 \cap V &= \{[-\boldsymbol{\gamma}, 1, 0] \mid \boldsymbol{\gamma} \in G\}. \end{aligned} \right\} \tag{3}$$

The group G depends only on the choice of coordinates. For any two such choices, the two groups G_1 and G_2 so obtained, satisfy $G_1 = TG_2a$ for some $a \in \mathbb{D}^*$ and $T \in GL_{d-1}(\mathbb{D})$.

Conversely, given any subgroup G of $(\mathbb{D}^{d-1}, +)$ of order n , (3) gives an embedding of a $TD(3, n)$ on the hyperplanes H_1, H_2, H_3 with equations $x_d = 0, x_d = x_{d+1}, x_{d+1} = 0$, respectively.

Proof. We show that the operation \odot defined in the introduction corresponds with addition in \mathbb{D}^{d-1} . Let $G = \{\boldsymbol{\gamma} \mid [\boldsymbol{\gamma}, 0, 1] \in h_1 \cap V\}$. Note that $\mathbf{o} \in G$. For any $\boldsymbol{\alpha}, \boldsymbol{\beta} \in G$, let $X = [\boldsymbol{\alpha}, 0, 1]$ and $Y = [\boldsymbol{\beta}, 0, 1]$. Then a simple calculation shows that $X' = [-\boldsymbol{\alpha}, 1, 0]$, $Y' = [\boldsymbol{\beta}, 1, 1]$, and $X \odot Y = [\boldsymbol{\alpha} + \boldsymbol{\beta}, 0, 1]$. Therefore, $\boldsymbol{\alpha} + \boldsymbol{\beta} \in G$, and \odot corresponds to addition in \mathbb{D}^{d-1} , restricted to G . Thus $(G, +)$ is a group. Also, $H_1 \cap V$ has homogeneous coordinates as stated. We furthermore obtain that $H_2 \cap V$ and $H_3 \cap V$ are as stated, by considering the coordinates of the points X' and Y' .

A calculation shows that for any two choices of coordinates as above, the coordinate transformation between them is $[\mathbf{x}, y, z] \mapsto [T\mathbf{x}, ay, az]$ for some $a \in \mathbb{D}^*$ and $T \in GL_{d-1}(\mathbb{D})$. Thus $[\boldsymbol{\gamma}, 0, 1]$ is mapped to $[T\boldsymbol{\gamma}, 0, a] = [T\boldsymbol{\gamma}a^{-1}, 0, 1]$, which gives a new group $G' = TGa^{-1}$.

The proof of the converse, that (3) gives a $TD(3, n)$ for any subgroup G of $(\mathbb{D}^{d-1}, +)$ of order n , is a simple calculation. \square

If \mathbb{D}^{d-1} contains a finite additive group G , then \mathbb{D} has prime characteristic p , say, and G is an \mathbb{F}_p -vector subspace of \mathbb{D}^{d-1} (and therefore isomorphic to a direct sum of finitely many copies of \mathbb{Z}_p).

Corollary 12. *Let a $TD(3, n)$ lie on three hyperplanes in $P^d(\mathbb{D})$.*

- *If \mathbb{D} has characteristic 0, the three hyperplanes intersect in a $(d - 3)$ -flat.*
- *If \mathbb{D} has prime characteristic p and the three hyperplanes intersect in a $(d - 2)$ -flat, then n is a power of p .*

Now we consider the case where $\dim(H_1 \cap H_2 \cap H_3) = d - 3$. After choosing $1_1 \in H_1 \cap V$ and $1_2 \in H_2 \cap V$, we may choose homogeneous coordinates such that $1_1 = [0, 1, 1, \mathbf{o}]$, and $1_2 = [1, 0, 1, \mathbf{o}]$, $1_3 = [-1, 1, 0, \mathbf{o}]$, and such that H_1 has equation $x_1 = 0$, H_2 equation $x_2 = 0$, and H_3 equation $x_3 = 0$. (Here \mathbf{o} is the $(d - 2)$ -dimensional zero vector.) Again, the coordinates of the points in V depend on the choices made above. The next proposition describes all possible coordinatisations. As in the

two-dimensional case, there is a group associated with the $TD(3, n)$, but this group now has a more complicated structure. Define an operation on the Cartesian product $\mathbb{D}^* \times \mathbb{D}^{d-2}$ by

$$(\alpha, \mathbf{x}) \cdot (\beta, \mathbf{y}) := (\alpha\beta, \mathbf{x}\beta + \mathbf{y}).$$

