Projective polynomials and some of their applications

Lukas Kölsch

University of South Florida

June 9th, 2026

(joined work with Faruk Göloğlu)

Projective polynomials

Let F be a field of characteristic $p > 0$.

Definition (Projective polynomial)

A *projective polynomial* is a polynomial of the form

$$P(x) = x^{[d]} + c_{d-1}x^{[d-1]} + \cdots + c_1 x^{[1]} + c_0 \in F[x],$$

where $[i] = (q^i - 1)/(q - 1)$ for some $q = p^k$. We say P has q-degree d.

Example

$P(x) = x^{q+1} + ax + b \in \mathbb{F}_{p^m}[x]$ where $q = p^k$ is a projective polynomial of q-degree 2.

Some more examples

Example

$$P(x) = x^{q^{k-1}+q^{k-2}+\cdots+1} + ax + b \in K(t)[x],$$

where K is a field of characteristic $p > 0$.

The name "projective polynomial" was coined by Abhyankar in 1997 who studied exactly the Galois groups of such polynomials over function fields.

This talk: F is a finite field.

Why do we care about projective polynomials?

Projective polynomials occur naturally in many different contexts:

Study of linearized polynomials (Ore 1933)

THEOREM 3. *The necessary and sufficient condition that the linear p-polynomial $x^p - \alpha x$ be a symbolic divisor of $F_p(x)$ is that α be a root of*

$$a_0 y^{(p^m-1)/(p-1)} + a_1 y^{(p^{m-1}-1)/(p-1)} + \cdots + a_{m-2} y^{p+1} + a_{m-1} y + a_m = 0, \tag{10}$$

i.e., α is equal to the $(p-1)$st power of a root of the equation $F_p(x) = 0$.

Why do we care about projective polynomials?

Construction of semifields (Knuth 1965)

7.4 THE FOUR TYPES. We obtain many proper semifields, which are quadratic over a weak nucleus, by the construction in the previous section. Those of Case I have the multiplication rule

$$(a + \lambda b)(c + \lambda d) = (ac + b^\alpha d^\beta f) + \lambda(a^\sigma d + bc) \tag{7.16}$$

where p is odd and f is a nonsquare; α, β, and σ are arbitrary automorphisms, but not all the identity. Dickson's construction (see Section 6.3) is a special case, indeed the only commutative semifield of this type.

Other semifields, those of Case II, are constructed by finding an automorphism $\sigma \neq I$ and elements $f, g \in F$ such that

$$y^{\sigma+1} + gy - f \neq 0, \qquad \text{for} \qquad y \in F.$$

Why do we care about projective polynomials?

Computing discrete logarithms in finite fields (Göloglu, Granger, McGuire, Zumbrägel 2013)

4.1 On-the-fly degree two elimination

In this subsection we review the on-the-fly degree two elimination method from [20], adjusted for the present framework. In [6] the affine portion of the set of polynomials obtained as linear fractional transformations of $X^q - X$ is parameterised as follows. Let $\mathcal{B}$ be the set of $B \in \mathbb{F}_{q^k}$ such that the polynomial $X^{q+1} - BX + B$ splits completely over $\mathbb{F}_{q^k}$, the cardinality of which is approximately q^{k-3} [6, Lemma 4.4]. Scaling and translating these polynomials means that all the polynomials $X^{q+1} + aX^q + bX + c$ with $c \neq ab$, $b \neq a^q$ and $B = \frac{(b-a^q)^{q+1}}{(c-ab)^q}$ split completely over $\mathbb{F}_{q^k}$ whenever $B \in \mathcal{B}$.

Why do we care about projective polynomials?

Constructions of highly nonlinear functions (Taniguchi, 2019)

Theorem 3 *Let m, n be positive integers with $n \geq 2$ and $GCD(m, n) = 1$. Let $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}^{\times}$. Let us define*

$$G(x, y) = x^{2^{2m}+2^{3m}} + ax^{2^{2m}}y^{2^m} + by^{2^m+1}. \tag{2}$$

Then $F(x, y) := (xy, G(x, y))$ is an APN function if and only if the polynomial $P(x) := x^{2^m+1} + ax + b$ has no root in $\mathbb{F}_{2^n}$.

In this talk we will mainly focus on the construction of highly nonlinear functions and semifields.

Projective polynomials and linearized polynomials

Let

$$P(x) = x^{[d]} + c_{d-1}x^{[d-1]} + \cdots + c_1x^{[1]} + c_0 \in \mathbb{F}_{p^m}[x]$$

where $[i] = (q^i - 1)/(q - 1)$ for $q = p^k$.

Then

$$L_P(x) := xP(x^{q-1}) = x^{q^d} + c_{d-1}x^{q^{d-1}} + \cdots + c_1x^q + c_0x \in \mathbb{F}_{p^m}[x]$$

is a linearized polynomial.

Number of roots of projective polynomials

The connection to linearized polynomials leads to strong restrictions on the number of roots.

