Constructing Dembowski–Ostrom permutation polynomials from upper triangular matrices

Yuyin Yu[a], Yanbin Zheng[b,*], Yongqiang Li[c], Jingang Liu[d,e]

[a] *School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China*
[b] *School of Mathematical Sciences, Qufu Normal University, Qufu 273165, China*
[c] *Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[d] *Guangdong Provincial Key Laboratory of Information Security Technology, Sun Yat-sen University, Guangzhou 510006, China*
[e] *School of Mathematics and Systems Science, Guangdong Polytechnic Normal University, Guangzhou 510665, China*

Abstract

We establish a one-to-one correspondence between Dembowski-Ostrom (DO) polynomials and upper triangular matrices. Based on this correspondence, we give a bijection between DO permutation polynomials and a special class of upper triangular matrices, and construct a new batch of DO permutation polynomials. To the best of our knowledge, almost all other known DO permutation polynomials are located in finite fields of $\mathbb{F}_{2^n}$, where n contains odd factors (see Table 1). However, there are no restrictions on n in our results, and especially the case of $n = 2^m$ has not been studied in the literature. For example, we provide a simple necessary and sufficient condition to determine when $\gamma \operatorname{Tr}(\theta_i x)\operatorname{Tr}(\theta_j x) + x$ (see Corollary 1) is a DO permutation polynomial. In addition, when the upper triangular matrix degenerates into a diagonal matrix and the elements on the main diagonal form a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, this diagonal matrix corresponds to all linearized permutation polynomials (see Corollary 2). In a word, we construct several new DO permutation polynomials, and our results can be viewed as an extension of linearized permutation polynomials.

Keywords: Finite fields, Permutations, Dembowski–Ostrom polynomials
2010 MSC: 11T06, 15A63, 15A03

1. Introduction 1

For q a prime power, let $\mathbb{F}_{q^n}$ be the finite field with q^n elements, and let $\mathbb{F}_{q^n}[x]$ be the ring of polynomials over $\mathbb{F}_{q^n}$. A polynomial $f(x) \in \mathbb{F}_{q^n}[x]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_{q^n}$ if it induces a bijection from $\mathbb{F}_{q^n}$ to itself. A polynomial $Q(x) \in \mathbb{F}_{q^n}[x]$ is called a *Dembowski–Ostrom polynomial* (DO polynomial) if it has the shape

$$Q(x) = \sum_{1 \le i \le j \le n} c_{ij} x^{q^{i-1}+q^{j-1}}.$$

*Corresponding author.
Email addresses: yuyuyin@163.com (Yuyin Yu), zheng@qfnu.edu.cn (Yanbin Zheng), yongq.lee@gmail.com (Yongqiang Li), liujingang@gpnu.edu.cn (Jingang Liu)

*Preprint submitted to **** *November 7, 2024*

This class of polynomials was described by Dembowski and Ostrom in [3].

Patarin's HFE cryptosystem [21] was based on DO polynomials over $\mathbb{F}_{2^n}$. The permutation behaviour of DO polynomials was studied in [1] and later in [12]. Both papers investigated DO permutation polynomials (DOPPs) of the form $L_1(x)L_2(x)$. The result of [1, 12] was extended in [22], which identified several types of DOPPs of the form $L_1(x)(L_2(x) + L_1(x)L_3(x))$. In the above, $L_i(x)$'s are linearized polynomials over $\mathbb{F}_{2^n}$.

There are several classes of DOPPs with few terms. For example, the permutation binomial $x^{2^m+2}+\alpha x$ of $\mathbb{F}_{2^{2m}}$ was covered by [31, Corollary 2.3], where m is odd, $\alpha \in \mathbb{F}_{2^{2m}}^*$, and $\mathrm{ord}(\alpha^{2^m-1}) = 3$. The PP $\alpha x^{2^s+1} + \alpha^{2^m} x^{2^{2m}+2^{m+s}}$ of $\mathbb{F}_{2^{3m}}$ was given in [2], where α is a primitive element of $\mathbb{F}_{2^{3m}}$ and m, s satisfy certain conditions. The permutation trinomial $x^{2^{m+1}+1} + x^3 + x$ of $\mathbb{F}_{2^n}$ with $n = 2m + 1$ was presented in [5]. The PP $x^{2^{m+2}+1} + x^{2^m+4} + x^5$ of $\mathbb{F}_{2^{2m}}$ was found in [7], and later two classes of DO permutation trinomials of $\mathbb{F}_{2^{2m}}$ of the form

