Projective polynomials in cryptography and algebra: nonlinear functions and finite semifields

Faruk Göloğlu

Charles University, Prague

Algebra Colloquium, MFF-KA, November 14, 2023

Finite semifields

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 $x \circ \epsilon = x = \epsilon \circ x$.

Semifields

- An algebraic object satisfying the first three of the above axioms is called a **pre-semifield**.
- If $\mathbb{P} = (P, +, \circ)$ is a pre-semifield, then $(P, +)$ is an elementary abelian p-group.
- If $\circ$ is associative then $\mathbb{S}$ is the finite field $\mathbb{F}_{p^n}$ by Wedderburn's theorem.
- By a result of Menichetti (known as Kaplansky's conjecture) when $n > 2$, there exist *proper* semifields of order p^n where $\circ$ is non-associative.

Semifields

- A pre-semifield $\mathbb{P} = (\mathbb{F}_p^n, +, \circ)$ can be converted to a semifield $\mathbb{S} = (\mathbb{F}_p^n, +, *)$ using *Kaplansky's trick* by defining the new multiplication as

$$(x \circ e) * (e \circ y) = (x \circ y),$$

for any nonzero element $e \in \mathbb{F}_p^n$, making $(e \circ e)$ the multiplicative identity of $\mathbb{S}$.

Semifields

- We have $\mathbb{F}_p$-bilinear $B : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^n$, satisfying

  $$B(x, y) = x \circ y,$$

  and $\mathbb{F}_p$-linear left and right multiplications $L_x, R_y : \mathbb{F}_p^n \to \mathbb{F}_p^n$, with

  $$L_x(y) := B(x, y) =: R_y(x).$$

- The mapping L_x (resp. R_y) is a bijection whenever $x \neq 0$ (resp. $y \neq 0$) by (S3).
- (S3) interchangeable with the **quasigroup axiom**.

Semifields

- Two pre-semifields $\mathbb{P}_1 = (\mathbb{F}_p^n, +, \circ_1)$ and $\mathbb{P}_2 = (\mathbb{F}_p^n, +, \circ_2)$ are said to be **isotopic** if there exist $\mathbb{F}_p$-linear bijections L, M and N of $\mathbb{F}_p^n$ satisfying

$$N(x \circ_1 y) = L(x) \circ_2 M(y).$$

- Such a triple $\gamma = (N, L, M)$ is called an **isotopism** between $\mathbb{P}_1$ and $\mathbb{P}_2$. If additionally $L = M$ holds, we call γ a **strong isotopism** and $\mathbb{P}_1$ and $\mathbb{P}_2$ **strongly isotopic**.

DO polynomials

- Every $\mathbb{F}_p$-linear mapping $L : \mathbb{F}_p^n \to \mathbb{F}_p^n$ can be written uniquely as a **linearized polynomial**

$$L(x) = \sum_{i=0}^{n-1} b_i x^{p^i},$$

in the polynomial ring $\mathbb{F}_{p^n}[x]$.

- Let p be an odd prime and consider the polynomials from $\mathbb{F}_{p^n}[x]$ of the form

$$F(x) = \sum_{0 \le i,j < n} a_{ij} x^{p^i + p^j}.$$

These polynomials are called **Dembowski-Ostrom (DO)** polynomials.

- The notions of degree.

DO polynomials

- The **polarization** of a DO polynomial F is defined as

$$\Delta_F(x,y) = F(x+y) - F(x) - F(y) + F(0).$$

- The mapping $\Delta_F : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^n$ is symmetric and $\mathbb{F}_p$-bilinear.
- If $\Delta_F(x,a) = 0$ implies $x = 0$ for all $a \in \mathbb{F}_{p^n}^\times = \mathbb{F}_{p^n} \setminus \{0\}$, then $\Delta_F(x,y)$ describes a commutative pre-semifield multiplication.
- Conversely, by a counting argument, every commutative pre-semifield multiplication can be written as $\Delta_F(x,y)$ for some DO polynomial F.
- In that case we will call $F(x)$ a **planar DO polynomial**.

Cryptography

Commutative semifields and APN functions in cryptography:

- In symmetric cryptography, **differential cryptanalysis**
- Let for $a, b \in \mathbb{F}_p^n$, where $a \neq 0$,

$$\delta_F(a,b) = \#\{x \in \mathbb{F}_p^n \ : \ F(x+a) - F(x) = b\}.$$

- If for carefully chosen a_i, b_i the value $\delta_F(a_i, b_i)$ are all *high*, one can devise a cryptanalysis of a cipher where the S-Box F is used in several consecutive *rounds*
- Perfect Nonlinear if $\delta_F(a,b) = 1$
- Almost Perfect Nonlinear if $\delta_F(a,b) \leq 2$ (optimal in characteristic two).