Theorem (von zur Gathen, Giesbrecht, Ziegler, 2010)

Let $\mathbb{F}_{p^d}$ be the fixed field of $x \mapsto x^q$ in $\mathbb{F}_{p^m}$. The number of roots of a projective polynomial of q-degree d over $\mathbb{F}_{p^m}$ is then

$$\sum_i \frac{p^{dn_i} - 1}{p^d - 1}$$

where n_i are non-negative integers summing up to at most d.

Example

Let P be a projective polynomial of q-degree 2. Then the number or roots is $\{0, 1, 2, p^d + 1\}$.

Number of roots of projective polynomials

For projective polynomials $P(x) = x^{q+1} + ax + b \in \mathbb{F}_{p^m}[x]$, precise counts on how many of them have $0, 1, 2, p^d + 1$ roots were determined by Bluher.

More general results for higher q-degrees were found by McGuire and Sheekey.

Twisted polynomials and projective polynomials

Twisted polynomial ring over a finite field: $\mathbb{F}_{p^m}[t;\sigma]$.

$\sigma\colon x \mapsto x^q$ is a field automorphism of $\mathbb{F}_{p^m}$.

Twisted polynomials and projective polynomials

Twisted polynomial ring over a finite field: $\mathbb{F}_{p^m}[t;\sigma]$.

$\sigma\colon x \mapsto x^q$ is a field automorphism of $\mathbb{F}_{p^m}$.

The elements of $\mathbb{F}_{p^m}[t;\sigma]$ are polynomials in t with:

- regular polynomial addition
- multiplication follows the rule $ta = a^q t$ for all $a \in \mathbb{F}_{p^m}$.

Twisted polynomials and projective polynomials

Twisted polynomial ring over a finite field: $\mathbb{F}_{p^m}[t;\sigma]$.

$\sigma\colon x \mapsto x^q$ is a field automorphism of $\mathbb{F}_{p^m}$.

The elements of $\mathbb{F}_{p^m}[t;\sigma]$ are polynomials in t with:

- regular polynomial addition
- multiplication follows the rule $ta = a^q t$ for all $a \in \mathbb{F}_{p^m}$.

Example

For instance:

$$\begin{aligned}(t^2+at+b)(t+c) &= t^3 + t^2c + at^2 + atc + bt + bc\\ &= t^3 + c^{q^2}t^2 + at^2 + ac^q t + bt + bc\\ &= t^3 + (c^{q^2}+a)t^2 + (ac^q+b)t + bc.\end{aligned}$$

Twisted polynomials and projective polynomials

Twisted polynomial rings were defined by Ore in 1933.

Theorem (Ore, 1933)

The projective polynomial $P(x) = x^{[k]} + c_{k-1}x^{[k-1]} + \cdots + c_1 x^{[1]} + c_0 \in \mathbb{F}_{p^m}[x]$ has no roots if and only if $p(t) = t^k + c_{k-1}t^{k-1} + \cdots + c_1 t + c_0 \in \mathbb{F}_{p^m}[t;\sigma]$ has no linear right divisor.

Twisted polynomials and projective polynomials

Twisted polynomial rings were defined by Ore in 1933.

Theorem (Ore, 1933)

The projective polynomial $P(x) = x^{[k]} + c_{k-1}x^{[k-1]} + \cdots + c_1 x^{[1]} + c_0 \in \mathbb{F}_{p^m}[x]$ *has no roots if and only if* $p(t) = t^k + c_{k-1}t^{k-1} + \cdots + c_1 t + c_0 \in \mathbb{F}_{p^m}[t;\sigma]$ *has no linear right divisor.*

Key: q-degree k in P becomes degree k in p.

Twisted polynomials and projective polynomials

Twisted polynomial rings were defined by Ore in 1933.

Theorem (Ore, 1933)

The projective polynomial $P(x) = x^{[k]} + c_{k-1}x^{[k-1]} + \cdots + c_1 x^{[1]} + c_0 \in \mathbb{F}_{p^m}[x]$ *has no roots if and only if* $p(t) = t^k + c_{k-1}t^{k-1} + \cdots + c_1 t + c_0 \in \mathbb{F}_{p^m}[t;\sigma]$ *has no linear right divisor.*

Key: q-degree k in P becomes degree k in p.

Note: Since twisted polynomial rings are not commutative anymore, we have to differentiate carefully between left and right division.

Twisted polynomials and projective polynomials

Twisted polynomial rings were defined by Ore in 1933.

Theorem (Ore, 1933)

The projective polynomial $P(x) = x^{[k]} + c_{k-1}x^{[k-1]} + \cdots + c_1 x^{[1]} + c_0 \in \mathbb{F}_{p^m}[x]$ has no roots if and only if $p(t) = t^k + c_{k-1}t^{k-1} + \cdots + c_1 t + c_0 \in \mathbb{F}_{p^m}[t;\sigma]$ has no linear right divisor.

Key: q-degree k in P becomes degree k in p.

