On the Spread Sets of Planar Dembowski-Ostrom Monomials

BFA 2023, September 03 – 08, 2023

Christof Beierle and Patrick Felke

RUHR UNIVERSITÄT BOCHUM RUB

University of Applied Sciences HOCHSCHULE EMDEN • LEER

Gefördert durch DFG Deutsche Forschungsgemeinschaft

HORST GÖRTZ INSTITUT

CASA CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Dembowski-Ostrom and planar polynomials

Let p be an odd prime and n a positive integer.

Dembowski-Ostrom Polynomial

A polynomial $g \in \mathbb{F}_{p^n}[x]$ is called <u>Dembowski-Ostrom (DO)</u> if
$g(x) = \sum_{0 \le i \le j \le n-1} u_{i,j} \cdot x^{p^i + p^j}, \quad u_{i,j} \in \mathbb{F}_{p^n}$.

Planar Polynomial [Dembowski and Ostrom, '68]

$g \in \mathbb{F}_{p^n}[x]$ is called <u>planar</u> if $\Delta_{g,\alpha}(x) := g(x+\alpha) - g(x) - g(\alpha)$ is a permutation polynomial for all $\alpha \in \mathbb{F}_{p^n}^*$.

- Only a few infinite families of planar polynomials are known
- In this talk, we focus on planar DO monomials, i.e., $g = x^e$.

Equivalence relation between planar polynomials

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

CCZ-equivalence [Carlet, Charpin, Zinoviev, '98]

Two polynomials $g, g' \in \mathbb{F}_{p^n}[x]$ are called equivalent if there is an affine permutation $\mathcal{A}$ over $\mathbb{F}_{p^n}^2$ such that $\{(z, g'(z)) \mid z \in \mathbb{F}_{p^n}\} = \mathcal{A}(\{(z, g(z)) \mid z \in \mathbb{F}_{p^n}\})$.

- CCZ- equivalence preserves the planarity property
- [Budaghyan, Helleseth and Kyureghyan, Pott, '08]: Two planar DO polynomials g, g' are equivalent if and only if there exist linear permutations L_1, L_2 over $\mathbb{F}_{p^n}$ such that

$$g'(z) = L_2(g(L_1(z))), \forall z \in \mathbb{F}_{p^n}.$$

Problem

Efficiently decide the equivalence between two planar (DO) polynomials.

Equivalence relation between planar polynomials

CCZ-equivalence [Carlet, Charpin, Zinoviev, '98]

Two polynomials $g, g' \in \mathbb{F}_{p^n}[x]$ are called equivalent if there is an affine permutation $\mathcal{A}$ over $\mathbb{F}_{p^n}^2$ such that $\{(z, g'(z)) \mid z \in \mathbb{F}_{p^n}\} = \mathcal{A}(\{(z, g(z)) \mid z \in \mathbb{F}_{p^n}\})$.

- CCZ- equivalence preserves the planarity property
- [Budaghyan, Helleseth and Kyureghyan, Pott, '08]: Two planar DO polynomials g, g' are equivalent if and only if there exist linear permutations L_1, L_2 over $\mathbb{F}_{p^n}$ such that

$$g'(z) = L_2(g(L_1(z))), \forall z \in \mathbb{F}_{p^n}.$$

Problem

Efficiently decide the equivalence between two planar (DO) polynomials.

Special case: Planar monomials

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Theorem: Classification of planar DO monomials [Coulter, Matthews, '97]

A DO monomial $x^e \in \mathbb{F}_{p^n}[x]$ is planar if and only if $e = p^\ell(p^k + 1)$ with $n/\gcd(k, n)$ being odd.

- The above description uses the characterization of CCZ-equivalent monomials from [Dempwolff, 2018]. Up to equivalence, w.l.o.g., we can assume $p^\ell = 1$.
- For $k = 0$, we get the planar monomial x^2.
- We know only one family of planar monomials that is not DO ([Coulter, Matthews, '97]). The general classification of planar monomials is open.

Planar DO polynomials and commutative semifields

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

[Coulter, Henderson, 2008]: Correspondence between commutative semifields (i.e., "fields without associativity") and planar DO polynomials.

- If g is DO, $\Delta_{g,\alpha}(x) := g(x+\alpha) - g(x) - g(\alpha)$ is a linearized polynomial
- If g is planar and DO, $\Delta_{g,\alpha}(x)$ corresponds to the mapping $x \mapsto \alpha \star x$ of left-multiplication with α in the corresponding commutative presemifield $\mathcal{R}_g$
- The set $\{x \mapsto \alpha \star x \mid \alpha \in \mathbb{F}_{p^n}\}$ is called the spread set of $\mathcal{R}_g$

Definition (Spread set of g)

For a planar DO polynomial $g \in \mathbb{F}_{p^n}[x]$, let us denote by $M_{g,\alpha}$ the $n \times n$ matrix over $\mathbb{F}_p$ associated to the evaluation map of $\Delta_{g,\alpha}$. We define the spread set of g as

$$\mathcal{D}_g := \{M_{g,\alpha} \mid \alpha \in \mathbb{F}_{p^n}\} \subseteq \mathrm{GL}(n, \mathbb{F}_p) \cup \{0\}.$$

Planar DO polynomials and commutative semifields

[Coulter, Henderson, 2008]: Correspondence between commutative semifields (i.e., "fields without associativity") and planar DO polynomials.

