

Translation Planes from
Dembowski Ostrom
Polynomials

U. Dempwolff, P. Müller

1. POLYNOMIALS. Let $F = \text{GF}(p^n)$ be a finite field, $P(X) \in F[X]$. Then $P : F \rightarrow F, x \mapsto P(x)$ is the **associated polynomial map**.

Definition.

(a) $P(X)$ is **$\text{GF}(p^m)$ -linear**, $m|n$, if the polynomial map P is a $\text{GF}(p^m)$ -endomorphism of F . In this case ($q = p^m, r = n/m$)

$$P(X) = \sum_{i=0}^{r-1} a_i X^{q^i}.$$

(b) $P(X)$ is a **DO polynomial** (DO = Dembowski Ostrom) if

$$P(X) = \sum_{i,j=0}^{n-1} a_{ij} X^{p^i + p^j}.$$

2. AFFINE PLANES.

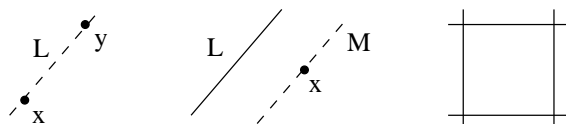
Definition. A $2 - (n^2, n, 1)$ design is an **affine plane of order n** .

AXIOMATIC DESCRIPTION: We call $A = (\mathbf{P}, \mathbf{L})$, $\mathbf{L} \subseteq 2^{\mathbf{P}}$, an **affine plane of order n** if $|\mathbf{P}| = n^2$ and:

(a) For two $x, y \in \mathbf{P}$ there exists precisely one $L \in \mathbf{L}$ with $x, y \in L$.

(b) (Parallel axiom) For $x \in \mathbf{P}$, $L \in \mathbf{L}$, $x \notin L$ there exists precisely one $M \in \mathbf{L}$ with $x \in M$ and $L \cap M = \emptyset$.

(c) A contains a quadrangle.



3. TRANSLATION PLANES.

Let q be a prime power, $F = GF(q)$, and W a $2n$ -dimensional F -space. A **spread** \mathcal{S} on W is a set of n -dimensional subspaces such that:

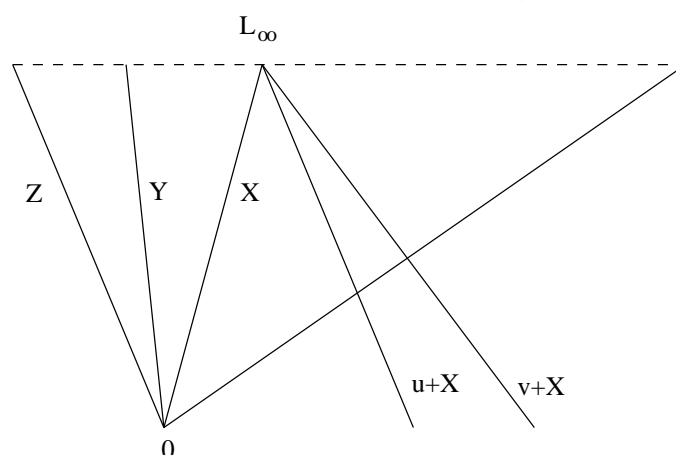
$$(1) W = \bigcup_{X \in \mathcal{S}} X, \quad (2) X \cap Y = \emptyset, \quad X, Y \in \mathcal{S}, \quad X \neq Y$$

Theorem. *Let \mathcal{S} be a spread on W . Set*

$$\mathbf{L} = \{X + w \mid X \in \mathcal{S}, w \in W\}.$$

Then $\mathbf{A} = \mathbf{A}(W, \mathcal{S}) = (W, \mathbf{L})$ is an affine plane.

Such a plane is called a **translation plane**.



Collineations:

For $u \in W$ the mapping

$$\tau_u : x \mapsto x + u, \quad X + w \mapsto X + (w + u)$$

defines a collineation, $\tau(W) \simeq W$ is the *translation group*. The group

$$G = \{T \in \Gamma L(W) \mid \mathcal{S}T = \mathcal{S}\}$$

is called the *translation complement* of \mathbf{A} . The full automorphism group of \mathbf{A} is the semidirect product of $\tau(W)$ with G . In particular the automorphism group is determined completely by the translation complement.