Projective and biprojective polynomials

- $\mathbb{L} = \mathbb{F}_{p^l}$ a finite field and $q = p^k$ with $0 \leq k < l$.
- A polynomial of the form
$$\phi_f(x) = ax^{q+1} + bx^q + cx + d \in \mathbb{L}[x] \tag{1}$$
is called a q-**projective polynomial** over $\mathbb{L}$.
- A polynomial of the form
$$f(x,y) = ax^{q+1} + bx^q y + cxy^q + dy^{q+1} \in \mathbb{L}[x,y]$$
is called a q-**biprojective polynomial** over $\mathbb{L}$. Note that
$$\phi_f(x) = f(x,1).$$
- We will use the shorthand notation
$$f = (a,b,c,d)_q$$

Projective and biprojective polynomials

Our main interest is in *cryptographic functions* of the following forms:

- (q, r)-**biprojective functions** of the form:

$$\begin{aligned} F : \mathbb{L} \times \mathbb{L} &\to \mathbb{L} \times \mathbb{L} \\ (x, y) &\mapsto (f(x, y), g(x, y)), \end{aligned}$$

  where f and g are q- and r-biprojective polynomials, and

- **fractional q-projective functions** of the form

$$\begin{aligned} \Pi : \mathcal{P}^1(\mathbb{L}) &\to \mathcal{P}^1(\mathbb{L}) \\ x &\mapsto \frac{\phi_f(x)}{\phi_g(x)}, \end{aligned}$$

  where ϕ_f and ϕ_g are q-projective polynomials. Note that we assume $\phi_f(x) = 0 = \phi_g(x)$ does not happen for $x \in \mathbb{L}$.

Representations of vectorial functions

- Let $n = mk$. $\mathbb{F}_p^n$ is a k-dimensional $\mathbb{F}_{p^m}$-vector space.
- For all possible factorizations of $n = mk$, we can represent a function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ as

$$F(x_1, \dots, x_k) = \sum_{0 \le i_1, \dots, i_k \le p^m - 1} a_{i_1, \dots, i_k} x_1^{i_1} \cdots x_k^{i_k}, \quad a_{i_1, \dots, i_k} \in \mathbb{F}_{p^m}^k,$$

in

$$\mathbb{F}_{p^m}[x_1, \dots, x_k]/(x_1^{p^m} - x_1, \dots, x_k^{p^m} - x_k).$$

Notions of degree

- **algebraic degree**

$$\deg F = \max \left\{ \sum_{j=1}^{k} \mathrm{wt}_p(i_j) \ : \ a_{i_1,\dots,i_k} \neq (0,0,\dots,0) \right\},$$

  where $\mathrm{wt}_p(i_j) = \sum_{l=1}^{m} i_{j\,l}$.

- Algebraic degree is independent of the representation.
- **polynomial degree**

$$\mathrm{pdeg}_k F = \max \left\{ \sum_{j=1}^{k} i_j \ : \ a_{i_1,\dots,i_k} \neq (0,0,\dots,0) \right\}.$$

- For $n = m_1 k_1$ and $n = m_2 k_2$, the polynomial degrees $\mathrm{pdeg}_{k_1} F$ and $\mathrm{pdeg}_{k_2} F$ are not necessarily the same.

Biprojectivity in relation with the notions of degree

Recall the notions of q-biprojectivity:

$$f(x,y) = ax^{q+1} + bx^q y + cxy^q + dy^{q+1} \in \mathbb{L}[x,y],$$

and (q,r)-biprojectivity:

$$\begin{aligned} F : \mathbb{L} \times \mathbb{L} &\to \mathbb{L} \times \mathbb{L} \\ (x,y) &\mapsto (f(x,y), g(x,y)). \end{aligned}$$

The (q,r)-biprojective functions $F = (f_1, f_2)$ are

- quadratic (in the sense of algebraic degree) vectorial functions in bivariate representation $F(x,y) = (f_1(x,y), f_2(x,y))$ where
- both f_1 and f_2 are homogeneous (in the sense of polynomial degree) of degrees $q+1$ and $r+1$ respectively.