Then $\mathbb{D}^* \times \mathbb{D}^{d-2} = (\mathbb{D}^* \times \mathbb{D}^{d-2}, \cdot)$ is a semidirect product of \mathbb{D}^* with \mathbb{D}^{d-2} [10, p. 137], and can be faithfully represented in $GL_{d-1}(\mathbb{D})$ by mapping (γ, \mathbf{x}) to

$$\begin{bmatrix} \gamma & \mathbf{0} \\ \mathbf{x} & I_{d-2} \end{bmatrix}.$$

For any $T \in GL_{d-2}(\mathbb{D})$ there is an automorphism

$$\phi_T : (\gamma, \mathbf{x}) \mapsto (\gamma, T\mathbf{x})$$

of $\mathbb{D}^* \times \mathbb{D}^{d-2}$.

Proposition 13. *Let $(V, \mathcal{P}, \mathcal{B})$ be a $TD(3, n)$ which lies on the hyperplanes H_1, H_2, H_3 of $P^d(\mathbb{D})$ such that $\dim(H_1 \cap H_2 \cap H_3) = d - 3$. If we choose homogeneous coordinates as above, then there exists a subgroup G of $\mathbb{D}^* \times \mathbb{D}^{d-2}$ of order n such that*

$$\left. \begin{aligned} H_1 \cap V &= \{[0, \gamma, 1, \mathbf{x}] \mid (\gamma, \mathbf{x}) \in G\}, \\ H_2 \cap V &= \{[\gamma, 0, 1, \mathbf{x}] \mid (\gamma, \mathbf{x}) \in G\}, \\ H_3 \cap V &= \{[-1, \gamma, 0, \mathbf{x}] \mid (\gamma, \mathbf{x}) \in G\}. \end{aligned} \right\} \quad (4)$$

The group G depends only on the choice of coordinates. For any two such choices, the two groups G_1 and G_2 so obtained satisfy $G_1 = (a, \mathbf{v}) \cdot \phi_T G_2 \cdot (a, \mathbf{v})^{-1}$ for some $(a, \mathbf{v}) \in \mathbb{D}^* \times \mathbb{D}^{d-2}$ and $T \in GL_{d-2}(\mathbb{D})$.

Conversely, given any subgroup G of $\mathbb{D}^* \times \mathbb{D}^{d-2}$ of order n , (4) gives an embedding of a $TD(3, n)$ on the hyperplanes H_1, H_2, H_3 with equations $x_1 = 0, x_2 = 0, x_3 = 0$, respectively.

Proof. We calculate the loop operation \odot . Let

$$G := \{(\gamma, \mathbf{x}) \in \mathbb{D}^* \times \mathbb{D}^{d-2} \mid [0, \gamma, 1, \mathbf{x}] \in V \text{ for some } \mathbf{x} \in \mathbb{D}^{d-2}\}.$$

Choose $X = [0, \alpha, 1, \mathbf{x}], Y = [0, \beta, 1, \mathbf{y}] \in H_1 \cap V$. Then easy calculations show that $X' = [-1, \alpha, 0, \mathbf{x}], Y' = [\beta, 0, 1, \mathbf{y}]$, and $X \odot Y = [0, \alpha\beta, 1, \mathbf{x}\beta + \mathbf{y}]$. This shows that G is a subgroup of $\mathbb{D}^* \times \mathbb{D}^{d-2}$, and that the coordinates of the $H_i \cap V$ are as stated.