Note: Since twisted polynomial rings are not commutative anymore, we have to differentiate carefully between left and right division.

The existence of irreducible twisted polynomials then implies the existence of projective polynomials without roots.

The big question

Question

How can we use projective polynomials to construct interesting objects?

Remember:

1. Projective polynomials of q-degree d correspond to degree d twisted polynomials. Idea: Use this to "twist" standard constructions relying on regular polynomials.
2. Existence of projective polynomials of any q-degree without any roots is guaranteed.

Semifields

Definition

A (finite) semifield $\mathbb{S} = (S, +, \circ)$ is a finite set S equipped with two operations $(+, \circ)$ satisfying the following axioms.

(S1) $(S, +)$ is a group.

(S2) For all $x, y, z \in S$,

- $x \circ (y + z) = x \circ y + x \circ z$,
- $(x + y) \circ z = x \circ z + y \circ z$.

(S3) For all $x, y \in S$, $x \circ y = 0$ implies $x = 0$ or $y = 0$.

(S4) There exists $\epsilon \in S$ such that $x \circ \epsilon = x = \epsilon \circ x$.

Basic properties

If $\circ$ is associative then $\mathbb{S}$ is a finite field (Wedderburn's Theorem).

The additive group of a semifield $(\mathbb{S}, +, \circ)$ is always an elementary abelian p-group.

We can thus identify the additive group of a semifield $\mathbb{S}$ with $(\mathbb{F}_p^n, +)$.

Connections

Every semifield can be used to construct translation planes.

There is a 1-to-1 relation between semifields and rank-metric codes with certain optimal parameters.

Even constructions of optimal rank-metric codes with other parameters are often based on semifield constructions.

A simple semifield construction via twisted polynomials

Recall the classical construction of a finite field:

$$\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(f),$$

where f is an irreducible polynomial of degree n. We can follow the same idea with twisted polynomials.

Semifields via twisted polynomials

Theorem (Petit, 1966)

Let $f \in \mathbb{F}_{p^m}[t;\sigma]$ be an irreducible twisted polynomial of degree d. Then

$$S_f := \mathbb{F}_{p^m}[t;\sigma]/(f)$$

is a semifield of size p^{md}. It is associative if and only if σ is trivial.

Again, we have to pay attention with left and right division. In particular, we have to specify if we take remainders with respect to right or left division. We get semifields in both cases.

Semifields from twisted polynomials

There is only one finite field of given size p^n.

Semifields from twisted polynomials

There is only one finite field of given size p^n.

This is not true for finite semifields!

We can "play around" with twists, twisted polynomials, and try to construct new semifields (and thus planes, codes,...).

Difficult: Find out if semifields are really "new".

Making things explicit

We would like to make things "explicit".

Let $S_f = \mathbb{F}_{p^m}[t;\sigma]/(f)$ where $\deg(f) = d$.

Let us see how multiplication with t (from the left) works.

Define $L_{t,f} \colon S_f \to S_f$ via $L_{t,f}(v) = (tv) \pmod{f}$.

It is easy to check that

- $L_{t,f}(av) = a^{\sigma} L_{t,f}(v)$ and
- $L_{t,f}(v + w) = L_{t,f}(v) + L_{t,f}(w)$ for all $v, w \in V$, $a \in \mathbb{F}_{p^m}$.

Making things explicit

Definition (Semilinear mapping)

Let $F = \mathbb{F}_{p^m}$ be a finite field, σ be an automorphism of F and let $V = F^d$. A mapping $L\colon V \to V$ is σ-semilinear if it satisfies

- $L(x+y) = L(x) + L(y)$ for all $x, y \in V$,
- $L(ax) = a^\sigma L(x)$ for all $x \in V$, $a \in F$.

The set of all bijective semilinear mappings is called $\Gamma L(d, F)$.

Note that $V \cong S_f = \mathbb{F}_{p^n}[t;\sigma]/(f)$ as vector spaces. So left-multiplying with t in S_f corresponds to a σ-semilinear mapping on V.

Making things explicit

Definition (Semilinear mapping)

Let $F = \mathbb{F}_{p^m}$ be a finite field, σ be an automorphism of F and let $V = F^d$. A mapping $L\colon V \to V$ is σ-semilinear if it satisfies

- $L(x+y) = L(x) + L(y)$ for all $x, y \in V$,
- $L(ax) = a^{\sigma} L(x)$ for all $x \in V$, $a \in F$.

The set of all bijective semilinear mappings is called $\Gamma L(d, F)$.

Note that $V \cong S_f = \mathbb{F}_{p^n}[t;\sigma]/(f)$ as vector spaces. So left-multiplying with t in S_f corresponds to a σ-semilinear mapping on V.

But which semilinear mappings correspond to the $L_{t,f}$ where f is irreducible?

Translating twisted polynomials into semilinear mappings

Recall: We call $L \in \Gamma L(d, F)$ irreducible if L has no non-trivial invariant subspaces.