Classical methods for finding new semifields

- Finding pre-semifields of order p^n is equivalent to finding bilinear mappings $B : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ satisfying

$$B(X,U) = 0 \iff XU = 0.$$

- $$B(X,U) = \sum_{0 \le i,j < n} A_{ij} X^{p^i} U^{p^j}, \quad A_{ij} \in \mathbb{F}_{p^n}.$$

- Natural to consider first the *simplest* bilinear mappings that have few terms in this representation.

Classical methods for finding new (commutative) semifields

- For commutative pre-semifields of order p^n when p is odd one can consider (polarizations of) DO polynomials

$$F(X) = \sum_{0 \le i,j < n} B_{ij} X^{p^i + p^j}, \quad B_{ij} \in \mathbb{F}_{p^n},$$

- Identify planar mappings among them in increasing complexity, i.e., monomials, binomials, and so on.

Monomials and binomials

- Monomial bilinear mappings

$$B(X, U) = AX^q U^r,$$

  describe pre-semifields (via $X * U = B(X, U)$) that are isotopic to finite fields where q, r are $\mathbb{F}_{p^n}$-automorphisms and $A \in \mathbb{F}_{p^n}^{\times}$.
- The simplest commutative semifield is the finite field whose multiplication is given by the simplest bilinear mapping $B(X, U) = XU$
- The finite field corresponds to the polarization of the planar DO polynomial

$$F(X) = \frac{1}{2}X^2.$$

Monomials and binomials

- (Albert's generalized twisted fields) Any binomial can be written up to isotopy

$$B(X,U) = AXU - X^q U^r,$$

and describes a pre-semifield if and only if

$$A \notin (\mathbb{F}_{p^n}^{\times})^{q-1}(\mathbb{F}_{p^n}^{\times})^{r-1}.$$

- Generalized twisted fields that are isotopic to a commutative semifield are isotopic to the twisted field

$$B(X,U) = X^q U + XU^q,$$

when $n/\gcd(k,n)$ is odd where $q = p^k$ (Albert '65).

- In this case the corresponding planar DO polynomial whose polarization gives a commutative twisted field is

$$F(X) = X^{q+1}.$$

Tri- and multinomials

- The natural approach that is used to classify the above cases does not seem to work for larger number of terms.
- Indeed, the only known (to the best of our knowledge) instance of trinomial (commutative) pre-semifields not isotopic to finite fields or generalized twisted fields are isotopic to the pre-semifield described by the bilinear map over $\mathbb{F}_{3^5} \times \mathbb{F}_{3^5}$.

$$B(X, U) = X^{81}U^9 + X^9U^{81} - XU$$

- Some commutative multinomials:
- Zha, Kyureghyan and Wang (Family $\mathcal{ZKW}$) and Bierbrauer (Families $\mathcal{B}_3$ and $\mathcal{B}_4$) — binomial DO mappings.
- Budaghyan and Helleseth (Family $\mathcal{BH}$) — multinomial planar functions, discovered independently by Zha and Wang — trinomial DO mappings.

The bivariate method of Dickson and others

- To construct a semifield of order p^n where p is odd and $n = 2m$ is even, one can consider a quadratic polynomial F in bivariate representation

$$F(x, y) = (f(x, y), g(x, y)).$$

- F is planar $\iff$ polarization of F has only trivial zeroes.
- In the bivariate method, this corresponds to solving

$$\begin{aligned} f(x+u, y+v) - f(x, y) - f(u, v) + f(0, 0) = 0, \\ g(x+u, y+v) - g(x, y) - g(u, v) + f(0, 0) = 0, \end{aligned}$$

simultaneously.

- Choose f to be the *simplest* nontrivial function $f(x, y) = xy$, i.e., the finite field multiplication
- First polarization becomes

$$\Delta_f((x, y), (u, v)) = xv + uy = 0,$$

  which in turn gives $x = -uy/v$ for nonzero v.
- Plug this into the second polarization to eliminate x and solve the problem for judicious choices of g.
- Starting with Dickson in 1935, many semifields by considering different g, again in increasing *complexity*: The family of Dickson (Family $\mathcal{D}$) the family of Zhou and Pott (Family $\mathcal{ZP}$) as well as Bierbrauer's (not necessarily commutative) family that includes $\mathcal{BH}/\mathcal{ZW}$
- Includes non-commutative and also weak nucleus semifields

Enumeration results (odd characteristic)

	commutative	general
before	$\approx n^2$	$\approx (p^n)^{1/2}$
after	$\approx (p^n)^{1/4}$	$\approx (p^n)^{2/3}$

Table: Known number of pairwise non-isotopic semifields of odd order p^n

Improving the number to an exponential level was considered a major open problem.