$$x^{2^{m+k}+2^m} + x^{2^{m+k}+1} + x^{2^k+1},$$
$$x^{2^{m+k}+2^m} + x^{2^m+2^k} + x^{2^k+1},$$

where $k = 1, 2$, were given in [29]. DO permutation quadrinomials of the form

$$x^{2^{m+1}+2^m} + c_1 x^{2^{m+1}+1} + c_2 x^{2^m+2} + c_3 x^3 \in \mathbb{F}_{2^{2m}}[x],$$

where m is odd, was studied in [24], and later was completely characterized in [14, 25]. The boomerang uniformity of this class of DOPPs was initially studied in [26]. Soon afterwards, [10, 11, 15, 16, 27] investigated the permutation behavior and the boomerang uniformity of DO quadrinomials of more general form

$$c_0 x^{2^{m+k}+2^m} + c_1 x^{2^{m+k}+1} + c_2 x^{2^m+2^k} + c_3 x^{2^k+1} \in \mathbb{F}_{2^{2m}}[x].$$

See [13, 18] for more information about the boomerang uniformity of DOPPs.

A *linearized polynomial* (or q-polynomial) over $\mathbb{F}_{q^n}$ is defined by

$$L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x].$$

The *trace function from* $\mathbb{F}_{q^n}$ *to* $\mathbb{F}_q$ is defined in this paper by

$$\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{q^i} = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}.$$

Zhou [30] gave an explicit representation of linearized PPs as follows.

Theorem 1 ([30, Corollary 2.3])**.** *Let α be a fixed primitive element in $\mathbb{F}_{q^n}$, then the set $\{f(x) = \sum_{s=0}^{n-1}(\alpha_0 + \alpha^{q^s}\alpha_1 + \alpha^{2q^s}\alpha_2 + \cdots + \alpha^{(n-1)q^s}\alpha_{n-1})x^{q^s} \in \mathbb{F}_{q^n}[x]$: where α_0, α_1, …, α_{n-1} is any basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q\}$ contains and only contains all the linearized PPs.*

Yuan and Zeng [28] provided a simple proof of Zhou's result and get the following theorem.

Theorem 2 ([28, Theorem 1.1])**.** *Let* $\{\omega_1, \omega_2, \ldots, \omega_n\}$ *be any given basis of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$*. Let* $L(x)$ *be a linearized polynomial over* $\mathbb{F}_{q^n}$*. Then there are* n *elements* $\theta_1, \theta_2, \ldots, \theta_n \in \mathbb{F}_{q^n}$ *such that*

$$L(x) = \mathrm{Tr}(\theta_1 x)\omega_1 + \cdots + \mathrm{Tr}(\theta_n x)\omega_n.$$

Moreover, $L(x)$ *is a PP if and only if* $\{\theta_1, \theta_2, \ldots, \theta_n\}$ *is a basis of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$*.*

Ling and Qu [17] generalized the result above to linearized polynomials with kernel of any given dimensions.

Theorem 3 ([17, Theorem 2.3])**.** *Let* $\{\theta_1, \theta_2, \ldots, \theta_n\}$ *be any basis of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$*, and let* $L(x)$ *be a linearized polynomial over* $\mathbb{F}_{q^n}$*. Then there exists a unique vector* $(\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{F}_{q^n}^n$ *such that*

$$L(x) = \mathrm{Tr}(\theta_1 x)\beta_1 + \cdots + \mathrm{Tr}(\theta_n x)\beta_n.$$

Moreover, let k *be an integer such that* $0 \leq k \leq n$*, then* $\dim_{\mathbb{F}_q}(\mathrm{Ker}(L)) = k$ *if and only if* $\mathrm{Rank}_{\mathbb{F}_q}\{\beta_1, \beta_2, \ldots, \beta_n\} = n - k$*.*

References [17, 28, 30] discussed the permutation property of linearized polynomials. Inspired by these works, we consider how to generalize linearized permutations to DO permutations.