- If g is DO, $\Delta_{g,\alpha}(x) := g(x+\alpha) - g(x) - g(\alpha)$ is a linearized polynomial
- If g is planar and DO, $\Delta_{g,\alpha}(x)$ corresponds to the mapping $x \mapsto \alpha \star x$ of left-multiplication with α in the corresponding commutative presemifield $\mathcal{R}_g$
- The set $\{x \mapsto \alpha \star x \mid \alpha \in \mathbb{F}_{p^n}\}$ is called the spread set of $\mathcal{R}_g$

Definition (Spread set of g)

For a planar DO polynomial $g \in \mathbb{F}_{p^n}[x]$, let us denote by $M_{g,\alpha}$ the $n \times n$ matrix over $\mathbb{F}_p$ associated to the evaluation map of $\Delta_{g,\alpha}$. We define the spread set of g as

$$\mathcal{D}_g := \{M_{g,\alpha} \mid \alpha \in \mathbb{F}_{p^n}\} \subseteq \mathrm{GL}(n, \mathbb{F}_p) \cup \{0\}.$$

Planar DO polynomials and commutative semifields

[Coulter, Henderson, 2008]: Correspondence between commutative semifields (i.e., "fields without associativity") and planar DO polynomials.

- If g is DO, $\Delta_{g,\alpha}(x) := g(x+\alpha) - g(x) - g(\alpha)$ is a linearized polynomial
- If g is planar and DO, $\Delta_{g,\alpha}(x)$ corresponds to the mapping $x \mapsto \alpha \star x$ of left-multiplication with α in the corresponding commutative presemifield $\mathcal{R}_g$
- The set $\{x \mapsto \alpha \star x \mid \alpha \in \mathbb{F}_{p^n}\}$ is called the spread set of $\mathcal{R}_g$

Definition (Spread set of g)

For a planar DO polynomial $g \in \mathbb{F}_{p^n}[x]$, let us denote by $M_{g,\alpha}$ the $n \times n$ matrix over $\mathbb{F}_p$ associated to the evaluation map of $\Delta_{g,\alpha}$. We define the spread set of g as

$$\mathcal{D}_g := \{M_{g,\alpha} \mid \alpha \in \mathbb{F}_{p^n}\} \subseteq \mathrm{GL}(n, \mathbb{F}_p) \cup \{0\}.$$

Quotient of the spread set

$$\mathcal{D}_g := \{M_{g,\alpha} \mid \alpha \in \mathbb{F}_{p^n}\} \subseteq \mathrm{GL}(n, \mathbb{F}_p) \cup \{0\}$$

Question

Can we exploit some structure in the spread sets to efficiently decide (in)equivalence between planar DO polynomials?

- Problem: The spread set is not invariant under equivalence. If g, g' are equivalent, we have $\mathcal{D}_{g'} = A^{-1} \cdot \mathcal{D}_g \cdot B$ for some $A, B \in \mathrm{GL}(n, \mathbb{F}_p)$ (see [Dempwolff, 2008])

Definition (Quotients in the spread set)

For a planar DO polynomial g, we define

$$\mathrm{Quot}(\mathcal{D}_g) := \{XY^{-1} \mid X, Y \in \mathcal{D}_g \text{ and } Y \neq 0\}.$$

Quotient of the spread set

$$\mathcal{D}_g := \{M_{g,\alpha} \mid \alpha \in \mathbb{F}_{p^n}\} \subseteq \mathrm{GL}(n, \mathbb{F}_p) \cup \{0\}$$

Question

Can we exploit some structure in the spread sets to efficiently decide (in)equivalence between planar DO polynomials?

- Problem: The spread set is not invariant under equivalence. If g, g' are equivalent, we have $\mathcal{D}_{g'} = A^{-1} \cdot \mathcal{D}_g \cdot B$ for some $A, B \in \mathrm{GL}(n, \mathbb{F}_p)$ (see [Dempwolff, 2008])

Definition (Quotients in the spread set)

For a planar DO polynomial g, we define

$$\mathrm{Quot}(\mathcal{D}_g) := \{XY^{-1} \mid X, Y \in \mathcal{D}_g \text{ and } Y \neq 0\}.$$

Quotient of the spread set

$$\mathcal{D}_g := \{M_{g,\alpha} \mid \alpha \in \mathbb{F}_{p^n}\} \subseteq \mathrm{GL}(n, \mathbb{F}_p) \cup \{0\}$$

Question

Can we exploit some structure in the spread sets to efficiently decide (in)equivalence between planar DO polynomials?