> *Deciding whether the number of nonisotopic (commutative) semifield[s] can be bounded by a polynomial in n [is] the main problem in connection with commutative semifields of [odd] order* p^n*.*

Alexander Pott. Almost perfect and planar functions. Des. Codes Cryptogr., 78(1):141–195, 2016.

Enumeration results (even characteristic)

- Until 1965 (Knuth) there were no known (proper) commutative semifield of even order (Dickson and Albert existed in odd case)
- Dramatic turn in 2003 with Kantor-Williams' family. Only a linear number (n) in the odd characteristic, the even characteristic case became super-polynomial (i.e., not bounded by a polynomial) in $q = p^n$.

  Finally, we come to the most important problem: much larger numbers of semifield planes are needed in all characteristics. The difficulty is the nonisomorphism question for planes, which is harder than that for the semifields themselves. Isotopies are notoriously difficult to deal with. [...] What is needed is a better and more general approach to proving nonisotopy.

William M. Kantor and Michael E. Williams. Symplectic semifield planes and Z4-linear codes. Trans. Amer. Math. Soc., 356(3):895–938, 2004.

(q, r)-biprojective (commmutative) semifields

Find planar (q, r)-biprojective mappings $F : \mathbb{M} \times \mathbb{M} \to \mathbb{M} \times \mathbb{M}$,

$$F : (x, y) \mapsto (f(x, y), g(x, y)),$$

wth,

$$f : (x, y) \mapsto a_0 x^{q+1} + b_0 x^q y + c_0 x y^q + d_0 y^{q+1},$$
$$g : (x, y) \mapsto a_1 x^{r+1} + b_1 x^r y + c_1 x y^r + d_1 y^{r+1}.$$

where $r = p^l$ for an integer $0 \leq l < m$ and $q = p^k$ for an integer $0 \leq k < m$.

- Consider $\mathrm{GL}(2, \mathbb{M})$, i.e., $(x, y) \mapsto (ax + by, cx + dy)$.
- In particular, $x \mapsto xz$ and $y \mapsto yz$ and divide by z^{q+1}

Advantages

Number of required permutations is low.

- $F(X) = X^{q+1}$ (for $q = p^k$)
- The polarizations are

$$\Delta_F(X, U) = X^q U + XU^q = 0,$$

- For every $U \in \mathbb{F}_{p^n}^\times$, apply $X \mapsto XU$ to get

$$U^{q+1}(X^q + X) = 0.$$

- This means that proving bijectivity of *one* linear mappping is enough. In this case, this mapping is described by $X \mapsto \Delta_F(X, 1) = X^q + X$.

Advantages

- Note that, for an arbitrary vectorial function, the number of required bijective linear mappings is $|\mathbb{F}_{p^n}^{\times}/\mathbb{F}_p^{\times}| = (p^n - 1)/(p-1)$.
- To show that the polarization $\Delta_F((x,y),(u,v)) = (x,y) * (u,v) = 0$ has a unique zero for each $(u,v) \in \mathbb{M} \times \mathbb{M} \setminus (0,0)$, by applying maps of the type $x \mapsto xu$, $y \mapsto yu$, $x \mapsto xv$, $y \mapsto yv$, $u \mapsto uv$ we see that showing bijective property of $p^{n/2}+1$ bijections is enough.

Lemma

Let $(x,y) \mapsto F(x,y) = (f(x,y), g(x,y))$ be a (q,r)-biprojective mapping of $\mathbb{M} \times \mathbb{M}$. Then F is planar if and only if the pair of equations

$$\mathrm{D}_f^u(x,y) = 0 = \mathrm{D}_g^u(x,y)$$

has exactly one solution for each $u \in \mathcal{P}^1(\mathbb{M})$.

Advantages

- Covers many previous constructions: Dickson, Albert, Zhou-Pott, FF, Budaghyan-Helleseth, Knuth, Taniguchi and many more.
- Let $q = p^k$ be an automorphism of $\mathbb{M}$ and $c, d \in \mathbb{M}$ such that

$$x^{q+1} + cx - d = 0$$

has no solutions $x \in \mathbb{M}$. The pre-semifields defined by

$$(x, y) * (u, v) = \begin{cases} (x^{q^2}v + yu^{q^2}, \quad y^q v + dx^q u + cyu^q), \\ (x^q v + yu^q, \quad y^q v + dxu^q + cyu^q), \\ (x^q v + yu^q, \quad yv^q + dx^q u + cyu^q), \\ (xv + yu, \quad y^q v + d^q x^q u + cy^q u), \end{cases}$$

are called Knuth semifields of Type II.i–iv.