The main purpose of this paper is to find some sufficient conditions for DO polynomials $Q(x)$ to be a PP of $\mathbb{F}_{q^n}$. Section 2 gives a bijection between DO polynomials and upper triangular matrices. In Section 3, we introduce the definition of DO permutation matrix (DOPM), and prove that a DO polynomial $Q(x)$ is a PP if and only if the corresponding matrix of $Q(x)$ is a DOPM. Furthermore, a simple method for constructing DOPMs is proposed, and then two classes of DOPPs are given. In Section 4, we prove that our method can construct new DOPPs compared with other method.

2. Bijection between DO polynomials and upper triangular matrices

Lemma 1. *Let* $\{\theta_1, \theta_2, \ldots, \theta_n\}$ *be any basis of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$ *and*

$$Q(x) = \sum_{1 \leq i \leq j \leq n} c_{ij} x^{q^{i-1}+q^{j-1}} \in \mathbb{F}_{q^n}[x]. \tag{1}$$

Then $Q(x)$ *can be written in the form*

$$Q(x) = X(x)\Phi X(x)^T, \tag{2}$$

where Φ *is an* $n \times n$ *matrix over* $\mathbb{F}_{q^n}$ *and* $X(x)^T$ *is the transpose of*

$$X(x) = (\mathrm{Tr}(\theta_1 x), \mathrm{Tr}(\theta_2 x), \ldots, \mathrm{Tr}(\theta_n x)). \tag{3}$$

Proof. According to [17, Theorem 2.3](see Theorem 3), we have

$$\sum_{i=1}^{j} c_{ij} x^{q^{i-1}} = \sum_{u=1}^{n} \mathrm{Tr}(\theta_u x)\beta_{uj} \quad \text{and} \quad \sum_{j=1}^{n} \beta_{uj} x^{q^{j-1}} = \sum_{v=1}^{n} \mathrm{Tr}(\theta_v x)\phi_{uv}$$

for some $\beta_{uj}, \phi_{uv} \in \mathbb{F}_{q^n}$. Thus,

$$
\begin{aligned}
Q(x) &= \sum_{j=1}^{n} \Big(\sum_{i=1}^{j} c_{ij} x^{q^{i-1}} \Big) x^{q^{j-1}} = \sum_{j=1}^{n} \Big(\sum_{u=1}^{n} \mathrm{Tr}(\theta_u x) \beta_{uj} \Big) x^{q^{j-1}} \\
&= \sum_{u=1}^{n} \mathrm{Tr}(\theta_u x) \sum_{j=1}^{n} \beta_{uj} x^{q^{j-1}} = \sum_{u=1}^{n} \mathrm{Tr}(\theta_u x) \sum_{v=1}^{n} \mathrm{Tr}(\theta_v x) \phi_{uv} \\
&= \sum_{u=1}^{n} \sum_{v=1}^{n} \mathrm{Tr}(\theta_u x) \phi_{uv} \mathrm{Tr}(\theta_v x) = X(x) \Phi X(x)^T,
\end{aligned}
$$

where $\Phi \in \mathbb{F}_{q^n}^{n \times n}$ and ϕ_{uv} is the element in the uth row and vth column of Φ. □

Assume that $\Phi = [\phi_{uv}]_{n \times n}$ is a square matrix of size n over $\mathbb{F}_{q^n}$. Then

$$
X(x)\Phi X(x)^T = \sum_{1 \le u \le n} \phi_{uu} \mathrm{Tr}(\theta_u x)^2 + \sum_{1 \le u \ne v \le n} (\phi_{uv} + \phi_{vu}) \mathrm{Tr}(\theta_u x) \mathrm{Tr}(\theta_v x). \tag{4}
$$

For another matrix $\Phi' = [\phi'_{uv}]_{n \times n}$ over $\mathbb{F}_{q^n}$, if $\phi'_{uu} = \phi_{uu}$ for $1 \le u \le n$ and $\phi'_{uv} + \phi'_{vu} = \phi_{uv} + \phi_{vu}$ for $1 \le u \ne v \le n$, then

$$
X(x)\Phi X(x)^T = X(x)\Phi' X(x)^T.
$$

Thus the correspondence in (2) between $Q(x)$ and Φ is not one-to-one. Next we introduce a matrix Ψ and establish a bijective correspondence between $Q(x)$ and Ψ.