- Problem: The spread set is not invariant under equivalence. If g, g' are equivalent, we have $\mathcal{D}_{g'} = A^{-1} \cdot \mathcal{D}_g \cdot B$ for some $A, B \in \mathrm{GL}(n, \mathbb{F}_p)$ (see [Dempwolff, 2008])

Definition (Quotients in the spread set)

For a planar DO polynomial g, we define

$$\mathrm{Quot}(\mathcal{D}_g) := \{XY^{-1} \mid X, Y \in \mathcal{D}_g \text{ and } Y \neq 0\}.$$

Properties of $\mathrm{Quot}(\mathcal{D}_g)$

$$\mathrm{Quot}(\mathcal{D}_g) := \{XY^{-1} \mid X, Y \in \mathcal{D}_g \text{ and } Y \neq 0\}$$

- Invariant (up to a choice of basis) under equivalence of g, i.e., for equivalent DO planar polynomials g, g', we have $\mathrm{Quot}(\mathcal{D}_{g'}) = A^{-1} \cdot \mathrm{Quot}(\mathcal{D}_g) \cdot A$ for $A \in \mathrm{GL}(n, \mathbb{F}_p)$.
- Since the evaluation map of $\Delta_{g,\alpha}$ is $\mathbb{F}_p$-linear, $\mathrm{Quot}(\mathcal{D}_g)$ contains the field $\mathbb{F}_p$ viz., $\{M_{g,c}M_{g,1}^{-1} \mid c \in \mathbb{F}_p\} = \{c \cdot M_{g,1}M_{g,1}^{-1} \mid c \in \mathbb{F}_p\} = \mathbb{F}_p$

Question

Can we identify some non-trivial algebraic structure in $\mathrm{Quot}(\mathcal{D}_g)$?

The structure of $\mathrm{Quot}(\mathcal{D}_{x^2})$

- We have $\Delta_{g,\alpha}(x) = g(x+\alpha) - g(x) - g(\alpha) = 2\alpha x$
- $g(x) = x^2$ corresponds (as a commutative semifield) to a finite field

Theorem (B., 2022, see invited talk BFA 2022 and our preprint)

Let $g \in \mathbb{F}_{p^n}[x]$ be planar and DO. Then, $\mathrm{Quot}(\mathcal{D}_g)$ is a field isomorphic to $\mathbb{F}_{p^n}$ if and only if g is equivalent to x^2.

- In particular, $|\mathrm{Quot}(\mathcal{D}_{x^2})| = p^n$
- Can be used to decide equivalence to x^2 very fast (see our preprint):

Theorem (B., Felke, 2022)

$\mathrm{Quot}(\mathcal{D}_g)$ being a field of order p^n can be decided using $\mathcal{O}(n^7 \log(p))$ elementary operations in $\mathbb{F}_p$ and $\mathcal{O}(n^2)$ evaluations of g.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^2})$

- We have $\Delta_{g,\alpha}(x) = g(x+\alpha) - g(x) - g(\alpha) = 2\alpha x$
- $g(x) = x^2$ corresponds (as a commutative semifield) to a finite field

Theorem (B., 2022, see invited talk BFA 2022 and our preprint)

Let $g \in \mathbb{F}_{p^n}[x]$ be planar and DO. Then, $\mathrm{Quot}(\mathcal{D}_g)$ is a field isomorphic to $\mathbb{F}_{p^n}$ if and only if g is equivalent to x^2.

- In particular, $|\mathrm{Quot}(\mathcal{D}_{x^2})| = p^n$
- Can be used to decide equivalence to x^2 very fast (see our preprint):

Theorem (B., Felke, 2022)

$\mathrm{Quot}(\mathcal{D}_g)$ being a field of order p^n can be decided using $\mathcal{O}(n^7 \log(p))$ elementary operations in $\mathbb{F}_p$ and $\mathcal{O}(n^2)$ evaluations of g.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$

- For $A \in \mathrm{GL}(n, \mathbb{F}_p)$, let $\mathbb{F}_p[A] := \{\sum_i a_i A^i \mid a_i \in \mathbb{F}_p\}$ denote the matrix algebra generated by A
- $\mathbb{F}_p[A]$ is a field isomorphic to $\mathbb{F}_p(\gamma)$ if and only if $A = B^{-1} T_\gamma B$ for $B \in \mathrm{GL}(n, \mathbb{F}_p)$ and T_γ corresponding to the linear map $x \mapsto \gamma x$

Main Theorem

Let $g = x^{p^k+1} \in \mathbb{F}_{p^n}[x]$ be a planar DO monomial. For any $\alpha, \beta \in \mathbb{F}_{p^n}^*$, the element $A := M_{g,\beta} M_{g,\alpha}^{-1} \in \mathrm{Quot}(\mathcal{D}_g)$ generates a field isomorphic to $\mathbb{F}_p(\alpha^{-1}\beta)$ viz. $\mathbb{F}_p[A]$, and $\mathbb{F}_p[A] \subseteq \mathrm{Quot}(\mathcal{D}_g)$.

