On the Spread Sets of Planar Dembowski-Ostrom Monomials*

Christof Beierle[1] and Patrick Felke[2]

[1]Faculty of Computer Science, Ruhr University Bochum, Bochum, Germany
[2]University of Applied Sciences Emden-Leer, Emden, Germany

Abstract

Let $g \in \mathbb{F}_{p^n}[x]$ be a planar Dembowski-Ostrom (DO) polynomial, where p is an odd prime and n a positive integer. Let $\mathrm{Quot}(\mathcal{D}_g)$ be the set of quotients XY^{-1} with $Y \neq 0, X$ being elements from the spread set of the commutative presemifield corresponding to g. We analyze the algebraic structure of $\mathrm{Quot}(\mathcal{D}_g)$ for all planar DO *monomials*. More precisely, for g being CCZ-equivalent to a planar DO monomial, we show that every non-zero element $X \in \mathrm{Quot}(\mathcal{D}_g)$ generates a field $\mathbb{F}_p[X] \subseteq \mathrm{Quot}(\mathcal{D}_g)$. In particular, $\mathrm{Quot}(\mathcal{D}_g)$ contains the field $\mathbb{F}_{p^n}$.

1 Introduction and Preliminaries

Let p be an odd prime and n a positive integer. By $\mathrm{Mat}_{\mathbb{F}_p}(n,n)$, we denote the ring of all $n \times n$ matrices with coefficients in the prime field $\mathbb{F}_p$ and by $\mathrm{GL}(n, \mathbb{F}_p)$ the subgroup of all invertible matrices in $\mathrm{Mat}_{\mathbb{F}_p}(n,n)$. Given $A \in \mathrm{Mat}_{\mathbb{F}_p}(n,n)$, we denote by $\mathbb{F}_p[A]$ the $\mathbb{F}_p$-algebra generated by A, i.e., $\mathbb{F}_p[A] = \{\sum_i a_i A^i \mid a_i \in \mathbb{F}_p\}$. A polynomial $g \in \mathbb{F}_{p^n}[x]$ is called *planar* if, for all $\alpha \in \mathbb{F}_{p^n}^*$,

$$\Delta_{g,\alpha}(x) \coloneqq g(x+\alpha) - g(x) - g(\alpha)$$

is a permutation polynomial in $\mathbb{F}_{p^n}[x]$ i.e., its evaluation map $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, y \mapsto \Delta_{g,\alpha}(y)$ is 1-to-1. Planar polynomials were introduced by Dembowski and Ostrom in [5]. Since we only study properties of evaluation maps in $\mathbb{F}_{p^n}$, we assume that $g \in \mathbb{F}_{p^n}[x]/(x^{p^n} - x)$, i.e., g has degree at most $p^n - 1$. A special type of polynomials in $\mathbb{F}_{p^n}[x]$ are *Dembowski-Ostrom* (DO) polynomials, which are those of the form

$$\sum_{0 \leq i \leq j \leq n-1} u_{i,j} \cdot x^{p^i + p^j}, \quad u_{i,j} \in \mathbb{F}_{p^n}.$$

If g is DO, $\Delta_{g,\alpha}$ is a linearized polynomial (i.e., its evaluation map is linear) for every $\alpha \in \mathbb{F}_{p^n}$. Let us denote by $M_{g,\alpha}$ the matrix (after fixing a choice of basis) associated to the evaluation map of $\Delta_{g,\alpha}$. For a planar DO polynomial g, we define its *spread set* $\mathcal{D}_g$ as

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

*This extended abstract is extracted from the full article available at `https://arxiv.org/abs/2211.17103`.

Remark 1. In [3], Coulter and Henderson showed a one-to-one correspondence between commutative presemifields of odd order and planar Dembowski-Ostrom polynomials. $\mathcal{D}_g$ is equal to the set of matrices corresponding to the mappings $x \to a \star x$ of left-multiplications with elements a in the corresponding commutative presemifield $\mathcal{R}_g$, hence $\mathcal{D}_g$ is equal to the spread set of $\mathcal{R}_g$ (see e.g., [6, Sec. 2.1]).

An equivalence relation between two polynomials that leaves the planarity property invariant is *CCZ-equivalence* [2]. CCZ-equivalence of two planar DO polynomials coincides with *linear equivalence* [1].

We study the *set of quotients in* $\mathcal{D}_g$, defined as

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

The following observation is immediate from the fact that $g(x+y) - g(x) - g(y)$ is symmetric in x and y and bilinear.