Theorem 4. *Let $Q(x)$, θ_i's, $X(x)$ and $\Phi = [\phi_{uv}]_{n \times n}$ be the same as in Lemma 1. Define an upper triangular matrix $\Psi = [\psi_{uv}]_{n \times n}$ over $\mathbb{F}_{q^n}$ such that*

$$
\psi_{uv} = \begin{cases} \phi_{uv} + \phi_{vu} & \text{if } u < v, \\ \phi_{uv} & \text{if } u = v, \\ 0 & \text{if } u > v, \end{cases} \tag{5}
$$

where $1 \le u, v \le n$. Then $Q(x)$ can be written in the form

$$
Q(x) = X(x) \Psi X(x)^T, \tag{6}
$$

and there is a one-to-one correspondence between $Q(x)$ and Ψ as follows:

$$
c_{ij} = \begin{cases} \sum\limits_{1 \le u \le v \le n} (\theta_u^{q^{i-1}} \theta_v^{q^{j-1}} + \theta_v^{q^{i-1}} \theta_u^{q^{j-1}}) \psi_{uv} & \text{if } i < j, \\ \sum\limits_{1 \le u \le v \le n} (\theta_u \theta_v)^{q^{i-1}} \psi_{uv} & \text{if } i = j, \end{cases} \tag{7}
$$

$$
\psi_{uv} = \begin{cases} \sum\limits_{1 \le i \le j \le n} (\alpha_u^{q^{i-1}} \alpha_v^{q^{j-1}} + \alpha_v^{q^{i-1}} \alpha_u^{q^{j-1}}) c_{ij} & \text{if } u < v, \\ \sum\limits_{1 \le i \le j \le n} \alpha_u^{q^{i-1} + q^{j-1}} c_{ij}, & \text{if } u = v, \end{cases} \tag{8}
$$

where $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is the dual basis of $\{\theta_1, \theta_2, \ldots, \theta_n\}$.

Proof. From (2), (4) and (5), we get (6). Then, by (6) and (3),

$$\begin{aligned}
Q(x) &= \sum_{1\le u\le v\le n} \psi_{uv}\,\mathrm{Tr}(\theta_u x)\mathrm{Tr}(\theta_v x) \\
&= \sum_{1\le u\le v\le n} \psi_{uv} \sum_{k=0}^{n-1} (\theta_u x)^{q^k} \sum_{\ell=0}^{n-1} (\theta_v x)^{q^\ell} \\
&= \sum_{1\le u\le v\le n} \psi_{uv} \sum_{k=0}^{n-1}\sum_{\ell=0}^{n-1} \theta_u^{q^k}\theta_v^{q^\ell} x^{q^k+q^\ell} \\
&= \sum_{k=0}^{n-1}\sum_{\ell=0}^{n-1}\sum_{1\le u\le v\le n} \theta_u^{q^k}\theta_v^{q^\ell}\,\psi_{uv}\, x^{q^k+q^\ell}.
\end{aligned} \tag{9}$$

By comparing the coefficients of $Q(x)$ in (1) and (9), we have (7).

Since $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is the dual basis of $\{\theta_1, \theta_2, \dots, \theta_n\}$, for $1 \le u \le n$,

$$\begin{aligned}
X(\alpha_u) &= (\mathrm{Tr}(\theta_1\alpha_u), \mathrm{Tr}(\theta_2\alpha_u), \dots, \mathrm{Tr}(\theta_n\alpha_u)) \\
&= (0, \dots, 0, \overset{u\text{th}}{1}, 0, \dots, 0) \\
&= e_u.
\end{aligned}$$