A calculation shows that for any two choices of coordinates as above, the coordinate transformation between them is

$$[\alpha, \beta, \gamma, \mathbf{x}] \mapsto [\alpha\alpha, a\beta, a\gamma, \mathbf{v}(\alpha + \beta - \gamma) + T\mathbf{x}]$$

for some $a \in \mathbb{D}^*, \mathbf{v} \in \mathbb{D}^{d-2}$ and $T \in GL_{d-2}(\mathbb{D})$. Then $[0, \gamma, 1, \mathbf{x}]$ is mapped to

$$\begin{aligned} [0, a\gamma, a, \mathbf{v}\gamma - \mathbf{v} + T\mathbf{x}] &= [0, a\gamma a^{-1}, 1, (\mathbf{v}\gamma - \mathbf{v} + T\mathbf{x})a^{-1}] \\ &= [0, \beta, 1, \mathbf{y}] \end{aligned}$$

where $(\beta, \mathbf{y}) = (a, \mathbf{v}) \cdot (\gamma, T\mathbf{x}) \cdot (a, \mathbf{v})^{-1}$, which gives a new group $G' = (a, \mathbf{v}) \cdot \phi_T G \cdot (a, \mathbf{v})^{-1}$.

The proof of the converse, that (4) gives a $TD(3, n)$ for any subgroup G of $\mathbb{D}^* \times \mathbb{D}^{d-2}$ of order n , is again a simple calculation. \square

Proposition 14. *Consider an embedding of a Latin square of side $n \geq 3$ with transversal in $P^d(\mathbb{D})$ with transversal point ∞ , such that the three hyperplanes of the embedding intersect in a $(d - 3)$ -flat. Then the embedding lies in a hyperplane passing through ∞ . In particular, if $d = 2$, such an embedding does not exist.*

Proof. Suppose that $(V, \mathcal{P}, \mathcal{B})$ lies on three hyperplanes H_1, H_2, H_3 that intersect in a $(d - 3)$ -flat. Let G be the group given by Proposition 13. The subgroup

$$G_1 = \{\gamma \in \mathbb{D}^* \mid [0, \gamma, 1, \mathbf{x}] \in H_1 \cap V \text{ for some } \mathbf{x} \in \mathbb{D}^{d-2}\}$$

of D^* is a homomorphic image of the p -group G , and is therefore also a p -group. By Lemma 7, G_1 is trivial. Since the transversal point does not lie on any H_i , we may write its homogeneous coordinates as $[1, a, b, \mathbf{c}]$ for some $a, b \in \mathbb{D}^*$ and $\mathbf{c} \in \mathbb{D}^{d-2}$. For any $\gamma \in G_1$ and $X = [0, \gamma, 1, \mathbf{x}] \in H_1 \cap V$, a calculation then shows that the projection of X from the transversal point $[1, a, b, \mathbf{c}]$ onto H_3 is $[-1, \gamma b - a, 0, \mathbf{x}b - \mathbf{c}]$. This gives $G_1 b - a \subseteq G_1$. Since any point in $H_3 \cap V$ is such a projection of some point in $H_1 \cap V$, we in fact have equality: $G_1 b = G_1 + a$. By Lemma 10, $G_1 = \{1\}$ and $b - a = 1$. The coordinates given by Proposition 13 become

$$\begin{aligned} H_1 \cap V &= \{[0, 1, 1, \mathbf{x}] \mid \mathbf{x} \in H\}, \\ H_2 \cap V &= \{[1, 0, 1, \mathbf{x}] \mid \mathbf{x} \in H\}, \\ H_3 \cap V &= \{[-1, 1, 0, \mathbf{x}] \mid \mathbf{x} \in H\}, \end{aligned}$$

and it follows that V lies on the hyperplane $x_1 + x_2 - x_3 = 0$. \square

Similar to the two-dimensional case, if G is any finite subgroup of $(\mathbb{D}^{d-1}, +)$ and $a \in \mathbb{D}$, then Ga is also a subgroup of $(\mathbb{D}^{d-1}, +)$, and $\mathbb{D}_G := \{a \in \mathbb{D} \mid Ga \subseteq G\}$ is a subfield of \mathbb{D} . As before, $(\mathbb{D}_G, +)$ is isomorphic to a subgroup of the p -group G , hence is a finite p -group itself. This can be seen as follows. Choose a coordinate $i \in \{1, \dots, d-1\}$ such that the projection G_i of G onto this coordinate is a nontrivial subgroup of $(\mathbb{D}, +)$. Then $\mathbb{D}_G \subseteq \mathbb{D}_{G_i} \subseteq g^{-1}G$ for any $g \in G \setminus \{0\}$.