Lemma 1. *Let $g \in \mathbb{F}_{p^n}[x]$ be a DO polynomial and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^n}$. For each $Y \in \mathrm{GL}(n, \mathbb{F}_p)$, the set $\mathcal{D}_g Y^{-1}$ is an n-dimensional $\mathbb{F}_p$-vector space with basis*

$$\{M_{g,\alpha_1} Y^{-1}, M_{g,\alpha_2} Y^{-1}, \ldots, M_{g,\alpha_n} Y^{-1}\}.$$

The reason we are interested in the set $\mathrm{Quot}(\mathcal{D}_g)$ is that it stays invariant up to a different choice of basis under linear-equivalence of g, hence yielding an invariant for the CCZ-equivalence of DO planar functions.

Proposition 1. *Let $g, g' \in \mathbb{F}_{p^n}[x]$ be two planar DO polynomials within the same linear-equivalence class. Then,* $\mathrm{Quot}(\mathcal{D}_{g'}) = A^{-1} \cdot \mathrm{Quot}(\mathcal{D}_g) \cdot A$ *for an element $A \in \mathrm{GL}(n, \mathbb{F}_p)$.*

Proof. This immediately follows from the fact that the spread sets of g and g' are related via $\mathcal{D}_{g'} = X^{-1} \cdot \mathcal{D}_g \cdot Y$ for some $X, Y \in \mathrm{GL}(n, \mathbb{F}_p)$ (see also [6, Sec. 2.1]). □

We would like to recall that any finite field $\mathbb{F}_{p^n}$ (resp., a proper subfield $\mathbb{F}_{p^m}$) is isomorphic to $\mathbb{F}_p[T_\beta]$, where T_β denotes a matrix corresponding to the linear mapping $x \mapsto \beta x$ over $\mathbb{F}_{p^n}$, for $\beta \in \mathbb{F}_{p^n}^*$ defining a polynomial basis of $\mathbb{F}_{p^n}$ (resp., of $\mathbb{F}_{p^m}$). For more details on *matrix representations* of finite fields, we refer to, e.g., [7] or [8]. Applying a change of basis transformation to all elements of a matrix algebra $\mathbb{F}_p[T]$ does not affect the property of being a field, hence $\mathbb{F}_p[T]$ is a finite field if and only if $A^{-1} \cdot \mathbb{F}_p[T] \cdot A$ is for all $A \in \mathrm{GL}(n, \mathbb{F}_p)$.

2 The Structure of $\mathrm{Quot}(\mathcal{D}_g)$ for a planar DO monomial g

In [4], Coulter and Matthews showed that any planar DO monomial in $\mathbb{F}_{p^n}[x]$ is CCZ-equivalent to $x^{p^k+1} \in \mathbb{F}_{p^n}[x]$ with $n/\gcd(k, n)$ being odd. We show that for any DO polynomial $h \in \mathbb{F}_{p^n}[x]$ CCZ-equivalent to a planar monomial, the set $\mathrm{Quot}(\mathcal{D}_h)$ always contains the finite field of order p^n. More precisely, we show the following.

Theorem 1. *Let p be an odd prime and n a positive integer. Let $g(x) \in \mathbb{F}_{p^n}[x]$ be a planar DO monomial. For any $\alpha, \beta \in \mathbb{F}_{p^n}^*$, the element $X \coloneqq M_{g,\beta} M_{g,\alpha}^{-1} \in \mathrm{Quot}(\mathcal{D}_g)$ generates a field isomorphic to $\mathbb{F}_p(\alpha^{-1}\beta)$ viz. $\mathbb{F}_p[X]$, and $\mathbb{F}_p[X] \subseteq \mathrm{Quot}(\mathcal{D}_g)$.*

Let us denote by $\phi_\alpha \colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, x \mapsto \alpha x^{p^k} + \alpha^{p^k} x$ the evaluation map of $\Delta_{x^{p^k+1}, \alpha} \in \mathbb{F}_{p^n}[x]$. It is well known that ϕ_α is invertible if and only if $n/\gcd(k, n)$ is odd (see [4]). We have the following for the inverse, which is a special case of of Thm. 2.1 of [10]. It can also be proven by straightforward calculation of $\phi_\alpha^{-1}(\phi_\alpha(x))$.