Example. $\dim W = 2$, $\mathcal{S} = 1$ -dimensional subspaces is a spread. The resulting plane is called **desarguesian**. The collineation group is:

$$\text{Aut}(\mathbf{A}(W, \mathcal{S})) \simeq \tau(W) \cdot \Gamma\text{L}(2, q)$$

We are interested in NONDESARGUESIAN planes.

4. COORDINATIZATION OF PLANES

Let V be a n -dimensional F -space, $F = \text{GF}(q)$. Furthermore let $0 \in \mathbf{S} \subseteq \text{GL}(V) \cup 0$ be a *spread set*, i.e.

$$\det(t - s) \neq 0, \quad t, s \in \mathbf{S}, \quad s \neq t \quad \text{and} \quad |\mathbf{S}| = q^n.$$

Set $W = V \times V$ and define

$$V(\infty) = 0 \times V, \quad V(t) = \{(x, xt) \mid x \in V\}$$

and $\mathcal{S} = \{V(\infty)\} \cup \{V(t) \mid t \in \mathbf{S}\}$. Then \mathcal{S} is a spread on W .

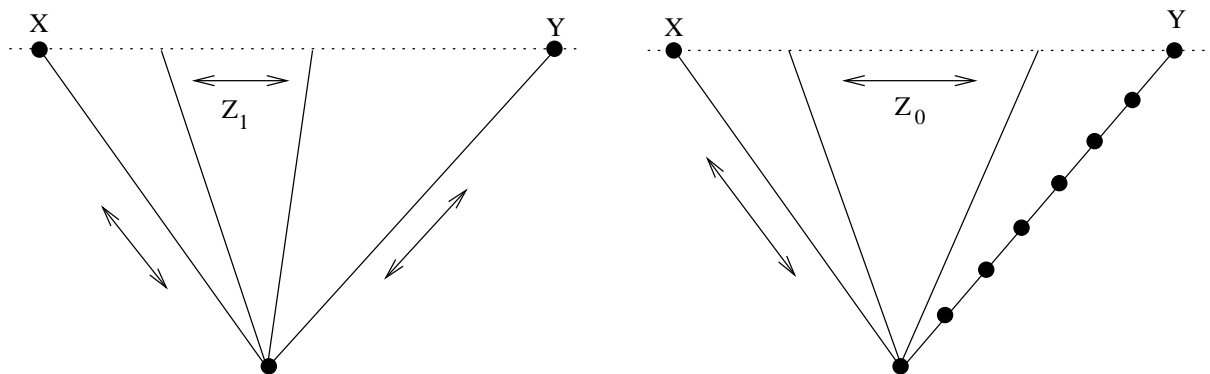
Vice versa starting with a spread we can coordinatize it by a spread set.

5. MOTIVATION: KANTOR-WILLIAMS

Kantor-Williams (2010) construct translation planes of order q^n (q even, n odd) such that:

(KW1) The translation complement contains a group $Z_1 \simeq C_{q^n-1}$ which acts fixed point freely on W and which fixes precisely two fibers of S , say X and Y . The representation of Z_1 on X is contragredient to the representation of Z_1 on Y .

(KW2) The plane admits a homology group $Z_0 \simeq K^*$, $K = GF(q)$, with coaxis X and axis Y .



POLYNOMIALS COME INTO PLAY

Assume now q, n odd and let $\mathbf{A} = \mathbf{A}(W, \mathcal{S})$ be a translation plane of order q^n satisfying (KW1-2).

Coordinatize!

Identify:

$$V = F = \text{GF}(q^n).$$

Fixed fibers $X = V(\infty), X = V(\infty)$

$V(t)$ third fiber such that

$$xt = L(x), \quad L(X) \in F[X] \text{ linear}$$

Leads to:

THEME OF THIS TALK

Theorem. *Let L be the linear polynomial obtained by the coordinatization. Let $\zeta \in \text{GF}(q)$ be a non-square.*

(1) $L : F \rightarrow F$ is bijective.