Translating twisted polynomials into semilinear mappings

Recall: We call $L \in \Gamma L(d, F)$ irreducible if L has no non-trivial invariant subspaces.

Theorem (Dempwolff 2010; Lavrauw, Sheekey, 2013)

Let $L_{t,f}$ be the mapping induced by left-multiplication by t on $V = \mathbb{F}_{p^n}[t;\sigma]/(f)$ for some irreducible twisted polynomial f. Then

- $L_{t,f} \in \Gamma L(d, \mathbb{F}_{p^n})$ *is irreducible.*
- *every irreducible semilinear mapping is* $\mathrm{GL}(d, \mathbb{F}_{p^n})$*-conjugate to* $L_{t,f}$ *for some irreducible twisted polynomial* f*.*

Translating twisted polynomials into semilinear mappings

Recall: We call $L \in \Gamma L(d, F)$ irreducible if L has no non-trivial invariant subspaces.

Theorem (Dempwolff 2010; Lavrauw, Sheekey, 2013)

Let $L_{t,f}$ be the mapping induced by left-multiplication by t on $V = \mathbb{F}_{p^n}[t;\sigma]/(f)$ for some irreducible twisted polynomial f. Then

- $L_{t,f} \in \Gamma L(d, \mathbb{F}_{p^n})$ *is irreducible.*
- *every irreducible semilinear mapping is* $\mathrm{GL}(d, \mathbb{F}_{p^n})$*-conjugate to* $L_{t,f}$ *for some irreducible twisted polynomial* f.

This means working with irreducible semilinear mappings on a vector space is the same as working with irreducible twisted polynomials.

Making things explicit

Question

How do we recognize irreducible semilinear mappings?

Use connection between projective polynomials and twisted polynomials.

Recall:

Theorem (Ore 1933)

The projective polynomial $P(x) = x^{[d]} + c_{d-1}x^{[d-1]} + \cdots + c_1 x^{[1]} + c_0 \in \mathbb{F}_{p^m}[x]$ has no roots if and only if $p(t) = t^d + c_{d-1}t^{d-1} + \cdots + c_1 t + c_0 \in \mathbb{F}_{p^m}[t;\sigma]$ has no linear right divisor.

$d = 2$: No linear right divisor $\Leftrightarrow$ irreducible.

Making things explicit

Theorem (Ore 1933)

The projective polynomial $P(x) = x^{q+1} + bx + a \in \mathbb{F}_{p^m}[x]$ has no roots if and only if $p(t) = t^2 + bt + a \in \mathbb{F}_{p^m}[t;\sigma]$ is irreducible.

Projective polynomials create a bridge between twisted polynomials and a general vector space view!

This allows us to compare semifields constructed using twisted polynomials and other semifields.

Irreducible semilinear mappings

Every semilinear mapping $L\colon F^d \to F^d$ can be written as

$$L(\mathbf{x}) = M_L \cdot \mathbf{x}^\sigma,$$

where $\mathbf{x} = (x_1, \ldots, x_d)^t$ and $\mathbf{x}^\sigma = (x_1^\sigma, \ldots, x_d^\sigma)^t$ and M_L is a $d \times d$ matrix with coefficients in F.

Proposition (Irreducible semilinear mappings for $d = 2$)

The mapping $L \in \Gamma L(2, F)$ with associated $M_L = \left(\begin{smallmatrix} 0 & \alpha \\ 1 & \beta \end{smallmatrix}\right) \in \mathrm{GL}(2, F)$ and field automorphism $\sigma\colon x \mapsto x^q$ is irreducible if and only if the polynomial $P(x) = x^{q+1} - \beta x - \alpha \in F[x]$ has no roots in F.

The vector space view and the twisted polynomial view

Many constructions of semifields use a 2-dimensional vector space view:

Hughes-Kleinfeld, 1960; Knuth, 1965:

Let $\mathbb{K}$ be a finite field. In [7] Knuth gave four multiplications for $(\mathbb{K}^2, +, \circ)$ all of which give semifields under the condition that $\eta, \mu \in \mathbb{K}$ and σ, an automorphism of $\mathbb{K}$, are chosen so that $x^{\sigma+1} + \mu x - \eta$ has no root in $\mathbb{K}$. They are

$\mathbb{S}_1$ defined by

$$(u, v) \circ (x, y) = (ux + \eta y^\sigma v^{\sigma^{-2}}, x^\sigma v + uy + \mu y^\sigma v^{\sigma^{-1}})$$

$\mathbb{S}_2$ defined by

$$(u, v) \circ (x, y) = (ux + \eta y^\sigma v, x^\sigma v + uy + \mu y^\sigma v)$$

$\mathbb{S}_3$ defined by

$$(u, v) \circ (x, y) = (ux + \eta y^{\sigma^{-1}} v^{\sigma^{-2}}, x^\sigma v + uy + \mu y v^{\sigma^{-1}})$$

and $\mathbb{S}_4$ defined by

$$(u, v) \circ (x, y) = (ux + \eta y^{\sigma^{-1}} v, x^\sigma v + uy + \mu y v).$$