- In particular, $\mathrm{Quot}(\mathcal{D}_g)$ contains $(p^n - 1)/(p^{\gcd(k,n)-1})$ copies of fields isomorphic to $\mathbb{F}_{p^n}$, all intersecting in $\mathbb{F}_{p^{\gcd(k,n)}}$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$

- For $A \in \mathrm{GL}(n, \mathbb{F}_p)$, let $\mathbb{F}_p[A] := \{\sum_i a_i A^i \mid a_i \in \mathbb{F}_p\}$ denote the matrix algebra generated by A
- $\mathbb{F}_p[A]$ is a field isomorphic to $\mathbb{F}_p(\gamma)$ if and only if $A = B^{-1} T_\gamma B$ for $B \in \mathrm{GL}(n, \mathbb{F}_p)$ and T_γ corresponding to the linear map $x \mapsto \gamma x$

Main Theorem

Let $g = x^{p^k+1} \in \mathbb{F}_{p^n}[x]$ be a planar DO monomial. For any $\alpha, \beta \in \mathbb{F}_{p^n}^*$, the element $A := M_{g,\beta} M_{g,\alpha}^{-1} \in \mathrm{Quot}(\mathcal{D}_g)$ generates a field isomorphic to $\mathbb{F}_p(\alpha^{-1}\beta)$ viz. $\mathbb{F}_p[A]$, and $\mathbb{F}_p[A] \subseteq \mathrm{Quot}(\mathcal{D}_g)$.

- In particular, $\mathrm{Quot}(\mathcal{D}_g)$ contains $(p^n - 1)/(p^{\gcd(k,n)-1})$ copies of fields isomorphic to $\mathbb{F}_{p^n}$, all intersecting in $\mathbb{F}_{p^{\gcd(k,n)}}$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Let $g = x^{p^k+1} \in \mathbb{F}_{p^n}[x]$ be planar and $\alpha, \beta \in \mathbb{F}_p^*$. Let $A := M_{g,\beta} M_{g,\alpha}^{-1}$. We need to show the following:

1. $\mathbb{F}_p[A]$ is isomorphic to $\mathbb{F}_p(\alpha^{-1}\beta)$, i.e., $A = B^{-1} T_{\alpha^{-1}\beta} B$ for some $B \in \mathrm{GL}(n, \mathbb{F}_p)$
2. $\mathbb{F}_p[A] \subseteq \mathrm{Quot}(\mathcal{D}_g)$

(Note: We will use matrices and their corresponding linear maps over $\mathbb{F}_{p^n}$ interchangeably)

Lemma

$M_{g,\beta}$ corresponds to the $\mathbb{F}_{p^{\gcd(k,n)}}$-linear map $x \mapsto \beta x^{p^k} + \beta^{p^k} x$.
A corresponds to the $\mathbb{F}_{p^{\gcd(k,n)}}$-linear map $x \mapsto (\beta^{p^k} - \alpha^{p^k-1}\beta) \cdot M_{g,\alpha}^{-1}(x) + \alpha^{-1}\beta x$.

- This implies that, if $\alpha^{-1}\beta \in \mathbb{F}_{p^{\gcd(k,n)}}$, we have $A(x) = \alpha^{-1}\beta \cdot x$, i.e., $A = T_{\alpha^{-1}\beta}$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

Let $g = x^{p^k+1} \in \mathbb{F}_{p^n}[x]$ be planar and $\alpha, \beta \in \mathbb{F}_p^*$. Let $A := M_{g,\beta} M_{g,\alpha}^{-1}$. We need to show the following:

1. $\mathbb{F}_p[A]$ is isomorphic to $\mathbb{F}_p(\alpha^{-1}\beta)$, i.e., $A = B^{-1} T_{\alpha^{-1}\beta} B$ for some $B \in \mathrm{GL}(n, \mathbb{F}_p)$
2. $\mathbb{F}_p[A] \subseteq \mathrm{Quot}(\mathcal{D}_g)$

(Note: We will use matrices and their corresponding linear maps over $\mathbb{F}_{p^n}$ interchangeably)

Lemma

$M_{g,\beta}$ corresponds to the $\mathbb{F}_{p^{\gcd(k,n)}}$-linear map $x \mapsto \beta x^{p^k} + \beta^{p^k} x$.
A corresponds to the $\mathbb{F}_{p^{\gcd(k,n)}}$-linear map $x \mapsto (\beta^{p^k} - \alpha^{p^k-1}\beta) \cdot M_{g,\alpha}^{-1}(x) + \alpha^{-1}\beta x$.

- This implies that, if $\alpha^{-1}\beta \in \mathbb{F}_{p^{\gcd(k,n)}}$, we have $A(x) = \alpha^{-1}\beta \cdot x$, i.e., $A = T_{\alpha^{-1}\beta}$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Lemma

Let $\alpha^{-1}\beta \notin \mathbb{F}_{p^{\gcd(k,n)}}$, then there is a linear mapping $\psi_{\alpha,\beta}$ such that $x \mapsto \psi_{\alpha,\beta} \circ A \circ \psi^{-1}_{\alpha,\beta}(x)$ equals $x \mapsto (\alpha^{-1}\beta)^{p^k} x$. More precisely,

$$\psi_{\alpha,\beta} \colon x \mapsto \alpha^{p^k} \cdot M_{g,\alpha}\left(\frac{1}{\beta^{p^k} - \alpha^{p^k-1}\beta} \cdot x\right).$$