Similarly, $X(\alpha_u + \alpha_v) = e_u + e_v$ for $1 \le u < v \le n$. Note that

$$Q(x) = \sum_{1\le i\le j\le n} c_{ij} x^{q^{i-1}+q^{j-1}} = X(x)\Psi X(x)^T.$$

Hence

$$Q(\alpha_u) = \sum_{1\le i\le j\le n} c_{ij}\alpha_u^{q^{i-1}+q^{j-1}} = X(\alpha_u)\Psi X(\alpha_u)^T = e_u \Psi e_u^T = \psi_{uu},$$

$$\begin{aligned}
Q(\alpha_u + \alpha_v) &= \sum_{1\le i\le j\le n} c_{ij}(\alpha_u + \alpha_v)^{q^{i-1}+q^{j-1}} = X(\alpha_u + \alpha_v)\Psi X(\alpha_u + \alpha_v)^T \\
&= (e_u + e_v)\Psi(e_u + e_v)^T = \psi_{uu} + \psi_{uv} + \psi_{vv}.
\end{aligned}$$

Then we obtain (8). This competes the proof. □

Remark 1. The DO polynomial $Q(x)$ can be viewed as a quadratic form in x_1, x_2, ..., x_n over $\mathbb{F}_{q^n}$, where $x_i = x^{q^{i-1}}$. Thus there is a natural bijection between $Q(x)$ and the upper triangular matrix $C = [c_{ij}]_{n\times n}$ as follows:

$$Q(x) = (x, x^q, \dots, x^{q^{n-1}})C(x, x^q, \dots, x^{q^{n-1}})^T, \tag{10}$$

where $(x, x^q, \dots, x^{q^{n-1}}) \in \mathbb{F}_{q^n}^n$. However, in the relationship (6), the vector

$$X(x) = (\mathrm{Tr}(\theta_1 x), \mathrm{Tr}(\theta_2 x), \dots, \mathrm{Tr}(\theta_n x)) \in \mathbb{F}_q^n$$

runs through all the vectors of $\mathbb{F}_q^n$ when x runs over $\mathbb{F}_{q^n}$. This property plays an important role in (11). It is the reason we establish the relationship (6) instead of directly using (10).

3. DO permutation polynomials and DO permutation matrices

In this section, two classes of DO permutation polynomials will be presented by constructing DO permutation matrices.

If q is odd, then $Q(x) = Q(-x)$ for each $x \in \mathbb{F}_{q^n} \setminus \{0\}$, and so $Q(x)$ is not a PP of $\mathbb{F}_{q^n}$. Therefore, we need only consider the case q is even.

We first introduce a definition of a special class of upper triangular matrices.

Definition 1. Let Ψ be an $n \times n$ upper triangular matrix over $\mathbb{F}_{q^n}$, and let

$$V = \{\overline{X}\Psi\overline{X}^T : \overline{X} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n\}.$$

If $\#V = q^n$, then Ψ is called a *DO permutation matrix (DOPM)* over $\mathbb{F}_{q^n}$.

Theorem 5. *Let $\{\theta_1, \theta_2, \dots, \theta_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and*

$$X(x) = (\mathrm{Tr}(\theta_1 x), \mathrm{Tr}(\theta_2 x), \dots, \mathrm{Tr}(\theta_n x)).$$

For any $n \times n$ upper triangular matrix Ψ over $\mathbb{F}_{q^n}$, let $Q(x) = X(x)\Psi X(x)^T$. Then $Q(x)$ is a DOPP of $\mathbb{F}_{q^n}$ if and only if Ψ is a DOPM over $\mathbb{F}_{q^n}$.

Proof. Let $\{\omega_1, \omega_2, \dots, \omega_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and define

$$L(x) = \mathrm{Tr}(\theta_1 x)\omega_1 + \mathrm{Tr}(\theta_2 x)\omega_2 + \cdots + \mathrm{Tr}(\theta_n x)\omega_n.$$

Then $L(x)$ is a PP of $\mathbb{F}_{q^n}$ by Theorem 2, and so $X(x)$ runs through all the vectors of $\mathbb{F}_q^n$ when x runs over $\mathbb{F}_{q^n}$. Therefore,

$$\{Q(x) = X(x)\Psi X(x)^T : x \in \mathbb{F}_{q^n}\} = \{\overline{X}\Psi\overline{X}^T : \overline{X} \in \mathbb{F}_q^n\} = V, \tag{11}$$

which implies that $Q(x)$ is a PP of $\mathbb{F}_{q^n}$ if and only if $\#V = q^n$. □

By Theorem 5, to find a DOPP $Q(x)$ of $\mathbb{F}_{q^n}$, we need only construct a DOPM Ψ over $\mathbb{F}_{q^n}$. Now we consider the affine equivalence relation between DOPPs.