The vector space view and the twisted polynomial view

Zhou-Pott, 2011; Taniguchi 2019

Theorem 1. *Let p be an odd prime, and let m, k be positive integers, such that $\frac{m}{\gcd(m,k)}$ is odd. Define $x \circ_k y = x^{p^k} y + y^{p^k} x$. For elements $(a, b), (c, d) \in \mathbb{F}_{p^m}^2$, define a binary operation $*$ as follows:*

$$(a, b) * (c, d) = (a \circ_k c + \alpha(b \circ_k d)^\sigma, ad + bc), \tag{4}$$

where α is a non-square element in $\mathbb{F}_{p^m}$ and σ is a field automorphism of $\mathbb{F}_{p^m}$. Then, $(\mathbb{F}_{p^{2m}}, +, *)$ is a presemifield, which we denote by $\mathbb{P}_{k,\sigma}$.

Theorem 5 *Let $(x, s), (y, t) \in F \times F$. We define a multiplication $*$ on $F \times F$ as follows. Then we have a presemifield $(F \times F, +, *)$.*

$$(x, s) * (y, t) := ((x \circ_\alpha y)^{\sigma^2} - a(x^\sigma t - \alpha y^\sigma s)^\sigma - b(s \circ_\alpha t), xt + ys). \tag{3}$$

The vector space view and the twisted polynomial view

On the other hand: Constructions using twisted polynomials (Sheekey, 2020)

Theorem 6. *Let L be a field, σ an automorphism of L with fixed field K, and ρ an automorphism of L over some field $K' \leq K$. Let $R = L[x;\sigma]$, let F be an irreducible polynomial in $K[y]$ of degree s, $E = \frac{K[y]}{(F(y))}$, and $R_F = \frac{R}{RF(x^n)}$.*
Then the set

$$S_{n,s,k}(\eta, \rho, F) := \{a + RF(x^n) : \deg(a) \leq ks, a_{ks} = \eta a_0^{\rho}\}$$

defines a K'-linear MRD code in $R_F \simeq M_n(E_F)$ with minimum distance $n - k + 1$ for any $\eta \in L$ such that $N_{L:K'}(\eta) N_{K:K'}((-1)^{sk(n-1)} F_0^k) \neq 1$.

Question

How do these two construction methods interact? Do they overlap?

Question

How do these two construction methods interact? Do they overlap?

Vector space view:

- Only small dimensions ($d = 2$, $d = 3$)
- More explicit
- Easier to check equivalence/novelty of semifields

Question

How do these two construction methods interact? Do they overlap?

Vector space view:

- Only small dimensions ($d = 2$, $d = 3$)
- More explicit
- Easier to check equivalence/novelty of semifields

Twisted polynomial view:

- Arbitrary dimension usually
- More structural
- Harder to check equivalence/novelty of semifields

Translating

Using our projective polynomials framework, we can translate from one view to the other!

Translating

Using our projective polynomials framework, we can translate from one view to the other!

Results:

Translating

Using our projective polynomials framework, we can translate from one view to the other!

Results:

- Some "vector space semifields" are equivalent to known twisted polynomial constructions

Translating

Using our projective polynomials framework, we can translate from one view to the other!

Results:

- Some "vector space semifields" are equivalent to known twisted polynomial constructions
- Many are not!

Question

Can we unify these approaches at least for low d, like $d = 2$?

Unifying approaches

Using a "unified approach", we are able to construct a framework that generalizes around a *dozen* families of semifields.

This

- "explains" many ad hoc vector space constructions and connects them to constructions using twisted polynomials.
- Shows that existing twisted polynomials constructions "left a lot on the table"

New unified construction

Construction

Let $V = F^2$, $\mathbf{x}, \mathbf{y} \in V$ with $\mathbf{y} = \left(\begin{smallmatrix} y_0 \\ y_1 \end{smallmatrix}\right)$ and σ be a field automorphism of F with fixed field K. Further, let $T_a \in \Gamma L(2, F)$, $a \in F^*$ be irreducible mappings satisfying $T_a + T_b = T_{a+b}$ for any $a, b \in F$ where we set $T_0 = T_0^{-1} = 0$. Then

$$\mathbf{x} \circ \mathbf{y} = y_0\mathbf{x} + \eta T_{y_1}(\mathbf{x}) + \det(M_{T_{y_1}})^{\overline{\sigma}} T_{y_1}^{-1}(\mathbf{x})$$

defines a semifield for any $\eta \in L$ with $N_{L:K}(\eta) \neq 1$.

There is a second similar construction as well...

