

Permutation Polynomials and Translation Planes

U. Dempwolff, P. Müller

1. POLYNOMIALS. Let F 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 a **permutation polynomial** if P is bijective.

(b) $P(X)$ is **additive** if $P(x + y) = P(x) + P(y), x, y \in F$.

Remark. Let $F = \text{GF}(p^n)$ then (if $\deg L < p^n - 1$)

$$L(X) \text{ additive} \quad \Leftrightarrow \quad L(X) = \sum_{i=0}^{n-1} a_i X^{p^i}$$

THEME OF THIS TALK

Permutation polynomials of the form:

$$L(X)X^k, L(X) \text{ additive}$$

Lemma. *Let $L(X)X^k$ be a permutation polynomial. Then $L(X)$ is a permutation polynomial too.*

Proof. Assume $L(x) = 0$. Then

$$L(x)x^k = 0 = L(0)0^k \quad \Rightarrow \quad x = 0$$

□

2. QUASIFIELDS.

Definition. Let $(F, +)$ be an abelian group and $* : F \times F \rightarrow F$ a binary composition. The triple $(F, +, *)$ is a **weak quasifield** if $(x, y, z \in F)$:

(a) $x * 0 = 0 * x = 0$.

(b) $(x + y) * z = x * z + y * z$.

(c) For $0 \neq a \in F$ the mappings $x \mapsto x * a$ and $x \mapsto a * x$ are bijective.

Remarks. (a) One calls F a **quasifield** if the multiplication $*$ has a neutral element. For this talk: "quasifield = weak quasifield".

(b) Let F be finite. Then F is an elementary abelian p -group. We can assume that $F = (\text{GF}(p^n), +)$.

Theorem. Let $L(X)X^k$, $L(X)$ additive, be a permutation polynomial on the finite field F . Define $*$: $F \times F \rightarrow F$ by $x * y = L(xy)y^k$. Then $(F, +, *)$ is a quasifield.

What is special about quasifields defined by $L(X)X^k$? Answer:

$$(c^{-1}x) * (cy) = c^k(x * y), \quad 0 \neq c \in F.$$

Moreover:

Theorem. A quasifield with the above property is defined by a permutation polynomial of the form $L(X)X^k$.

Set $W = F \times F$ ($2n$ -dimensional $\text{GF}(p)$ -space) and define

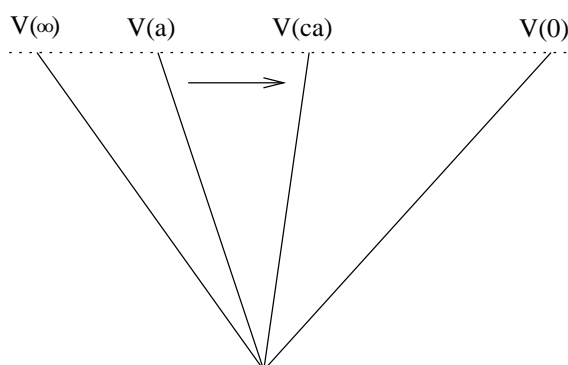
$$V(\infty) = 0 \times F, \quad V(a) = \{(x, a * x) \mid x \in F\}$$

and a spread $\mathcal{S} = \{V(\infty)\} \cup \{V(a) \mid a \in F\}$.

The property

$$(c^{-1}x) * (cy) = c^k(x * y), \quad c \in F$$

implies that the translation plane defined the polynomial $L(X)X^k$ admits a collineation group $\simeq F^*$ which fixes $V(\infty)$ and $V(0)$ and permutes the fibers of $\mathcal{S} - \{V(\infty), V(0)\}$ transitively.



AIM:

Find $L(X)X^k$ which defines a NONDESARGUESIAN plane.

For instance additive polynomials $L(X)$ ($k = 0$) define only desarguesian planes.

3. EXAMPLES.

Let $F = \text{GF}(p^n)$. Permutation polynomials of the form $L(X)X^k$ with

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

define always desarguesian planes but there are examples

$$L(X) = aX^{p^\ell} + bX^{p^{n-\ell}}$$

which define nondesarguesian planes, so called **twisted field** planes.

Theorem. *Let $L(X)X^k$ be a permutation polynomial on $\text{GF}(p^n)$, $(k, q^n - 1) = 1$. Assume that $L(X)$ and $L^{-1}(X)$ have at least three terms. Then $L(X)X^k$ defines a plane which is not a semifield plane, in particular a nondesarguesian plane.*

Example. (Kantor-Williams, 2010, simple version) $F_0 = \text{GF}(q)$, $2 < q$ even, $F_1 = \text{GF}(q^n)$, n odd and $T : F_1 \rightarrow F_0$ trace map. Let $0, 1 \neq c \in F_0$.