Definition 2. Let F and F' be two functions from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$. Then F and F' are called **affine equivalent** if

$$F'(x) = A_1(F(A_2(x))),$$

where A_1 and A_2 are affine permutations of $\mathbb{F}_{q^n}$.

Lemma 2. *Let σ be any permutation of $\mathbb{F}_{q^n}$. Then there exists an affine independent subset $\{\gamma_0, \gamma_1, \dots, \gamma_n\}$ over $\mathbb{F}_q$ such that $\{\sigma(\gamma_0), \sigma(\gamma_1), \dots, \sigma(\gamma_n)\}$ is also affine independent over $\mathbb{F}_q$.*

Remark 2. Hou [8] proved Lemma 2 when $q = 2$. In fact, Hou's method can be generalized to $q = p^r$ for any prime p and positive integer r. Please turn to [8, Lemma 2.2] for a proof.

Theorem 6. *Let $Q(x)$ be a DOPP of $\mathbb{F}_{q^n}$ and $X(x)$ be the same as in Theorem 5. Then $Q(x)$ is affine equivalent to*

$$Q'(x) = X(x)\Psi' X(x)^T,$$

where Ψ' is a DOPM over $\mathbb{F}_{q^n}$ and the entries on the main diagonal of Ψ' form a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Proof. In Theorem 5, we proved that $X(x)$ runs through all the vectors of $\mathbb{F}_q^n$ when x runs over $\mathbb{F}_{q^n}$. Thus there exist $a_0 = 0$ and a_i's in $\mathbb{F}_{q^n}$ such that

$$X(a_i) = (0, \ldots, 0, \underset{i\text{th}}{1}, 0, \ldots, 0) = e_i \quad \text{for } 1 \leq i \leq n.$$

Since $Q(x)$ is a PP of $\mathbb{F}_{q^n}$, by Lemma 2, there exists an affine independent subset $\{\gamma_0, \gamma_1, \ldots, \gamma_n\}$ such that $\{Q(\gamma_0), Q(\gamma_1), \ldots, Q(\gamma_n)\}$ is also affine independent. Let $\beta_0 = 0$ and let $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Choose affine permutations h, g such that $g(a_i) = \gamma_i$ and $h(Q(\gamma_i)) = \beta_i$ for $0 \leq i \leq n$. Set

$$Q' = h \circ Q \circ g.$$

Then Q is affine equivalent to $Q'(x)$, and so $Q'(x)$ is a DOPP of $\mathbb{F}_{q^n}$. From Theorems 4 and 5, $Q'(x)$ can be uniquely represented as $Q'(x) = X(x)\Psi' X(x)^T$ and Ψ' is a DOPM over $\mathbb{F}_{q^n}$. The ith entry on the main diagonal of Ψ' is

$$e_i \Psi' e_i^T = X(a_i)\Psi' X(a_i)^T = Q'(a_i) = h \circ Q \circ g(a_i) = \beta_i, \quad 1 \leq i \leq n. \qquad \square$$

Theorem 6 allows us to study only the DOPMs whose main diagonal entries form a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We will give a simple method for constructing such DOPMs after the notations below.

Definition 3. For a set $\Upsilon = \{\alpha_1, \alpha_2, \ldots, \alpha_k\} \subseteq \mathbb{F}_{q^n}$, define

$$\operatorname{span}(\Upsilon) = \{\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_k\alpha_k : \lambda_i \in \mathbb{F}_q\}.$$

If Υ is an empty set, denote $\operatorname{span}(\Upsilon) = \{0\}$.