Lemma 2 (Special case of Thm. 2.1 of [10])**.** *Let k be such that $n/\gcd(k,n)$ is odd. Let $d \coloneqq n/\gcd(k,n)$. For $\alpha \in \mathbb{F}_{p^n}^*$, the inverse of $\phi_\alpha\colon x \mapsto \alpha x^{p^k} + \alpha^{p^k} x$ is given by*

$$\phi_\alpha^{-1}\colon x \mapsto \frac{\alpha}{2} \cdot \sum_{i=0}^{d-1} (-1)^i \alpha^{-(p^k+1)p^{ki}} x^{p^{ki}}.$$

The following lemma is immediate.

Lemma 3. *Let k be such that $n/\gcd(k,n)$ is odd and let $\phi_\alpha\colon x \mapsto \alpha x^{p^k} + \alpha^{p^k} x$. For any $\alpha, \beta \in \mathbb{F}_{p^n}^*$, we have $\phi_\beta(\phi_\alpha^{-1}(x)) = (\beta^{p^k} - \alpha^{p^k-1}\beta) \cdot \phi_\alpha^{-1}(x) + \alpha^{-1}\beta x$.*

The monomial $g(x) = x^{p^k+1}$ admits a non-trivial self equivalence via $g(x) = \gamma^{-(p^k+1)} \cdot g(\gamma x)$, where γ is an arbitrary non-zero element of $\mathbb{F}_{p^n}$. From this, we obtain the following.

Lemma 4. *Let k be such that $n/\gcd(k,n)$ is odd and let $\phi_\alpha\colon x \mapsto \alpha x^{p^k} + \alpha^{p^k} x$. For any $\alpha, \beta, \gamma \in \mathbb{F}_{p^n}$, $\alpha, \gamma \neq 0$, we have $\phi_\beta(\phi_\alpha^{-1}(x)) = \gamma^{-(p^k+1)} \cdot \phi_{\gamma\beta}(\phi_{\gamma\alpha}^{-1}(\gamma^{p^k+1}x))$.*

To show Theorem 1, we will first deduce that each element in $\mathrm{Quot}(\mathcal{D}_g)$ generates (a subfield of) $\mathbb{F}_{p^n}$. To do so, we show that each element in $\mathrm{Quot}(\mathcal{D}_g)$ corresponds (up to a choice of basis) to a multiplication with an element of $\mathbb{F}_{p^n}$.

Lemma 5. *Let k be such that $n/\gcd(k,n)$ is odd. Let $\alpha, \beta \in \mathbb{F}_{p^n}, \alpha \neq 0$. If $\alpha^{-1}\beta \in \mathbb{F}_{p^{\gcd(k,n)}}$, the mapping $\phi_\beta \circ \phi_\alpha^{-1}$ is equal to $x \mapsto \alpha^{-1}\beta x$. If $\alpha^{-1}\beta$ lies not in $\mathbb{F}_{p^{\gcd(k,n)}}$, the mapping $\psi_{\alpha,\beta} \circ \phi_\beta \circ \phi_\alpha^{-1} \circ \psi_{\alpha,\beta}^{-1}$ is equal to $x \mapsto (\alpha^{-1}\beta)^{p^k} x$, where*

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

Proof. We first observe that $\beta^{p^k} - \alpha^{p^k-1}\beta$ is equal to zero if and only if $\beta = 0$ or $(\alpha^{-1}\beta)^{p^k-1} = 1$, i.e., if and only if $\alpha^{-1}\beta$ is contained in the subfield $\mathbb{F}_{p^{\gcd(k,n)}} \subseteq \mathbb{F}_{p^n}$. Hence, by Lemma 3, the statement is trivial for the case of $\alpha^{-1}\beta \in \mathbb{F}_{p^{\gcd(k,n)}} \subseteq \mathbb{F}_{p^n}$.

In the other case, the mapping $\psi_{\alpha,\beta}$ is well defined and we can decompose $\psi_{\alpha,\beta}$ as $C \circ B \circ A$, where A is a multiplication by $(\beta^{p^k} - \alpha^{p^k-1}\beta)^{-1}$, $B = \phi_\alpha$, and C is a multiplication by α^{p^k}. For all $x \in \mathbb{F}_{p^n}$, we then have:

$$L_1(x) \coloneqq A(\phi_\beta(\phi_\alpha^{-1}(A^{-1}(x)))) = \phi_\alpha^{-1}\left((\beta^{p^k} - \alpha^{p^k-1}\beta)x\right) + \alpha^{-1}\beta x.$$