- Biprojectivity not identified.

Advantages

- Consider two isotopic twisted fields $B_1(X,Y) = X^qY + DXY^q$ and $B_2(X,Y) = X^{q'}Y + EXY^{q'}$
- An isotopism triple $(L,M,N) \in (\mathrm{GL}(n,\mathbb{F}_p))^3$ mapping B_1 to B_2, i.e.,
$$N(B_1(X,Y)) = B_2(L(X),M(Y)),$$
satisfy $(L,M,N) \in \Gamma\mathrm{L}(1,\mathbb{F}_{p^n})^3$ which immediately implies q and q' should *agree*, i.e., $q' \in \{q,\overline{q}\}$.
- Moreover, (L,M,N) satisfies (setting $q = q'$),
$$L(X) = AX^r, M(Y) = BY^r, \text{ and } N(Z) = A^qBZ^r,$$
where $A,B \in \mathbb{F}_{p^n}^\times$ and r is an $\mathbb{F}_{p^n}$-automorphism satisfying $D^r/E = (B/A)^{q-1}$.
- Generalize this notion (in a sense) to $\Gamma\mathrm{L}(2,\mathbb{F}_{p^{n/2}})$.

Mauro Biliotti, Vikram Jha, and Norman L. Johnson. The collineation groups of generalized twisted field planes. Geom. Dedicata, 76(1):97–126, 1999.

Advantages

- There are many free spots for field coefficients
- Let us go back to the bilinear multiplications of GTFs of order p^n, i.e., $B(X,Y) = X^q Y + DXY^r$. Here we have two options for *variation*:
  - different choices for the field automorphisms q, r, and
  - different choices for the field coefficient D.
- Biprojective setting supplies many more spots for field coefficients even in the commutative case:

$$F = ((a_0, b_0, c_0, d_0)_q, (a_1, b_1, c_1, d_1)_r),$$

where

$$a_i, b_i, c_i, d_i \in \mathbb{M}, q, r \in \mathrm{Gal}(\mathbb{M}/\mathbb{F}_p).$$

- Explain intuitively why the known biprojective constructions were not able to exploit these spots — $\mathrm{GL}(2, \mathbb{M})$ connection.

Known biprojective cases

Finite field type coefficients,

$$((0,0,1,0)_q,(1,0,0,a)_r),$$

for a non-square $a \in \mathbb{M} \setminus \mathbb{M}^\times$ and

$$(q,r) = \begin{cases} (1,1) & \text{for finite fields,} \\ (q,1) & \text{for Family } \mathcal{D}, \\ (1,r) & \text{for Family } \mathcal{BH}/\mathcal{ZW}_{\text{odd}}, \\ (q,r) & \text{for Family } \mathcal{ZP}, \end{cases}$$

for judicious choices of q and r. For **Albert type coefficients**, i.e.,

$$((0,1,b,0)_q,(1,0,0,a)_r),$$

with select $a, b \in \mathbb{M}^\times$, we have

$$(q,r) = \begin{cases} (1,1) & \text{for finite fields,} \\ (q,q) & \text{for Family } \mathcal{A}, \\ (1,r) & \text{for Families } \mathcal{ZP} \text{ and } \mathcal{BH}/\mathcal{ZW}_{\text{odd}}, \\ (q,1) & \text{for Family } \mathcal{BH}/\mathcal{ZW}_{\text{even}}, \end{cases}$$

again for judicious choices of q and r.

New commutative semifields

Theorem (with Lukas Kölsch)

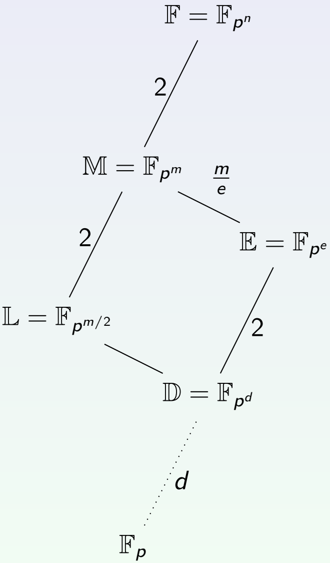
Let $a \in \mathbb{L}^\times$ *and* $B \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^2$ *and let*

$$F : \mathbb{M} \times \mathbb{M} \to \mathbb{M} \times \mathbb{M}$$

be defined as

$$F(x,y) = [(1,0,0,B)_q, (0,1,a/B,0)_r].$$

Then F *is planar.*


$\mathbb{F} = \mathbb{F}_{p^n}$
2
$\mathbb{M} = \mathbb{F}_{p^m}$
$\frac{m}{e}$
$\mathbb{E} = \mathbb{F}_{p^e}$
2
$\mathbb{L} = \mathbb{F}_{p^{m/2}}$
2
$\mathbb{D} = \mathbb{F}_{p^d}$
d
$\mathbb{F}_p$