Theorem 15. *Let $(V, \mathcal{P}, \mathcal{B})$ be a $\text{TD}(3, n)$ with transversal point ∞ with a proper embedding into three hyperplanes H_1, H_2, H_3 of $P^d(\mathbb{D})$. Then $\dim(H_1 \cap H_2 \cap H_3) = d - 2$, and if homogeneous coordinates are chosen as in Proposition 11 with G the group associated with the embedding, then the transversal point $\infty = [\boldsymbol{\gamma}, a, 1]$, where $\boldsymbol{\gamma} \in G$ and $a \in \mathbb{D}_G \setminus \{0, 1\}$. Conversely, any point with these coordinates is a transversal point.*

In particular, a transversal point lies on a line with equation $x_d = ax_{d+1}$ for some $a \in \mathbb{D}_G \setminus \{0, 1\}$. A Latin square embedded in three hyperplanes that intersect in a $(d - 2)$ -flat has a transversal if and only if $|\mathbb{D}_G| \geq 3$.

Proof. By Proposition 14, $\dim(H_1 \cap H_2 \cap H_3) = d - 2$. Consider the group G and coordinates as in Proposition 11. Since the transversal point $\infty \notin H_3$, we may write its coordinates as $[\boldsymbol{\alpha}, \beta, 1]$. The line through ∞ and an arbitrary point $[-\boldsymbol{\gamma}, 1, 0] \in H_3 \cap V$ intersects H_1 in $[\boldsymbol{\gamma}\beta + \boldsymbol{\alpha}, 0, 1]$. Since this point is in V , it has to be of the form $[\boldsymbol{\gamma}', 0, 1]$, and therefore, $\{\boldsymbol{\gamma}\beta + \boldsymbol{\alpha} \mid \boldsymbol{\gamma} \in G\} = G$, i.e., $G\beta + \boldsymbol{\alpha} = G$. It follows that $\boldsymbol{\alpha} \in G$ and $\beta \in \mathbb{D}_G$. Since $[\boldsymbol{\alpha}, \beta, 1] \notin H_1, H_2$, it follows that $\beta \neq 0, 1$.

It is easily checked that for any $\boldsymbol{\alpha} \in G$ and $\beta \in \mathbb{D}_G \setminus \{0, 1\}$, the lines through $[\boldsymbol{\alpha}, \beta, 1]$ define a transversal of the Latin square. \square

Corollary 16. *Suppose that $(V, \mathcal{P}, \mathcal{B})$ is a $\text{TD}(3, n)$ that lies on three hyperplanes of $P^d(\mathbb{D})$ that intersect in a $(d - 3)$ -flat. If $(V, \mathcal{P}, \mathcal{B})$ is also embeddable in three hyperplanes of $P^d(\mathbb{D})$ that intersect in a $(d - 2)$ -flat, then the embedding of V is not proper.*

Proof. By Corollary 12, if the $\text{TD}(3, n)$ is embeddable in three hyperplanes that intersect in a $(d - 2)$ -flat, then \mathbb{D} has prime characteristic p , and $n = p^k$ for some $k \geq 1$ and G is a p -group. If it furthermore lies on three hyperplanes that intersect in a $(d - 3)$ -flat, then consider the subgroup G of $\mathbb{D}^* \times \mathbb{D}^{d-2}$ given by Proposition 13. Define G_1 as in the proof of Proposition 14. As before, G_1 is trivial. As in the proof of Proposition 14 it follows that V (as well as the transversal point) is contained in the hyperplane $x_1 + x_2 - x_3 = 0$. \square

The next theorem is a generalisation of Bruen and Colbourn's Theorem 5.1 [2]. (Note that in their Theorem 5.1 it should be assumed that the embeddings are proper, as is already clear from Proposition 14.)

Theorem 17. Let $(V, \mathcal{P}, \mathcal{B})$ be a $\text{TD}(k, n)$, $n \geq 3$, $k \geq 4$ with a proper embedding into $P^d(\mathbb{D})$ on hyperplanes H_1, H_2, \dots, H_k . Then $\dim(H_1 \cap H_2 \cap \dots \cap H_k) = d - 2$, coordinates can be chosen such that H_1, H_2, H_3 are as in Proposition 11, and there exist distinct $a_4, \dots, a_k \in \mathbb{D}_G \setminus \{0, 1\}$ such that

$$H_i \cap V = \{[\boldsymbol{\gamma}, a_i, 1] \mid \boldsymbol{\gamma} \in G\}, \quad i = 4, \dots, k,$$

where G is a subgroup of $(\mathbb{D}^{d-1}, +)$ of order n . Furthermore, n is a prime power p^m , G is isomorphic to \mathbb{Z}_p^m , $|\mathbb{D}_G| = p^t$ for some $t \leq m$, and $k \leq |\mathbb{D}_G| + 1$.