$$\begin{aligned} L_2(x) \coloneqq B(L_1(B^{-1}(x))) &= (\beta^{p^k} - \alpha^{p^k-1}\beta) \cdot \phi_\alpha^{-1}(x) + \phi_\alpha(\alpha^{-1}\beta \cdot \phi_\alpha^{-1}(x)) \\ &= \beta^{p^k} \cdot \left(\phi_\alpha^{-1}(x) + \alpha^{-p^k+1}(\phi_\alpha^{-1}(x))^{p^k}\right). \end{aligned}$$

$$\begin{aligned} L_3(x) \coloneqq C(L_2(C^{-1}(x))) &= \beta^{p^k} \cdot \left(\alpha^{p^k}\phi_\alpha^{-1}(\alpha^{-p^k}x) + \alpha(\phi_\alpha^{-1}(\alpha^{-p^k}x))^{p^k}\right) \\ &= \beta^{p^k} \cdot \phi_\alpha(\phi_\alpha^{-1}(\alpha^{-p^k}x)) = (\alpha^{-1}\beta)^{p^k} x. \end{aligned}$$

The proof is complete since $L_3 = \psi_{\alpha,\beta} \circ \phi_\beta \circ \phi_\alpha^{-1} \circ \psi_{\alpha,\beta}^{-1}$. $\square$

The more complicated part is to show that, for any $X \in \mathrm{Quot}(\mathcal{D}_g)$, the matrix algebra $\mathbb{F}_p[X]$ is indeed a subset of $\mathrm{Quot}(\mathcal{D}_g)$. We do this in the following.

Proof of Theorem 1. Let $\alpha, \beta \in \mathbb{F}_{p^n}^*$ and let $X := M_{g,\beta} M_{g,\alpha}^{-1}$. By Lemma 5, the linear mapping $\phi_\beta \circ \phi_\alpha^{-1}$ is similar to $x \mapsto \alpha^{-1}\beta x$. Hence, the $\mathbb{F}_p$-algebra $\mathbb{F}_p[X]$ is isomorphic to $\mathbb{F}_p(\alpha^{-1}\beta)$ and thus a field. It is left to show that $\mathbb{F}_p[X] \subseteq \mathrm{Quot}(\mathcal{D}_g)$. The case of $\alpha^{-1}\beta \in \mathbb{F}_{p^{\gcd(k,n)}}$ is trivial and we therefore assume in the following that $\alpha^{-1}\beta \notin \mathbb{F}_{p^{\gcd(k,n)}}$. We will first handle the case of $\alpha = 1$ and show that $\left(M_{g,\beta} M_{g,1}^{-1}\right)^r \in \mathrm{Quot}(\mathcal{D}_g)$ for any integer $r \geq 2$. By Lemma 5, we have

$$\psi_{1,\beta} \circ \left(\phi_\beta \circ \phi_1^{-1}\right)^r \circ \psi_{1,\beta}^{-1}(x) = \left(\psi_{1,\beta} \circ \phi_\beta \circ \phi_1^{-1} \circ \psi_{1,\beta}^{-1}\right)^r (x) = \beta^{rp^k} x.$$

Further,

$$\beta^{rp^k} x = \begin{cases} \psi_{1,\beta^r} \circ \phi_{\beta^r} \circ \phi_1^{-1} \circ \psi_{1,\beta^r}^{-1}(x) & \text{if } \beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}} \\ \beta^r x = \phi_{\beta^r} \circ \phi_1^{-1}(x) & \text{otherwise} \end{cases},$$

and thus

$$\left(\phi_\beta \circ \phi_1^{-1}\right)^r = \begin{cases} \psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r} \circ \phi_{\beta^r} \circ \phi_1^{-1} \circ \psi_{1,\beta^r}^{-1} \circ \psi_{1,\beta} & \text{if } \beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}} \\ \psi_{1,\beta}^{-1} \circ \phi_{\beta^r} \circ \phi_1^{-1} \circ \psi_{1,\beta} & \text{otherwise} \end{cases}. \tag{1}$$

We will now prove that the latter composition is equal to $\phi_\delta \circ \phi_\gamma^{-1}$ for properly chosen field elements δ, γ.