- Hence, for $\alpha^{-1}\beta \notin \mathbb{F}_{p^{\gcd(k,n)}}$, we have $A = B^{-1} T_{(\alpha^{-1}\beta)^{p^k}} B$ for some $B \in \mathrm{GL}(n, \mathbb{F}_p)$. Since a Frobenius automorphism corresponds to a change of basis, we have $A = C^{-1} T_{\alpha^{-1}\beta} C$
- This completes the proof of 1.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Lemma

Let $\alpha^{-1}\beta \notin \mathbb{F}_{p^{\gcd(k,n)}}$, then there is a linear mapping $\psi_{\alpha,\beta}$ such that $x \mapsto \psi_{\alpha,\beta} \circ A \circ \psi_{\alpha,\beta}^{-1}(x)$ equals $x \mapsto (\alpha^{-1}\beta)^{p^k} x$. More precisely,

$$\psi_{\alpha,\beta} \colon x \mapsto \alpha^{p^k} \cdot M_{g,\alpha}\left(\frac{1}{\beta^{p^k} - \alpha^{p^k-1}\beta} \cdot x\right).$$

- Hence, for $\alpha^{-1}\beta \notin \mathbb{F}_{p^{\gcd(k,n)}}$, we have $A = B^{-1} T_{(\alpha^{-1}\beta)^{p^k}} B$ for some $B \in \mathrm{GL}(n, \mathbb{F}_p)$. Since a Frobenius automorphism corresponds to a change of basis, we have $A = C^{-1} T_{\alpha^{-1}\beta} C$
- This completes the proof of 1.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

- Left to show: $\mathbb{F}_p[A] \subseteq \mathrm{Quot}(\mathcal{D}_g)$
- Proof idea: Focus on $\alpha = 1, \beta \notin \mathbb{F}_{p^{\gcd(k,n)}}$. Show that $(M_{g,\beta} M_{g,1}^{-1})^r \in \mathrm{Quot}(\mathcal{D}_g)$.
- From the previous lemma, on can deduce

$$\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \begin{cases} \psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r} \circ M_{g,\beta^r} \circ M_{g,1}^{-1} \circ \psi_{1,\beta^r}^{-1} \circ \psi_{1,\beta} & \text{if } \beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}} \\ \psi_{1,\beta}^{-1} \circ M_{g,\beta^r} \circ M_{g,1}^{-1} \circ \psi_{1,\beta} & \text{otherwise} \end{cases}$$

- In case $\beta^r \in \mathbb{F}_{p^{\gcd(k,n)}}$, we get the left-hand side equal to $M_{g,\beta^r} \circ M_{g,1}^{-1}$ from the $\mathbb{F}_{p^{\gcd(k,n)}}$-linearity of $\psi_{1,\beta}$.
- In case $\beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}}$, the mapping $\psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r}$ is equal to $x \mapsto \lambda x$ for $\lambda \in \mathbb{F}_{p^n}^*$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

- Left to show: $\mathbb{F}_p[A] \subseteq \mathrm{Quot}(\mathcal{D}_g)$
- Proof idea: Focus on $\alpha = 1, \beta \notin \mathbb{F}_{p^{\gcd(k,n)}}$. Show that $(M_{g,\beta} M_{g,1}^{-1})^r \in \mathrm{Quot}(\mathcal{D}_g)$.
- From the previous lemma, on can deduce

$$\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \begin{cases} \psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r} \circ M_{g,\beta^r} \circ M_{g,1}^{-1} \circ \psi_{1,\beta^r}^{-1} \circ \psi_{1,\beta} & \text{if } \beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}} \\ \psi_{1,\beta}^{-1} \circ M_{g,\beta^r} \circ M_{g,1}^{-1} \circ \psi_{1,\beta} & \text{otherwise} \end{cases}$$

- In case $\beta^r \in \mathbb{F}_{p^{\gcd(k,n)}}$, we get the left-hand side equal to $M_{g,\beta^r} \circ M_{g,1}^{-1}$ from the $\mathbb{F}_{p^{\gcd(k,n)}}$-linearity of $\psi_{1,\beta}$.
- In case $\beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}}$, the mapping $\psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r}$ is equal to $x \mapsto \lambda x$ for $\lambda \in \mathbb{F}_{p^n}^*$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

- Left to show: $\mathbb{F}_p[A] \subseteq \mathrm{Quot}(\mathcal{D}_g)$
- Proof idea: Focus on $\alpha = 1, \beta \notin \mathbb{F}_{p^{\gcd(k,n)}}$. Show that $(M_{g,\beta} M_{g,1}^{-1})^r \in \mathrm{Quot}(\mathcal{D}_g)$.
- From the previous lemma, on can deduce

$$\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \begin{cases} \psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r} \circ M_{g,\beta^r} \circ M_{g,1}^{-1} \circ \psi_{1,\beta^r}^{-1} \circ \psi_{1,\beta} & \text{if } \beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}} \\ \psi_{1,\beta}^{-1} \circ M_{g,\beta^r} \circ M_{g,1}^{-1} \circ \psi_{1,\beta} & \text{otherwise} \end{cases}$$