New unified construction

Construction

Let $V = F^2$, $\mathbf{x}, \mathbf{y} \in V$ with $\mathbf{y} = \binom{y_0}{y_1}$ and σ be a field automorphism of F with fixed field K. Further, let $T_a \in \Gamma L(2, F)$, $a \in F^*$ be irreducible mappings satisfying $T_a + T_b = T_{a+b}$ for any $a, b \in F$ where we set $T_0 = T_0^{-1} = 0$. Then

$$\mathbf{x} \circ \mathbf{y} = y_0\mathbf{x} + \eta T_{y_1}(\mathbf{x}) + \det(M_{T_{y_1}})^{\overline{\sigma}} T_{y_1}^{-1}(\mathbf{x})$$

defines a semifield for any $\eta \in L$ with $N_{L:K}(\eta) \neq 1$.

How can we find that?

Projective polynomials to the rescue

Let $T_a \in \Gamma L(2, F)$, $a \in F^*$ be irreducible transformations satisfying $T_a + T_b = T_{a+b}$ for any $a, b \in F$

Proposition (Irreducible mappings for $d = 2$)

The mapping $L \in \Gamma L(2, F)$ *with associated* $M_L = \left(\begin{smallmatrix} 0 & \alpha \\ 1 & \beta \end{smallmatrix}\right) \in \mathrm{GL}(2, F)$ *and field automorphism* $\sigma \colon x \mapsto x^q$ *is irreducible if and only if the polynomial* $P(x) = x^{q+1} - \beta x - \alpha \in F[x]$ *has no roots in* F.

So this turns into a question on projective polynomials!

Results

Family	Construction	Notes
(Generalized) Dickson	Construction 1	—
Knuth I	Construction 2	—
Knuth II,III,IV, Hughes-Kleinfeld	Construction 2	—
Bierbrauer, Budaghyan-Helleseth	Construction 1	Contains commutative semifields
Dempwolff	Construction 1	Unnecessary conditions in original paper
Zhou-Pott	Construction 1	For parameter $\eta = -1$
Taniguchi	Construction 1	Largest known construction for p odd
(Twisted) cyclic semifields	Constructions 1,2	Construction only covers $d = 2$

Table: Known infinite families of semifields of order p^{2m} and how to recreate them

New semifields

The constructions also lead to a large family of semifields of size p^{2m} for all p, m, the new multiplication is:

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \circ \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = y_0\mathbf{x} + \eta \begin{pmatrix} 0 & y_1\alpha \\ y_1^\tau & 0 \end{pmatrix} \mathbf{x}^\sigma + \begin{pmatrix} 0 & -(y_1\alpha)^{\overline{\sigma}} \\ -y_1^{\tau\overline{\sigma}} & 0 \end{pmatrix} \mathbf{x}^{\overline{\sigma}}$$
$$= \begin{pmatrix} x_0 y_0 + \eta\alpha x_1^\sigma y_1 - x_1^{\overline{\sigma}}(\alpha y_1)^{\overline{\sigma}} \\ x_1 y_0 + \eta x_0^\sigma y_1^\tau - x_0^{\overline{\sigma}} y_1^{\tau\overline{\sigma}} \end{pmatrix}.$$

Taking stock

We use the connections between irreducible twisted polynomials, irreducible semilinear mappings, and projective polynomials for $d = 2$.

Taking stock

We use the connections between irreducible twisted polynomials, irreducible semilinear mappings, and projective polynomials for $d = 2$.

Question

Can we do make similar progress also for $d > 2$?

Ore's theorem

Theorem (Ore 1933)

The projective polynomial $P(x) = x^{[d]} + c_{d-1}x^{[d-1]} + \cdots + c_1 x^{[1]} + c_0 \in \mathbb{F}_{p^m}[x]$ *has no roots if and only if* $p(t) = t^d + c_{d-1}t^{d-1} + \cdots + c_1 t + c_0 \in \mathbb{F}_{p^m}[t;\sigma]$ *has no linear right divisor.*

If $d > 3$ then it is not true anymore that p irreducible $\Leftrightarrow$ P has no roots.

Ore's theorem

Theorem (Ore 1933)

The projective polynomial $P(x) = x^{[d]} + c_{d-1}x^{[d-1]} + \cdots + c_1 x^{[1]} + c_0 \in \mathbb{F}_{p^m}[x]$ *has no roots if and only if* $p(t) = t^d + c_{d-1}t^{d-1} + \cdots + c_1 t + c_0 \in \mathbb{F}_{p^m}[t;\sigma]$ *has no linear right divisor.*

If $d > 3$ then it is not true anymore that p irreducible $\Leftrightarrow$ P has no roots.

Things become *less explicit*. The "vector space view" is much harder!

Is the degree $d = 3$ case another sweet spot?

Highly nonlinear functions

Definition

Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be a vectorial function. The difference distribution table of F is defined as

$$\mathrm{DDT}_F(u, v) := \#\{x \in \mathbb{F}_p^n : F(x + u) - F(x) = v\}.$$

The differential uniformity of F is

$$\Delta_F := \max\{\mathrm{DDT}_F(u, v) : u, v \in \mathbb{F}_p^n, u \neq 0\}.$$

We call F such that $\Delta_F = 1$ *perfect nonlinear (PN)*.