- p is an odd prime.
- $n = 2m$, m is even.
- $Q = p^{m/2}, \quad Q^2 = p^m$.
- $q = p^k, \quad r = p^{k+m/2} = Qq$ with $1 \leq k \leq m-1$.
- $e = \gcd(k, m)$ with m/e odd.
- $d = \gcd(k + m/2, m)$.
- $e = 2d$.
- $\mathbb{E} = \mathbb{F}_q \cap \mathbb{M} = \mathbb{F}_{q^2} \cap \mathbb{M} = \mathbb{F}_{r^2} \cap \mathbb{M}$.
- $\mathbb{D} = \mathbb{F}_r \cap \mathbb{M}$.

Few words on the proof

Since there are too many nonzero coefficients on the both parts of

$$F(x, y) = [(1, 0, 0, B)_q, (0, 1, a/B, 0)_r].$$

the proof is essentially different from Dickson's method. The proof uses intricate relations of non-squares that results in a contradiction.

The isotopy technique that works for any two biprojective semifields is then used to show non-isotopy and in enumeration.

Analogy with Albert

- A theorem of Albert states (under certain conditions) that every isotopism δ between two twisted fields with defining field automorphisms q and q' respectively, has to satisfy:
  - $\delta \in \Gamma\mathrm{L}(1, \mathbb{F})^3$,
  - q and q' should agree, and
  - L, M, N, the component linear maps of δ, satisfy further restrictions.
- We prove that **if there is an isotopism δ between two biprojective semifields with defining field automorphisms (q, r) and (q', r') respectively, then there is an isotopism γ between these semifields** with
  - $\gamma \in \Gamma\mathrm{L}(2, \mathbb{M})^3$,
  - (q, r) and (q', r') should *agree*, and
  - L, M, N, the component linear maps of γ, satisfy further restrictions.

Number of non-isotopic semifields in the new family

Corollary

Let $N_{\mathcal{S}}(p,n)$ be the number of non-isotopic pre-semifields in Family $\mathcal{S}$ on $\mathbb{F}_p^n$. Then

$$\frac{\sigma(n)-1}{2} \cdot \frac{p^{n/4}-1}{n} \leq N_{\mathcal{S}}(p,n) \leq \frac{\sigma(n)-1}{2}\left(p^{n/4}-1\right).$$

Corollary

The number of pairwise non-isotopic Taniguchi semifields of order p^{2m} is $\Theta(p^{4m/3})$.

Classification of (q, q)-biprojective APN functions

Theorem

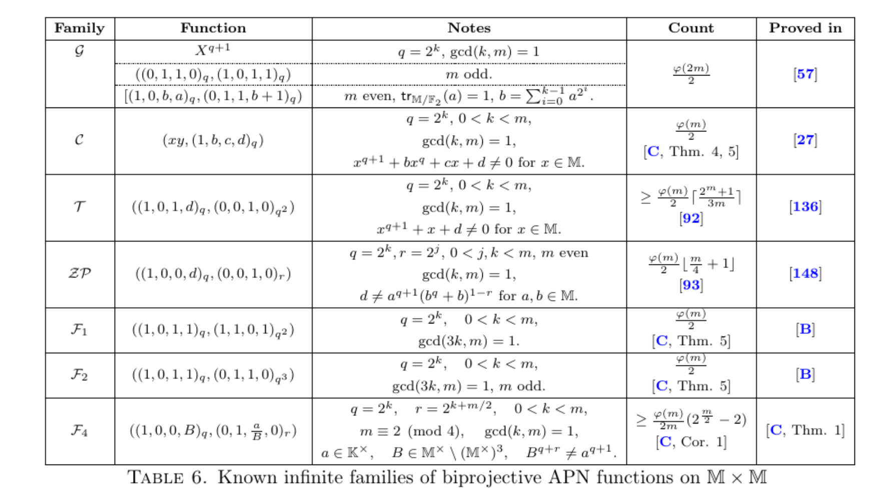
Let $q = 2^k$, $r = 2^l$, $\mathbb{L} = \mathbb{F}_{2^l}$ with $0 < k < l$ and $F : \mathbb{L} \times \mathbb{L} \to \mathbb{L} \times \mathbb{L}$ be a (q, q)-biprojective function. Then F is APN if and only if $\gcd(k, l) = 1$, and