- In case $\beta^r \in \mathbb{F}_{p^{\gcd(k,n)}}$, we get the left-hand side equal to $M_{g,\beta^r} \circ M_{g,1}^{-1}$ from the $\mathbb{F}_{p^{\gcd(k,n)}}$-linearity of $\psi_{1,\beta}$.
- In case $\beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}}$, the mapping $\psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r}$ is equal to $x \mapsto \lambda x$ for $\lambda \in \mathbb{F}_{p^n}^*$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

- Left to show: $\mathbb{F}_p[A] \subseteq \mathrm{Quot}(\mathcal{D}_g)$
- Proof idea: Focus on $\alpha = 1, \beta \notin \mathbb{F}_{p^{\gcd(k,n)}}$. Show that $(M_{g,\beta}M_{g,1}^{-1})^r \in \mathrm{Quot}(\mathcal{D}_g)$.
- From the previous lemma, on can deduce

$$\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \begin{cases} \psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r} \circ M_{g,\beta^r} \circ M_{g,1}^{-1} \circ \psi_{1,\beta^r}^{-1} \circ \psi_{1,\beta} & \text{if } \beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}} \\ \psi_{1,\beta}^{-1} \circ M_{g,\beta^r} \circ M_{g,1}^{-1} \circ \psi_{1,\beta} & \text{otherwise} \end{cases}$$

- In case $\beta^r \in \mathbb{F}_{p^{\gcd(k,n)}}$, we get the left-hand side equal to $M_{g,\beta^r} \circ M_{g,1}^{-1}$ from the $\mathbb{F}_{p^{\gcd(k,n)}}$-linearity of $\psi_{1,\beta}$.
- In case $\beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}}$, the mapping $\psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r}$ is equal to $x \mapsto \lambda x$ for $\lambda \in \mathbb{F}_{p^n}^*$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

- Left to show: $\mathbb{F}_p[A] \subseteq \mathrm{Quot}(\mathcal{D}_g)$
- Proof idea: Focus on $\alpha = 1, \beta \notin \mathbb{F}_{p^{\gcd(k,n)}}$. Show that $(M_{g,\beta} M_{g,1}^{-1})^r \in \mathrm{Quot}(\mathcal{D}_g)$.
- From the previous lemma, on can deduce

$$\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \begin{cases} \psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r} \circ M_{g,\beta^r} \circ M_{g,1}^{-1} \circ \psi_{1,\beta^r}^{-1} \circ \psi_{1,\beta} & \text{if } \beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}} \\ \psi_{1,\beta}^{-1} \circ M_{g,\beta^r} \circ M_{g,1}^{-1} \circ \psi_{1,\beta} & \text{otherwise} \end{cases}$$

- In case $\beta^r \in \mathbb{F}_{p^{\gcd(k,n)}}$, we get the left-hand side equal to $M_{g,\beta^r} \circ M_{g,1}^{-1}$ from the $\mathbb{F}_{p^{\gcd(k,n)}}$-linearity of $\psi_{1,\beta}$.
- In case $\beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}}$, the mapping $\psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r}$ is equal to $x \mapsto \lambda x$ for $\lambda \in \mathbb{F}_{p^n}^*$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

- Hence, in this case, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \lambda \cdot (M_{g,\beta^r} \circ M_{g,1}^{-1})(\lambda^{-1}x)$

Lemma

If $n/\gcd(k,n)$ is odd, $\lambda \in \mathbb{F}_{p^n}^*$ can be written as $u\gamma^{p^k+1}$ for $\gamma \in \mathbb{F}_{p^n}^*$, $u \in \mathbb{F}_{p^{\gcd(k,n)}}^*$.

- Hence, in this case, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \gamma^{p^k+1} \cdot (M_{g,\beta^r} \circ M_{g,1}^{-1})(\gamma^{-(p^k+1)}x)$ from the $\mathbb{F}_{p^{\gcd(k,n)}}$-linearity of M_{g,β^r} and $M_{g,1}$.

Lemma

For any $\gamma \in \mathbb{F}_{p^n}^*$, we have $M_{g,\beta}M_{g,\alpha}^{-1}(x) = \gamma^{-(p^k+1)}M_{g,\gamma\beta}M_{g,\gamma\alpha}^{-1}(\gamma^{p^k+1}x)$

- This comes from the fact that $g(\gamma x) = \gamma^{p^k+1}g(x)$.
- Hence, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = M_{g,\gamma\beta^r} \circ M_{g,\gamma}^{-1}$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Hence, in this case, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \lambda \cdot (M_{g,\beta^r} \circ M_{g,1}^{-1})(\lambda^{-1}x)$

Lemma

If $n/\gcd(k,n)$ is odd, $\lambda \in \mathbb{F}_{p^n}^*$ can be written as $u\gamma^{p^k+1}$ for $\gamma \in \mathbb{F}_{p^n}^*$, $u \in \mathbb{F}_{p^{\gcd(k,n)}}^*$.