If $p = 2$, $\mathrm{DDT}_F(u, v)$ is even so $\Delta_F \geq 2$. We call F such that $\Delta_F = 2$ *almost perfect nonlinear (APN)*.

Finding highly nonlinear functions

To find a PN/APN function we need to control the number of solutions of $F(x+u)-F(x)=v$ for all $u \neq 0$, v. Total: $(p^n-1)p^n$ equations.

Finding highly nonlinear functions

To find a PN/APN function we need to control the number of solutions of $F(x+u)-F(x)=v$ for all $u \neq 0$, v. Total: $(p^n-1)p^n$ equations.

If F is *quadratic* then $F(x+u)-F(x)$ is an affine function for all u, so calculating a kernel replaces the equations for all v.

Finding highly nonlinear functions

To find a PN/APN function we need to control the number of solutions of $F(x+u)-F(x)=v$ for all $u \neq 0$, v. Total: $(p^n-1)p^n$ equations.

If F is *quadratic* then $F(x+u)-F(x)$ is an affine function for all u, so calculating a kernel replaces the equations for all v.

If $F = x^d$ is a monomial over a finite field then

$$(x+u)^d - x^d = u^d \left((x/u+1)^d - (x/u)^d\right),$$

so instead of $u \in \mathbb{F}_{p^n}^*$ we only need to verify $u = 1$.

Finding highly nonlinear functions

To find a PN/APN function we need to control the number of solutions of $F(x+u)-F(x)=v$ for all $u \neq 0$, v. Total: $(p^n-1)p^n$ equations.

If F is *quadratic* then $F(x+u)-F(x)$ is an affine function for all u, so calculating a kernel replaces the equations for all v.

If $F=x^d$ is a monomial over a finite field then

$$(x+u)^d - x^d = u^d\left((x/u+1)^d - (x/u)^d\right),$$

so instead of $u \in \mathbb{F}_{p^n}^*$ we only need to verify $u=1$.

Can we replicate a similar effect?

Projective functions

Let $F\colon \mathbb{F}_q^2 \to \mathbb{F}_q^2$ defined via $F(x,y) = (f_1(x,y), f_2(x,y))$, where f_1, f_2 are d-homogeneous. Then

$$\begin{aligned}
&F(x+u_1, y+u_2) - F(x,y)\\
&= F\left(u_2\left(\frac{x}{u_2}+\frac{u_1}{u_2}\right), u_2\left(\frac{y}{u_2}+1\right)\right) - F\left(u_2\frac{x}{u_2}, u_2\frac{y}{u_2}\right)\\
&= u_2^d\left(F\left(\frac{x}{u_2}+\frac{u_1}{u_2}, \frac{y}{u_2}+1\right) - F\left(\frac{x}{u_2}, \frac{y}{u_2}\right)\right)\\
&= u_2^d\left(F\left(x'+\frac{u_1}{u_2}, y'+1\right) - F\left(x', y'\right)\right)
\end{aligned}$$

So instead of ranging over all $(u_1, u_2) \in \mathbb{F}_q^2$ it is enough to range over all $(u,1) \in \mathbb{F}_q^2$ (and $(1,0) \in \mathbb{F}_q^2$).

Check the projective line instead of $\mathbb{F}_q^2$!

Constructions

Let $F\colon \mathbb{F}_q^2 \to \mathbb{F}_q^2$ defined via $F(x,y) = (f_1(x,y), f_2(x,y))$, where f_1, f_2 are d-homogeneous.

Some known constructions of APN/PN functions can be written like this!

Constructions

Let $F\colon \mathbb{F}_q^2 \to \mathbb{F}_q^2$ defined via $F(x,y) = (f_1(x,y), f_2(x,y))$, where f_1, f_2 are d-homogeneous.

Some known constructions of APN/PN functions can be written like this!

Note: If $(S, +, \circ)$ is a commutative semifield in odd characteristic then $F(x) = x \circ x$ is a PN function.

These constructions basically correspond to the semifields I presented earlier for the $d = 2$ case.

The same is true to a lesser degree for APN functions.

So what if $d > 2$?

Some generalizations

Let $F\colon \mathbb{F}_{p^m}^k \to \mathbb{F}_{p^m}^k$ defined by $F(\mathbf{x}) = (f_1(\mathbf{x}), \dots, f_k(\mathbf{x}))$, where all f_i are $q+1$-homogeneous and quadratic, where $q = p^k$.

We have $F(a\mathbf{x}) = a^{q+1}F(\mathbf{x})$. If $F(\mathbf{x}) = 0$ only for $\mathbf{x} = 0$, F can be viewed purely on the projective space $\mathbb{P}^{k-1}(\mathbb{F}_{p^m})$.

We call the resulting function $\overline{F}\colon \mathbb{P}^{k-1}(\mathbb{F}_{p^m}) \to \mathbb{P}^{k-1}(\mathbb{F}_{p^m})$.