(2) $|P(F^*)| = \frac{q^n - 1}{2}$, $P(X) = L(X)X$ (DO polynomial).

(3) $P(F^*) \cap \zeta P(F^*) = \emptyset$.

ASSOCIATED SPREAD SET

Let

$$L(X) = \sum_{i=0}^{n-1} a_i X^{q^i}$$

be a polynomial satisfying (1)-(3). For $z \in F^*$ define an invertible, linear polynomial $L_z(X)$ by

$$L_z(X) = \sum_{i=0}^{n-1} a_i z^{1+q^i} X^{q^i}.$$

The spread set defined by (1)-(3) has the form

$$\mathbf{S} = \{L_z, \zeta L_z \mid z \in F\}.$$

Note $L_z = L_y \Leftrightarrow z = \pm y$.

AIM:

Find linear polynomials $L(X) \in F[X]$ satisfying (1)-(3) (of the theorem) such that the DO polynomial $L(X)X$ defines

NONDESARGUESIAN translation plane.

6. EXAMPLES.

Let $F = \text{GF}(q^n)$ and $K = \text{GF}(q)$, q, n odd.

(a) DO polynomials of the form $L(X)X$ with

$$L(X) = aX^{q^m}$$

define always desarguesian planes.

(b) Let $0 < r < n$, $a \in F^*$, such that

$$a^{(q^n-1)/(q^{(n,r)}-1)} \neq 1.$$

Define

$$L(X) = A_{a,r}(X) = X^{q^r} - aX^{q^{-r}}.$$

Then the DO polynomial $A_{a,r}(X)X$ defines non-desarguesian plane, so called **twisted field** plane.

Example. (D. - P. Müller, 2011) $K = \text{GF}(q)$, $3 < q$ odd, $F = \text{GF}(q^n)$, n odd, $0 < r < n$, and $b \in F^*$ such that

$$b^{(q^n-1)/(q^{(n,r)}-1)} \neq \pm 1.$$

Lemma. Set

$$B_{b,r}(X) = 2A^{-1}(X) - X,$$

where

$$A(X) = X - bX^{q^r}.$$

Then the polynomial $B_{b,r}(X)$ satisfies (1)-(3).

Proof. One may assume $(n, r) = 1$. Set $no(x) = x^{(q^n-1)/(q-1)}$. Condition (1) is easy.

Define permutation polynomials $C(X) = X - b^2X^{q^r}$ and $B(X) = B_{b,r}(X)$. Since $P(X) = 2A^{-1}(X)X - X^2$ we have for $x \in F$:

$$\begin{aligned} P(A(x)) &= 2A^{-1}(A(x))A(x) - A(x)^2 \\ &= A(x)(2x - A(x)) \\ &= (x - bx^{q^r})(2x - x + bx^{q^r}) \\ &= x^2 - b^2(x^2)^{q^r} = C(x^2) \end{aligned}$$

Then (2) holds.

Assume (3) is false. Then there exist $u, v \in F$, $u \neq v$, such that $\zeta P(u) = P(v)$. Write $u = A(x)$ and $v = A(y)$. Then

$$\zeta(x^2 - b^2(x^2)^{q^r}) = \zeta C(x^2) = C(y^2) = y^2 - b^2(y^2)^{q^r}.$$

Then $\zeta x^2 - y^2 = b^2(\zeta x^2 - y^2)^{q^r}$ and

$$b^2 = (\zeta x^2 - y^2)^{1-q^r}.$$

Therefore $no(b^2) = 1 \Rightarrow no(b) = \pm 1$, a contradiction. \square

7. VARIATION: TWO POLYNOMIALS

Let $q, n, F = \text{GF}(q^n), \zeta$ etc. have the same meaning as before. Let $L(X), L'(X) \in F[X]$ satisfy (1)-(3). Define DO polynomials $P_L(X) = L(X)X$ and $P_{L'}(X) = L'(X)X$. Assume

$$(4) P_L(F) = P_{L'}(F).$$

Define as before linear operators L_z and L'_z , i.e.

$$xL_z = \sum_{i=0}^{n-1} a_i z^{1+q^i} x^{q^i}, \quad \text{for} \quad L(X) = \sum_{i=0}^{n-1} a_i X^{q^i}$$

(and similar for L'_z).