Case $\beta^r \in \mathbb{F}_{p^{\gcd(k,n)}}$. In this case, $\left(\phi_\beta \circ \phi_1^{-1}\right)^r (x) = \psi_{1,\beta}^{-1} \circ \phi_{\beta^r} \circ \phi_1^{-1} \circ \psi_{1,\beta}(x) = \psi_{1,\beta}^{-1}(\beta^r \cdot \psi_{1,\beta}(x)) = \beta^r \cdot \psi_{1,\beta}^{-1}(\psi_{1,\beta}(x)) = \beta^r x = \phi_{\beta^r} \circ \phi_1^{-1}(x)$, since $\psi_{1,\beta}$ is $\mathbb{F}_{p^{\gcd(k,n)}}$-linear.

Case $\beta^r \notin \mathbb{F}_{p^{\gcd(k,n)}}$. We first observe that $\psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r}(x) = \frac{\beta^{p^k} - \beta}{\beta^{rp^k} - \beta^r} x$. Let us define $\lambda := \frac{\beta^{p^k} - \beta}{\beta^{rp^k} - \beta^r} \in \mathbb{F}_{p^n}^*$. The image of the mapping $x \mapsto x^{p^k+1}$ over $\mathbb{F}_{p^n}$ is equal to the set of squares in $\mathbb{F}_{p^n}$. Indeed, every element in the image is a square as $p^k + 1$ is even, and $x \mapsto x^{p^k+1}$ is 2-to-1 as a DO planar function [9]. Hence, if λ is a square, we have $\lambda = \gamma^{p^k+1}$ for an element $\gamma \in \mathbb{F}_{p^n}^*$ and, otherwise, we have $\lambda = u\gamma^{p^k+1}$ with $u \in \mathbb{F}_{p^n}^*$ being an arbitrary non-square. Note that we can always choose $u \in \mathbb{F}_{p^{\gcd(k,n)}}^*$. Indeed, let $n = 2^m \ell$ and $k = 2^{m'} \ell'$ with ℓ, ℓ' being odd, we necessarily have $m' \geq m$, as otherwise $n/\gcd(k,n)$ would be even. So, $\mathbb{F}_{p^{\gcd(k,n)}}$ contains $\mathbb{F}_{p^{2^m}}$ as a subfield and the extension degree $[\mathbb{F}_{p^n} : \mathbb{F}_{p^{\gcd(k,n)}}]$ is odd. The claim then follows as a non-square in a finite field stays a non-square in any extension field of odd extension degree.

Let us therefore assume that $\lambda = u\gamma^{p^k+1}$ with $\gamma \in \mathbb{F}_{p^n}^*$ and $u \in \mathbb{F}_{p^{\gcd(k,n)}}^*$. We have

$$\begin{aligned} \psi_{1,\beta}^{-1} \circ \psi_{1,\beta^r} \circ \phi_{\beta^r} \circ \phi_1^{-1} \circ \psi_{1,\beta^r}^{-1} \circ \psi_{1,\beta}(x) &= \lambda \cdot \left(\phi_{\beta^r} \circ \phi_1^{-1}\right) \left(\lambda^{-1} x\right) \\ &= \gamma^{p^k+1} \cdot \left(\phi_{\beta^r} \circ \phi_1^{-1}\right) \left(\gamma^{-(p^k+1)} x\right), \end{aligned} \tag{2}$$

where the last equality follows from the fact that $u \in \mathbb{F}_{p^{\gcd(k,n)}}^*$. By Lemma 4, we have $\gamma^{p^k+1} \cdot \left(\phi_{\beta^r} \circ \phi_1^{-1}\right) \left(\gamma^{-(p^k+1)} x\right) = \phi_{\gamma\beta^r} \circ \phi_\gamma^{-1}(x)$.

To handle the case of $\alpha \neq 1$, we apply Lemma 4 with $\gamma = \alpha^{-1}$ and obtain $\phi_\beta(\phi_\alpha^{-1}(x)) = \alpha^{p^k+1} \cdot \phi_{\alpha^{-1}\beta}(\phi_1^{-1}(\alpha^{-(p^k+1)} x))$, hence,

$$\begin{aligned} (\phi_\beta \circ \phi_\alpha^{-1})^r(x) &= \alpha^{p^k+1} \cdot (\phi_{\alpha^{-1}\beta} \circ \phi_1^{-1})^r (\alpha^{-(p^k+1)} x) \\ &= \alpha^{p^k+1} \cdot \left(\phi_{\delta'} \circ \phi_{\gamma'}^{-1}(\alpha^{-(p^k+1)} x)\right) = \phi_{\alpha\delta'} \circ \phi_{\alpha\gamma'}^{-1}(x) \end{aligned}$$

for appropriate elements γ', δ'. We have now established that, for $\alpha^{-1}\beta$ being a generator of $\mathbb{F}_{p^n}^*$, the algebra $\mathbb{F}_p[X]$ is a field of order p^n contained in $\mathrm{Quot}(\mathcal{D}_g)$.