In particular, if a Latin square with transversal can be properly embedded into $P^d(\mathbb{D})$, then the Latin square can be extended to a $\text{TD}(|\mathbb{D}_G| + 1, n)$ with an embedding that extends the original embedding.

Proof. We claim that each $H_i \cap V$ spans H_i . Suppose to the contrary that $H_1 \cap V$, say, spans a $(d-2)$ -flat F . Choose an arbitrary point $\infty \in V \setminus H_1$. Without loss of generality, $\infty \in H_k$. Then, since ∞ is a transversal point of the $\text{TD}(k-1, n)$ lying on H_1, \dots, H_{k-1} , it follows that $V \cap (H_1 \cup \dots \cup H_{k-1})$ lies on the hyperplane spanned by F and ∞ . Similarly, $V \cap (H_1 \cup H_3 \cup H_4 \cup \dots \cup H_k)$ lies on the same hyperplane. It follows that the whole of V lies on a hyperplane, contrary to assumption.

By Theorem 15, by taking any transversal point in V not lying on three hyperplanes H_i , the intersection of any three hyperplanes is $(d-2)$ -dimensional. It follows that $\dim(H_1 \cap \dots \cap H_k) = d - 2$.

We may now choose coordinates such that H_1, H_2, H_3 are as in Proposition 11. By Theorem 15, each point in $V \setminus (H_1 \cup H_2 \cup H_3)$ has coordinates $[\boldsymbol{\gamma}, a, 1]$ with $\boldsymbol{\gamma} \in G$ and $a \in \mathbb{D}_G \setminus \{0, 1\}$. It remains to show for each $i = 4, \dots, k$, that if $[\boldsymbol{\gamma}, a, 1], [\boldsymbol{\gamma}', a', 1] \in V \cap H_i$, then $a = a'$. Since the $(d-2)$ -flat $F = H_1 \cap H_2 \cap H_3 \cap H_4$ also lies on the hyperplanes $x_d = ax_{d+1}$ and $x_d = a'x_{d+1}$, H_4 is spanned by F and a and also by F and a' . This implies $a = a'$. \square

Acknowledgments

We thank the referees for their suggestions leading to an improved paper.

References

- [1] S.A. Amitsur, Finite subgroups of division rings, *Trans. Amer. Math. Soc.* 80 (1955) 361–386.
- [2] A.A. Bruen, C.J. Colbourn, Transversal designs in classical planes and spaces, *J. Combin. Theory Ser. A* 92 (2000) 88–94.
- [3] C.J. Colbourn, J.H. Dinitz (Eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996.
- [4] H.S.M. Coxeter, The binary polyhedral groups, and other generalizations of the quaternion group, *Duke Math. J.* 7 (1940) 367–379.
- [5] I.N. Herstein, Finite multiplicative subgroups in division rings, *Pacific J. Math.* 1 (1953) 121–126.
- [6] L.M. Kelly, S. Nwankpa, Affine embeddings of Sylvester–Gallai designs, *J. Combin. Theory Ser. A* 14 (1973) 422–438.
- [7] T.Y. Lam, Finite groups embeddable in division rings, *Proc. Amer. Math. Soc.* 129 (2001) 3161–3166.
- [8] Th. Motzkin, The lines and planes connecting the points of a finite set, *Trans. Amer. Math. Soc.* 70 (1951) 451–464.
- [9] L.M. Pretorius, K.J. Swanepoel, The Sylvester–Gallai theorem, colourings and algebra, *Discrete Math.* 309 (2009) 385–399, arXiv:math/0606131v1.
- [10] J.J. Rotman, *An Introduction to the Theory of Groups*, fourth ed., Springer-Verlag, New York, 1995.
- [11] W. Szmielew, *From Affine to Euclidean Geometry. An Axiomatic Approach*, D. Reidel, Dordrecht, 1983.