1. *l is even and $F \approx_{\mathfrak{L}} G_{q+1}$ or $F \approx_{\mathfrak{L}} G_{q+r}$, or*
2. *l is odd, k is odd, and $F \approx_{\mathfrak{L}} G_{q+1}$, or*
3. *l is odd, k is even, and $F \approx_{\mathfrak{L}} G_{q+r}$, or*
4. *$l = 3$ and $F \approx_{\mathfrak{L}} \kappa$.*

- κ: the only known APN permutation on an even dimension.
- G_s: the Gold maps $X \mapsto X^s$ which are not *equivalent* to permutations on even extensions (with P. Langevin)
- $F \approx_{\mathfrak{L}} G$ means

$$M \circ F \circ N = G \text{ for some } M, N \in \mathrm{GL}(2, \mathbb{L}).$$

Classification of (q, q)-biprojective APN functions



Family	Function	Notes	Count	Proved in
$\mathcal{G}$	X^{q+1}	$q = 2^k$, $\gcd(k, m) = 1$	$\frac{\varphi(2m)}{2}$	[57]
	$((0, 1, 1, 0)_q, (1, 0, 1, 1)_q)$	m odd.		
	$[(1, 0, b, a)_q, (0, 1, 1, b + 1)_q)$	m even, $\mathrm{tr}_{\mathbb{M}/\mathbb{F}_2}(a) = 1$, $b = \sum_{i=0}^{k-1} a^{2^i}$.		
$\mathcal{C}$	$(xy, (1, b, c, d)_q)$	$q = 2^k$, $0 < k < m$, $\gcd(k, m) = 1$, $x^{q+1} + bx^q + cx + d \neq 0$ for $x \in \mathbb{M}$.	$\frac{\varphi(m)}{2}$ [C, Thm. 4, 5]	[27]
$\mathcal{T}$	$((1, 0, 1, d)_q, (0, 0, 1, 0)_{q^2})$	$q = 2^k$, $0 < k < m$, $\gcd(k, m) = 1$, $x^{q+1} + x + d \neq 0$ for $x \in \mathbb{M}$.	$\geq \frac{\varphi(m)}{2} \lceil \frac{2^m+1}{3m} \rceil$ [92]	[136]
$\mathcal{ZP}$	$((1, 0, 0, d)_q, (0, 0, 1, 0)_r)$	$q = 2^k, r = 2^j$, $0 < j, k < m$, m even $\gcd(k, m) = 1$, $d \neq a^{q+1}(b^q + b)^{1-r}$ for $a, b \in \mathbb{M}$.	$\frac{\varphi(m)}{2} \lfloor \frac{m}{4} + 1 \rfloor$ [93]	[148]
$\mathcal{F}_1$	$((1, 0, 1, 1)_q, (1, 1, 0, 1)_{q^2})$	$q = 2^k$, $0 < k < m$, $\gcd(3k, m) = 1$.	$\frac{\varphi(m)}{2}$ [C, Thm. 5]	[B]
$\mathcal{F}_2$	$((1, 0, 1, 1)_q, (0, 1, 1, 0)_{q^3})$	$q = 2^k$, $0 < k < m$, $\gcd(3k, m) = 1$, m odd.	$\frac{\varphi(m)}{2}$ [C, Thm. 5]	[B]
$\mathcal{F}_4$	$((1, 0, 0, B)_q, (0, 1, \frac{a}{B}, 0)_r)$	$q = 2^k$, $r = 2^{k+m/2}$, $0 < k < m$, $m \equiv 2 \pmod 4$, $\gcd(k, m) = 1$, $a \in \mathbb{K}^\times$, $B \in \mathbb{M}^\times \setminus (\mathbb{M}^\times)^3$, $B^{q+r} \neq a^{q+1}$.	$\geq \frac{\varphi(m)}{2m}(2^{\frac{m}{2}} - 2)$ [C, Cor. 1]	[C, Thm. 1]

Table 6. Known infinite families of biprojective APN functions on $\mathbb{M} \times \mathbb{M}$

Classification of (q,q)-biprojective APN functions

Method

- Boils down to proving that

$$\pi(x) = \frac{f(x,1)}{g(x,1)} = \frac{s}{r}$$

  has a unique solution $x \in \mathbb{P}^1(\mathbb{L})$ for every $s/r \in \mathbb{P}^1(\mathbb{L})$, i.e., $x \mapsto \pi(x)$ is bijective.
- Thus the problem of classifying biprojective APN function has reduced to the classification of fractional projective permutations.