To handle the general case where $\alpha^{-1}\beta$ is not a generator of $\mathbb{F}_{p^n}^*$, we will show that X is equal to $(M_{g,\beta'}M_{g,\alpha'}^{-1})^r$ for some generator $\alpha'^{-1}\beta'$ of $\mathbb{F}_{p^n}^*$ and some non-negative integer r. Then, it would immediately follow that $\mathbb{F}_p[X] \subseteq \mathbb{F}_p[M_{g,\beta'}M_{g,\alpha'}^{-1}] \subseteq \mathrm{Quot}(\mathcal{D}_g)$. Indeed, let $\bar{\beta}$ be a generator of $\mathbb{F}_{p^n}^*$ such that $\bar{\beta}^r = \alpha^{-1}\beta$ and let

$$\frac{\bar{\beta}^{p^k} - \bar{\beta}}{\bar{\beta}^{rp^k} - \bar{\beta}^r} = u\gamma^{p^k+1}$$

with $\gamma \in \mathbb{F}_{p^n}^*$ and $u \in \mathbb{F}_{p^{\gcd(k,n)}}^*$. By extensively applying Lemma 4 and the result we established above, we obtain

$$\begin{aligned}
(\phi_{\alpha\gamma^{-1}\bar{\beta}} \circ \phi_{\alpha\gamma^{-1}}^{-1})^r(x) &= \left((\alpha^{-1}\gamma)^{-(p^k+1)} \cdot \phi_{\bar{\beta}} \circ \phi_1^{-1}((\alpha^{-1}\gamma)^{p^k+1}x)\right)^r \\
&= (\alpha^{-1}\gamma)^{-(p^k+1)} \cdot \left(\phi_{\bar{\beta}} \circ \phi_1^{-1}\right)^r ((\alpha^{-1}\gamma)^{p^k+1}x) \\
&= (\alpha^{-1}\gamma)^{-(p^k+1)} \cdot \phi_{\gamma\bar{\beta}^r} \circ \phi_\gamma^{-1}((\alpha^{-1}\gamma)^{p^k+1}x) \\
&= (\alpha^{-1}\gamma)^{-(p^k+1)} \cdot \phi_{\alpha^{-1}\gamma\beta} \circ \phi_\gamma^{-1}((\alpha^{-1}\gamma)^{p^k+1}x) = \phi_\beta \circ \phi_\alpha^{-1}(x).
\end{aligned}$$

□

Remark 2. For $g(x) = x^{p^k+1} \in \mathbb{F}_{p^n}[x]$ planar, we have $|\mathrm{Quot}(\mathcal{D}_g)| = \frac{(p^n - p^{\gcd(k,n)}) \cdot (p^n-1)}{p^{\gcd(k,n)}-1} + p^{\gcd(k,n)}$.

References

[1] L. Budaghyan and T. Helleseth. New commutative semifields defined by new PN multinomials. *Cryptogr. Commun.*, 3(1):1–16, 2011.

[2] C. Carlet, P. Charpin, and V. A. Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[3] R. S. Coulter and M. Henderson. Commutative presemifields and semifields. *Adv. Math.*, 217(1):282–304, 2008.

[4] R. S. Coulter and R. W. Matthews. Planar functions and planes of lenz-barlotti class II. *Des. Codes Cryptogr.*, 10(2):167–184, 1997.

[5] P. Dembowski and T. G. Ostrom. Planes of order n with collineation groups of order n^2. *Math. Z.*, 103(3):239–258, 1968.

[6] U. Dempwolff. Semifield planes of order 81. *J. Geom.*, 89:1–16, 2008.

[7] D. Hachenberger and D. Jungnickel. *Topics in Galois fields.* Springer, 2020.

[8] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications.* Cambridge university press, 1994.

[9] G. Weng and X. Zeng. Further results on planar DO functions and commutative semifields. *Des. Codes Cryptogr.*, 63(3):413–423, 2012.

[10] B. Wu. The compositional inverses of linearized permutation binomials over finite fields. *arXiv preprint arXiv:1311.2154*, 2013.