Theorem 7. *Let $\{\theta_1, \theta_2, \ldots, \theta_n\}$ and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be two bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where q is even. For any $\gamma \in \mathbb{F}_{q^n}$ and fixed $i, j \in \{1, 2, \ldots, n\}$ with $i \neq j$, define*

$$Q(x) = \gamma \operatorname{Tr}(\theta_i x)\operatorname{Tr}(\theta_j x) + \sum_{1 \leq u \leq n} \beta_u (\operatorname{Tr}(\theta_u x))^2.$$

Then $Q(x)$ is a DOPP of $\mathbb{F}_{q^n}$ if and only if

$$\gamma \in \operatorname{span}(\{\beta_1, \beta_2, \ldots, \beta_n\} \setminus \{\beta_i, \beta_j\}). \tag{12}$$

Proof. Indeed, $Q(x) = X(x)\Psi X(x)^T$, where $\Psi = [\psi_{uv}] \in \mathbb{F}_{q^n}^{n \times n}$ such that

$$\psi_{uv} = \begin{cases} \beta_u & \text{if } u = v, \\ \gamma & \text{if } u = i \text{ and } v = j, \\ 0 & \text{otherwise}, \end{cases}$$

and $X(x) = (\operatorname{Tr}(\theta_1 x), \operatorname{Tr}(\theta_2 x), \ldots, \operatorname{Tr}(\theta_n x))$. By Theorem 5, we need only prove that Ψ is a DOPM over $\mathbb{F}_{q^n}$ (i.e., $\#V = q^n$) if and only if (12) holds, where $V = \{\overline{X}\Psi\overline{X}^T : \overline{X} \in \mathbb{F}_q^n\}$.

We may without loss of generality assume that $i = 1$ and $j = 2$. Then

$$\Psi = \begin{bmatrix} \beta_1 & \gamma & \cdots & 0 \\ 0 & \beta_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \beta_n \end{bmatrix}.$$

Since $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, there are c_i's in $\mathbb{F}_q$ such that

$$\gamma = c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n.$$

Then

$$\begin{aligned} V &= \left\{ \overline{X}\Psi\overline{X}^T : \ \overline{X} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n \right\} \\ &= \left\{ \beta_1 x_1^2 + \beta_2 x_2^2 + \cdots + \beta_n x_n^2 + \gamma x_1 x_2 : x_i \in \mathbb{F}_q \right\} \\ &= \left\{ \textstyle\sum_{u=1}^{n} \beta_u (x_u^2 + c_u x_1 x_2) : x_i \in \mathbb{F}_q \right\}. \end{aligned} \tag{13}$$

Note that x^2 runs through all the elements of $\mathbb{F}_q$ when x runs over $\mathbb{F}_q$. Thus

$$\begin{aligned} V_0 &:= \left\{ X_0 \Psi X_0^T : X_0 = (0, x_2, x_3, \ldots, x_n) \in \mathbb{F}_q^n \right\} \\ &= \left\{ \beta_2 x_2^2 + \beta_3 x_3^2 + \cdots + \beta_n x_n^2 : x_i \in \mathbb{F}_q \right\} \\ &= \left\{ \lambda_2\beta_2 + \lambda_3\beta_3 + \cdots + \lambda_n\beta_n : \lambda_i \in \mathbb{F}_q \right\}. \end{aligned} \tag{14}$$

(i) If $\gamma \in \mathrm{span}(\{\beta_3, \beta_4, \ldots, \beta_n\})$, then $c_1 = c_2 = 0$, and so by (13),

$$V = \left\{ \beta_1 x_1^2 + \beta_2 x_2^2 + \textstyle\sum_{u=3}^{n} \beta_u (x_u^2 + c_u x_1 x_2) : x_i \in \mathbb{F}_q \right\}.$$

For $3 \le u \le n$ and any fixed $x_1, x_2 \in \mathbb{F}_q$, $x_u^2 + c_u x_1 x_2$ runs through $\mathbb{F}_q$ when x_u runs over $\mathbb{F}_q$. Hence $\#V = q^n$. (ii) If $\gamma \notin \mathrm{span}(\{\beta_3, \beta_4, \ldots, \beta_n\})$, then $c_1 \neq 0$ or $c_2 \neq 0$. We may assume, without loss of generality, that $c_1 \neq 0$. For fixed $a_2, \ldots, a_n \in \mathbb{F}_q$ with $a_2 \neq 0$, let $X_1 = (c_1 a_2, a_2, a_3, \ldots, a_n)$. By (13) and (14),

$$X_1 \Psi X_1^T = (1 + c_1 c_2) a_2^2 \beta_2 + \textstyle\sum_{u=3}^{n} (a_u^2 + c_u c_1 a_2^2) \beta_u \in V_0.$$