- Hence, in this case, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \gamma^{p^k+1} \cdot (M_{g,\beta^r} \circ M_{g,1}^{-1})(\gamma^{-(p^k+1)}x)$ from the $\mathbb{F}_{p^{\gcd(k,n)}}$-linearity of M_{g,β^r} and $M_{g,1}$.

Lemma

For any $\gamma \in \mathbb{F}_{p^n}^*$, we have $M_{g,\beta}M_{g,\alpha}^{-1}(x) = \gamma^{-(p^k+1)}M_{g,\gamma\beta}M_{g,\gamma\alpha}^{-1}(\gamma^{p^k+1}x)$

- This comes from the fact that $g(\gamma x) = \gamma^{p^k+1}g(x)$.
- Hence, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = M_{g,\gamma\beta^r} \circ M_{g,\gamma}^{-1}$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

- Hence, in this case, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \lambda \cdot (M_{g,\beta^r} \circ M_{g,1}^{-1})(\lambda^{-1}x)$

Lemma

If $n/\gcd(k,n)$ is odd, $\lambda \in \mathbb{F}_{p^n}^*$ can be written as $u\gamma^{p^k+1}$ for $\gamma \in \mathbb{F}_{p^n}^*$, $u \in \mathbb{F}_{p^{\gcd(k,n)}}^*$.

- Hence, in this case, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \gamma^{p^k+1} \cdot (M_{g,\beta^r} \circ M_{g,1}^{-1})(\gamma^{-(p^k+1)}x)$ from the $\mathbb{F}_{p^{\gcd(k,n)}}$-linearity of M_{g,β^r} and $M_{g,1}$.

Lemma

For any $\gamma \in \mathbb{F}_{p^n}^*$, we have $M_{g,\beta}M_{g,\alpha}^{-1}(x) = \gamma^{-(p^k+1)}M_{g,\gamma\beta}M_{g,\gamma\alpha}^{-1}(\gamma^{p^k+1}x)$

- This comes from the fact that $g(\gamma x) = \gamma^{p^k+1}g(x)$.
- Hence, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = M_{g,\gamma\beta^r} \circ M_{g,\gamma}^{-1}$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

- Hence, in this case, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \lambda \cdot (M_{g,\beta^r} \circ M_{g,1}^{-1})(\lambda^{-1}x)$

Lemma

If $n/\gcd(k,n)$ is odd, $\lambda \in \mathbb{F}_{p^n}^*$ can be written as $u\gamma^{p^k+1}$ for $\gamma \in \mathbb{F}_{p^n}^*$, $u \in \mathbb{F}_{p^{\gcd(k,n)}}^*$.

- Hence, in this case, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \gamma^{p^k+1} \cdot (M_{g,\beta^r} \circ M_{g,1}^{-1})(\gamma^{-(p^k+1)}x)$ from the $\mathbb{F}_{p^{\gcd(k,n)}}$-linearity of M_{g,β^r} and $M_{g,1}$.

Lemma

For any $\gamma \in \mathbb{F}_{p^n}^*$, we have $M_{g,\beta}M_{g,\alpha}^{-1}(x) = \gamma^{-(p^k+1)}M_{g,\gamma\beta}M_{g,\gamma\alpha}^{-1}(\gamma^{p^k+1}x)$

- This comes from the fact that $g(\gamma x) = \gamma^{p^k+1}g(x)$.
- Hence, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = M_{g,\gamma\beta^r} \circ M_{g,\gamma}^{-1}$.

The structure of $\mathrm{Quot}(\mathcal{D}_{x^{p^k+1}})$ (cont.)

- Hence, in this case, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \lambda \cdot (M_{g,\beta^r} \circ M_{g,1}^{-1})(\lambda^{-1}x)$

Lemma

If $n/\gcd(k,n)$ is odd, $\lambda \in \mathbb{F}_{p^n}^*$ can be written as $u\gamma^{p^k+1}$ for $\gamma \in \mathbb{F}_{p^n}^*$, $u \in \mathbb{F}_{p^{\gcd(k,n)}}^*$.

- Hence, in this case, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = \gamma^{p^k+1} \cdot (M_{g,\beta^r} \circ M_{g,1}^{-1})(\gamma^{-(p^k+1)}x)$ from the $\mathbb{F}_{p^{\gcd(k,n)}}$-linearity of M_{g,β^r} and $M_{g,1}$.

Lemma

For any $\gamma \in \mathbb{F}_{p^n}^*$, we have $M_{g,\beta}M_{g,\alpha}^{-1}(x) = \gamma^{-(p^k+1)}M_{g,\gamma\beta}M_{g,\gamma\alpha}^{-1}(\gamma^{p^k+1}x)$

- This comes from the fact that $g(\gamma x) = \gamma^{p^k+1}g(x)$.
- Hence, $\left(M_{g,\beta} \circ M_{g,1}^{-1}\right)^r = M_{g,\gamma\beta^r} \circ M_{g,\gamma}^{-1}$.