Proposition. *The set*

$$\mathbf{S} = \{L_z, \zeta L'_z \mid z \in F\}$$

is a spread set.

Remark. The associated plane still admits a cyclic collineation group Z_1 satisfying (KW1).

Question: Are there pairs satisfying (1)-(4)?

Theorem. *Let $L(X) \in F[X]$ satisfy (1)-(3). Let $L^{-1}(X) \in F[X]$ be the polynomial of degree $< |F|$ which induces the map L^{-1} . Then the pair $L(X), L^{-1}(X)$ satisfies (1)-(4).*

Proof. Let $y = L(x)x$, $x \neq 0$. Set $z = L^{-1}(x)$. Then $y = zL^{-1}(z)$. \square

Theorem. *Let $b \in F^*$. Assume $a = b^2$ and $b^{(q^n-1)/(q^{(n,r)}-1)} \neq \pm 1$. Then*

$$P_{A_{a,r}}(F) = P_{B_{b,-r}}(F).$$

8. EXAMPLES.

(a) (Suetake, 1992) Choose $L(X) = A_{a,r}(X)$ and $L'(X) = L^{-1}(X)$. These planes were found by Suetake by different means (not polynomials).

(b) (D. 2011) Choose $L(X) = B_{b,r}(X)$ and $L'(X) = L^{-1}(X)$.

(c) (D. 2011) Choose $L(X) = B_{b,-r}(X)$ and $L'(X) = P_{A_{a,r}}(X)$.

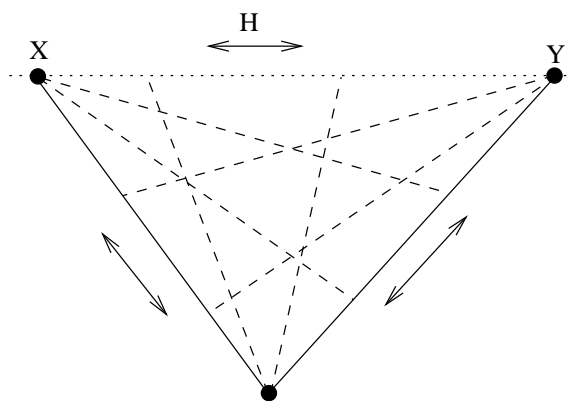
All other variations only produce planes which appear under (a)-(c).

FINAL REMARKS.

1. One can compute the automorphism group of our translation planes and count the number of non-isomorphic planes as a function of the parameters q and n . Main group theoretic tool: the subgroups of $GL(W)$ containing the cyclic groups $Z_1 \simeq C_{q^n-1}$ can be determined by results of Hering, Liebrck and others (needs the classification of finite simple groups).

2. Pairs of polynomials satisfying (1)-(4) produce *also semifield planes* of order q^{2n} (not q^n).

3. Let $\mathbf{A} = \mathbf{A}(W, \mathcal{S})$ be a translation plane and H a subgroup of the translation complement which fixes two affine lines X, Y ($\subseteq \mathcal{S}$) and which acts transitively on the non-vertex points of the triangle X, Y, L_∞ . Then \mathbf{A} is called *triangle transitive* (Jha-Johnson) or *nearly flag transitive* (Kantor-Williams).



Known examples:

- . **nearfield** planes
- . some **twisted field** planes
- . some **André** planes
- . planes of **Suetake**
- . planes of **Kantor-Williams**
- . planes of **D.-Müller** discussed here and planes of even order from **D.-Müller** (2011) connected with permutation polynomials
- . planes of **D.** discussed under example (b) in the last section