Lemma. Set $L(X) = (1 + c)X + cT(X)$. Then $L(X)X$ is a permutation polynomial.

Proof. Exercise! Hint: Apply T to

$$(1 + c)x^2 + cT(x)x = (1 + c)y^2 + cT(y)y$$

□

Example. (Kantor-Williams, 2010, general version) $F_0 = \text{GF}(q)$, $2 < q$ even, $d_1 | d_2 | \cdots | d_s$, d_s odd. Set $F_i = \text{GF}(q^{d_i})$ and for $j > i$ let $T_{j:i} : F_j \rightarrow F_i$ be the trace map. Let $0, 1 \neq c_i \in F_i$, $0 \leq i < s$, s. t. $\sum_{i=0}^k c_i \neq 0$ all k .

Lemma. Set

$$L(X) = \left(1 + \sum_{i=0}^{s-1} c_i\right)X + \sum_{i=0}^{s-1} c_i T_{s:i}(X).$$

Then $L(X)X$ is a permutation polynomial.

Proof. Apply $T_{s:s-1}$ to $L(x)x = L(y)y$. Now telescoping and induction. \square

The Kantor-Williams spreads are **symplectic** but the following twisted polynomials produce **non-symplectic** spreads.

Example. (D.-M., 2011, "twisted" Kantor-Williams) Define the d_i 's, the F_i 's ($=\text{GF}(q^{d_i})$), and the c_i 's as before. Pick $0 \neq c \in F_0$ and choose $1 \leq \ell < d_0$ such that

$$(2^\ell + 1, 2^{d_0} - 1) = 1.$$

Lemma. *Set*

$$L(X) = \left(\sum_{i=0}^{s-1} c_i \right) X + \sum_{i=0}^{s-1} c_i T_{s:i}(X) + c T_{s:0}(X)^{2^\ell}$$

Then $L(X)X$ is a permutation polynomial.

Example. (D.-M., 2011). More difficult to prove is:

Lemma. Let $F = \text{GF}(2^n)$, n odd, and let $1 < m < n$ be odd such that $(m, n) = 1$. Set

$$L(X) = \sum_{i=0}^{m-1} X^{2^i}, \quad k = 2^{n-1} - 2^{m-1} - 1.$$

Pick $1 \leq \ell < 2^n$, ℓ odd, such that $k\ell \equiv 1 \pmod{2^{m-1}}$. Then

$$L(X)X^k$$

and

$$L(X)X^\ell$$

are permutation polynomials.

Both polynomials are related to **exceptional polynomials**, i.e. polynomials which are permutation polynomials in infinitely many finite fields.

The polynomials

$$L(X)X^k$$

are related to the class of **Dickson polynomials**. One can show: "Equivalence transformations" produce polynomials satisfying the relation

$$f(Z + Z^{-1}) = Z^{2m-1} + Z^{-2m+1}.$$

Well known defining property for Dickson polynomials.

The polynomials

$$L(X)X^\ell$$

are equivalent to polynomials

$$f(X) = \frac{L(X)^{2^m+1}}{X^{2^m}},$$

exceptional polynomials of **Cohen-Matthews** 1995.

The proof of the permutation property for Dickson polynomials, i.e. $L(X)X^k$, is not too hard.

The verification for the polynomials of Cohen-Matthews, i.e. of $L(X)X^\ell$, used the classification of finite simple groups! (But **Dillon-Dobbertin** 2004, discrete Four. transf.).

Observation: the spread induced by $L(X)X^k$ on W is isomorphic to the spread induced by $L(X)X^\ell$ on the dual space W^* .

This leads to a simple proof of the permutation property for the Cohen-Matthews polynomials.

FINAL REMARKS.

1. For $F = \text{GF}(2^n)$, n a **prime**, computer computations indicate that the examples should belong to the last class (pols. related to Dickson or Cohen-Matthews).
2. What about odd orders? There are examples too (D.-M., 2011). But they are better to describe by polynomials of the form $L(X)X$ which are not perm. pols. but **planar**.
3. Applications of exceptional polynomials in discrete mathematics: difference sets, APN-functions, bent functions, double error correcting codes ... See Guralnik, Rosenberg, Zieve Ann. Math. (2) 172(2010),1361-1390 for classifications of exceptional polynomials and their applications.
4. One can compute the automorphism group of our translation planes.

5. One knows $\text{Aut}(W, \mathcal{S}) = W \cdot G$

$$G = \{T \in \text{GL}(W) \mid \mathcal{S}T = \mathcal{S}\}.$$

Let $H \leq G$ such that H fixes two affine lines X, Y ($\subseteq \mathcal{S}$) such that H acts transitively on the non-vertex points of the triangle X, Y, L_∞ . Then (W, \mathcal{S}) 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-M**