$\mathrm{GL}(2,\mathbb{L})$ and $\mathrm{PGL}(2,\mathbb{L})$

- GL can be viewed as: $(x, y) \mapsto (ax + by, cx + dy)$ such that $ad - bc \neq 0$
- PGL can be viewed as:

  $$x \mapsto \mu(x) = \frac{ax + b}{cx + d},$$

  where $\mu(\infty) = a/c$.
- Recall the (q, q)-biprojective maps are of the form

  $$\begin{aligned}(x, y) \mapsto (a_0 x^q x + b_0 x^q y + c_0 x y^q + d_0 y^q y,\\ a_1 x^q x + b_1 x^q y + c_1 x y^q + d_1 y^q y)\end{aligned}$$

Algebraic degree-2 functions that are homogenous (using both notions of the degree)

Classify

- (q,q)-biprojective functions of the form:

$$\begin{aligned} F : \mathbb{L} \times \mathbb{L} &\to \mathbb{L} \times \mathbb{L} \\ (x,y) &\mapsto (f(x,y), g(x,y)), \end{aligned}$$

  where f and g are q-biprojective polynomials, and

- fractional q-projective functions of the form

$$\begin{aligned} \pi : \mathcal{P}^1(\mathbb{L}) &\to \mathcal{P}^1(\mathbb{L}) \\ x &\mapsto \frac{\phi_f(x)}{\phi_g(x)}, \end{aligned}$$

  where ϕ_f and ϕ_g are q-projective polynomials.

The classification theorem for fractional projective permutations

Theorem

Let $\pi(x)$ *be a fractional q-projective permutation of* $\mathcal{P}^1(\mathbb{L})$ *over a finite field* $\mathbb{L}$. *Then,* $\mathrm{char}(\mathbb{L}) = 2$ *and* $\pi(x)$ *is equivalent to, either*

1.
$$\pi(x) \sim \frac{x^{q+1} + (\epsilon_q + 1)x + \epsilon_2 + \delta + \epsilon_1}{x^q + x + \epsilon_q},$$

   with $\mathrm{tr}_{\mathbb{D}/\mathbb{F}_2}(\epsilon_1) = 1$, *or*

2.
$$\pi(x) \sim \frac{x^{q+1} + (\epsilon_q + 1)x + \epsilon_2 + \delta}{x^q + x + \epsilon_q}.$$

Classification explained

- (The case $[\mathbb{L} : \mathbb{D}]$ is odd.) Then,
  1. π_1 is the *projectivization* of X^j for some $j \in \{q+1, q+r\}$ depending on whether $[\mathbb{K} : \mathbb{D}]$ is odd or even; and
  2. $\pi_2 \sim x^{q+1}$. Note the biprojective version

$$(x, y) \mapsto (x^{q+1}, y^{q+1}).$$

- (The case $[\mathbb{L} : \mathbb{D}]$ is even.) Then, π_1, π_2 are projectivizations of X^j where $j \in \{q+1, q+r\}$.

$$\mathbb{L} = \mathbb{F}_r, \mathbb{K} = \mathbb{F}_q, \mathbb{D} = \mathbb{K} \cap \mathbb{L}$$

More applications in cryptography

1. **Discrete logarithm problem:** Efficient algorithms that solve the discrete logarithm problem on the multiplicative group of a finite field. These algorithms were then employed to **break two records for computing discrete logarithms in largest order finite fields**.
2. Joint work with Robert Granger, Gary McGuire, Jens Zumbrägel (who gave a seminar on this topic last year), and another work with Antoine Joux.

- F. Göloğlu and L. Kölsch, *An exponential bound on the number of non-isotopic commutative semifields*, Trans. Amer. Math. Soc. **376(3)** (2023), 1683–1716.

- F. Göloğlu, *Classification of fractional projective permutations over finite fields*, Finite Fields Appl. **81** (2022), Paper No. 102027, 50 pages.

- F. Göloğlu, *Classification of (q, q)-biprojective APN functions*, IEEE Trans. Inform. Theory **69** (2022), no. 3, 1988–1999.

- F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel, *On the function field sieve and the impact of higher splitting probabilities: application to discrete logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$*, Advances in cryptology—CRYPTO 2013. Part II, LNCS, vol. 8043, Springer, 2013, pp. 109–128.

- F. Göloğlu and A. Joux, *A simplified approach to rigorous degree 2 elimination in discrete logarithm algorithms*, Math. Comp. **88** (2019), no. 319, 2485–2496.

Thanks for your attention.