Connection between PN/APN and $\overline{F}$

Theorem (GK, 2025+)

If $\overline{F}$ is bijective on $\mathbb{P}^{k-1}(\mathbb{F}_{p^m})$ then F is $\gcd(q+1, p^m-1)$-to-1 on $\mathbb{F}_{p^m}^k \setminus \{\mathbf{0}\}$.

In particular, if p is odd, we can choose q in a way that $\gcd(q+1, p^m-1) = 2$.

Weng, Zeng 2012: Such functions are always PN.

Connection between PN/APN and $\overline{F}$

Theorem (GK, 2025+)

If $\overline{F}$ is bijective on $\mathbb{P}^{k-1}(\mathbb{F}_{p^m})$ then F is $\gcd(q+1, p^m-1)$-to-1 on $\mathbb{F}_{p^m}^k \setminus \{\mathbf{0}\}$.

In particular, if p is odd, we can choose q in a way that $\gcd(q+1, p^m-1) = 2$.
Weng, Zeng 2012: Such functions are always PN.

If $p = 2$, m even, we can choose q in a way that $\gcd(q+1, p^m-1) = 3$
Kölsch, Kriepke, Kyureghyan, 2021: Such functions are always APN.

If $p = 2$, m odd, we can choose q in a way that $\gcd(q+1, p^m-1) = 1$, so F is a bijection.

Finding a bijection of the projective space

Question

How can we find such bijections of the projective space?

For $k = 2$ (bijections of $\mathbb{P}^1(\mathbb{F}_{p^m})$): Göloğlu and Ding-Zieve have proven that all examples are "degenerate" or equivalent to monomials.

Question

Are there such bijections of the projective space that are not equivalent to monomials?

A new bijection of the projective plane

Theorem (GK, 2026+)

Let $f, g, h\colon \mathbb{F}_{p^m}^3 \to \mathbb{F}_{p^m}$ be defined as

$$f(x,y,z) = x^{q+1} + ay^q z + bx^q y + cx^q z,$$
$$g(x,y,z) = ay^{q+1} + z^q x + bz^q y + cx^q y,$$
$$h(x,y,z) = z^{q+1} - x^q y,$$

where $a, b, c \in \mathbb{F}_{p^m}$ and $q = p^k$.
Then $\overline{F} = (\overline{f, g, h})$ is bijective if and only if the equation

$$ax^{q^2+q+1} + bx^{q+1} + cx + 1 = 0 \tag{1}$$

has no solution $x \in \mathbb{F}_{p^m}$.

The resulting APN/PN functions

Choosing q correctly we get

- PN functions for p odd on $\mathbb{F}_{p^m}^3$ for all $m > 1$.
- 3-to-1 APN functions for $p = 2$ on $\mathbb{F}_{2^m}^3$ for all even m.

The resulting APN/PN functions

Choosing q correctly we get

- PN functions for p odd on $\mathbb{F}_{p^m}^3$ for all $m > 1$.
- 3-to-1 APN functions for $p = 2$ on $\mathbb{F}_{2^m}^3$ for all even m.
- APN permutations for $p = 2$ on $\mathbb{F}_{2^m}^3$ for all odd $m > 1$. (GK, 2026+)

This widely generalizes several known families of PN functions (Zha-Kyureghyan-Wang, Bierbrauer) and APN functions (Li-Kaleyski, Bartoli-Stanica).

The resulting APN/PN functions

Choosing q correctly we get

- PN functions for p odd on $\mathbb{F}_{p^m}^3$ for all $m > 1$.
- 3-to-1 APN functions for $p = 2$ on $\mathbb{F}_{2^m}^3$ for all even m.
- APN permutations for $p = 2$ on $\mathbb{F}_{2^m}^3$ for all odd $m > 1$. (GK, 2026+)

This widely generalizes several known families of PN functions (Zha-Kyureghyan-Wang, Bierbrauer) and APN functions (Li-Kaleyski, Bartoli-Stanica).

And explains their existence in a nice way!

Questions

Question

Is this new family somehow related to twisted polynomial constructions?

Question

Can we find similar constructions in dimensions > 3*? What happens to the projective polynomials?*

Questions

Question

Is this new family somehow related to twisted polynomial constructions?

Question

Can we find similar constructions in dimensions > 3? What happens to the projective polynomials?

Theorem (Ore 1933)

The projective polynomial $P(x) = x^{[d]} + c_{d-1}x^{[d-1]} + \cdots + c_1 x^{[1]} + c_0 \in \mathbb{F}_{p^m}[x]$ *has no roots if and only if* $p(t) = t^d + c_{d-1}t^{d-1} + \cdots + c_1 t + c_0 \in \mathbb{F}_{p^m}[t;\sigma]$ *has no linear right divisor.*

Merci!

Projective polynomials and some of their applications

Lukas Kölsch

University of South Florida

June 9th, 2026

(joined work with Faruk Göloğlu)