Conclusion

- $\mathrm{Quot}(\mathcal{D}_g) := \{XY^{-1} \mid X, Y \in \mathcal{D}_g \text{ and } Y \neq 0\}$ is an invariant (up to choice of basis) for (CCZ)-equivalence of planar DO polynomials
- $\mathrm{Quot}(\mathcal{D}_g)$ is the finite field $\mathbb{F}_{p^n}$ if and only if g is equivalent to x^2 (can be used for a polynomial-time test against equivalence of g to x^2)
- If g is equivalent to a planar DO monomial, $\mathrm{Quot}(\mathcal{D}_g)$ contains copie(s) of the field $\mathbb{F}_{p^n}$ (can be used to quickly establish inequivalence to a monomial in some cases):

Corollary

If g is equivalent to a planar DO monomial, then each element $M_{g,\beta}M_{g,\alpha}^{-1}$ for $\alpha \neq 0$ has an irreducible minimal polynomial.

Open Question

Can we develop an efficient test against equivalence to a planar DO monomial?

Conclusion

- $\mathrm{Quot}(\mathcal{D}_g) := \{XY^{-1} \mid X, Y \in \mathcal{D}_g$ and $Y \neq 0\}$ is an invariant (up to choice of basis) for (CCZ)-equivalence of planar DO polynomials
- $\mathrm{Quot}(\mathcal{D}_g)$ is the finite field $\mathbb{F}_{p^n}$ if and only if g is equivalent to x^2 (can be used for a polynomial-time test against equivalence of g to x^2)
- If g is equivalent to a planar DO monomial, $\mathrm{Quot}(\mathcal{D}_g)$ contains copie(s) of the field $\mathbb{F}_{p^n}$ (can be used to quickly establish inequivalence to a monomial in some cases):

Corollary

If g is equivalent to a planar DO monomial, then each element $M_{g,\beta}M_{g,\alpha}^{-1}$ for $\alpha \neq 0$ has an irreducible minimal polynomial.

Open Question

Can we develop an efficient test against equivalence to a planar DO monomial?

Conclusion

- $\mathrm{Quot}(\mathcal{D}_g) := \{XY^{-1} \mid X, Y \in \mathcal{D}_g \text{ and } Y \neq 0\}$ is an invariant (up to choice of basis) for (CCZ)-equivalence of planar DO polynomials
- $\mathrm{Quot}(\mathcal{D}_g)$ is the finite field $\mathbb{F}_{p^n}$ if and only if g is equivalent to x^2 (can be used for a polynomial-time test against equivalence of g to x^2)
- If g is equivalent to a planar DO monomial, $\mathrm{Quot}(\mathcal{D}_g)$ contains copie(s) of the field $\mathbb{F}_{p^n}$ (can be used to quickly establish inequivalence to a monomial in some cases):

Corollary

If g is equivalent to a planar DO monomial, then each element $M_{g,\beta}M_{g,\alpha}^{-1}$ for $\alpha \neq 0$ has an irreducible minimal polynomial.

Open Question

Can we develop an efficient test against equivalence to a planar DO monomial?

Conclusion

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- $\mathrm{Quot}(\mathcal{D}_g) := \{XY^{-1} \mid X, Y \in \mathcal{D}_g$ and $Y \neq 0\}$ is an invariant (up to choice of basis) for (CCZ)-equivalence of planar DO polynomials
- $\mathrm{Quot}(\mathcal{D}_g)$ is the finite field $\mathbb{F}_{p^n}$ if and only if g is equivalent to x^2 (can be used for a polynomial-time test against equivalence of g to x^2)
- If g is equivalent to a planar DO monomial, $\mathrm{Quot}(\mathcal{D}_g)$ contains copie(s) of the field $\mathbb{F}_{p^n}$ (can be used to quickly establish inequivalence to a monomial in some cases):

Corollary

If g is equivalent to a planar DO monomial, then each element $M_{g,\beta}M_{g,\alpha}^{-1}$ for $\alpha \neq 0$ has an irreducible minimal polynomial.

Open Question

Can we develop an efficient test against equivalence to a planar DO monomial?

Conclusion

- $\mathrm{Quot}(\mathcal{D}_g) := \{XY^{-1} \mid X, Y \in \mathcal{D}_g$ and $Y \neq 0\}$ is an invariant (up to choice of basis) for (CCZ)-equivalence of planar DO polynomials
- $\mathrm{Quot}(\mathcal{D}_g)$ is the finite field $\mathbb{F}_{p^n}$ if and only if g is equivalent to x^2 (can be used for a polynomial-time test against equivalence of g to x^2)
- If g is equivalent to a planar DO monomial, $\mathrm{Quot}(\mathcal{D}_g)$ contains copie(s) of the field $\mathbb{F}_{p^n}$ (can be used to quickly establish inequivalence to a monomial in some cases):

Corollary

If g is equivalent to a planar DO monomial, then each element $M_{g,\beta}M_{g,\alpha}^{-1}$ for $\alpha \neq 0$ has an irreducible minimal polynomial.

Open Question

Can we develop an efficient test against equivalence to a planar DO monomial?