Thus there is a vector $X_0' = (0, x_2', \ldots, x_n') \in \mathbb{F}_q^n$ such that $X_0' \neq X_1$ and

$$X_1 \Psi X_1^T = X_0' \Psi {X_0'}^T.$$

So $\#V < q^n$. (iii) Hence $\#V = q^n$ if and only if $\gamma \in \mathrm{span}(\{\beta_3, \beta_4, \ldots, \beta_n\})$. □

Theorem 7 gives a simple criterion for $Q(x)$ to be a DOPP by employing the upper triangle matrix Ψ. However, it is difficult to find this criterion by using the coefficient matrix of $Q(x)$. Hence our method is preferable over quadratic forms.

Since $\{\theta_1, \theta_2, \ldots, \theta_n\}$ and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ are arbitrary bases, we can assume that they are normal bases and one is the dual basis of the other. In this case, the expression of $Q(x)$ becomes very explicit.

Corollary 1. *Let $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ be a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, and let $\{\beta, \beta^2, \ldots, \beta^{2^{n-1}}\}$ be its dual basis. For any $\gamma \in \mathbb{F}_{2^n}$ and $0 \le i \neq j \le n-1$, define*

$$Q(x) = \gamma\, \mathrm{Tr}(\alpha^{2^i} x)\mathrm{Tr}(\alpha^{2^j} x) + x.$$

Then $Q(x)$ is a DOPP of $\mathbb{F}_{2^n}$ if and only if

$$\gamma \in \mathrm{span}(\{\beta, \beta^2, \ldots, \beta^{2^{n-1}}\} \setminus \{\beta^{2^i}, \beta^{2^j}\}).$$

Proof. By Theorem 7, we need only show $\sum_{u=0}^{n-1}\beta^{2^u}(\mathrm{Tr}(\alpha^{2^u}x))^2 = x^{2^n}$. Indeed,

$$\begin{aligned}\sum_{0\le u\le n-1}\beta^{2^u}(\mathrm{Tr}(\alpha^{2^u}x))^2 &= \sum_{0\le u\le n-1}\beta^{2^u}\sum_{0\le k\le n-1}(\alpha^{2^u}x)^{2^{k+1}}\\ &= \sum_{0\le k\le n-1}\sum_{0\le u\le n-1}\beta^{2^u}(\alpha^{2^{k+1}})^{2^u}x^{2^{k+1}}\\ &= \sum_{0\le k\le n-1}\mathrm{Tr}(\beta\alpha^{2^{k+1}})x^{2^{k+1}}\\ &= x^{2^n}.\end{aligned}$$ □

Corollary 1 presents an explicit class of DOPPs of $\mathbb{F}_{2^n}$, where n is an arbitrary positive integer. However, the first 15 results of Table 1 in Section 4 require that n has an odd divisor or $n \equiv 4 \pmod 8$. Therefore, Corollary 1 provides new class of DOPPs.

In Theorem 7, if $\gamma = 0$, then Ψ becomes a diagonal matrix and $Q(x)$ degenerates into a linearized polynomial. Thus we can also investigate the permutation property of linearized polynomials by diagonal matrices.

Corollary 2. *Let $\{\theta_1,\theta_2,\ldots,\theta_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where q is even. Let*

$$Q(x) = \sum_{u=1}^{n}\beta_u\big(\mathrm{Tr}(\theta_u x)\big)^2,$$

where $\beta_1,\beta_2,\ldots,\beta_n \in \mathbb{F}_{q^n}$. Then the following statements hold:

(1) *$Q(x)$ is a permutation polynomial over $\mathbb{F}_{q^n}$ if and only if $\{\beta_1,\beta_2,\ldots,\beta_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$;*
(2) *$\dim_{\mathbb{F}_q}(\mathrm{Ker}(Q)) = k$ if and only if $\mathrm{Rank}_{\mathbb{F}_q}\{\beta_1,\beta_2,\ldots,\beta_n\} = n-k$, where $0\le k\le n$.*

Note that $Q(x)$ in Corollary 2 is affine equivalent to $L(x) = \sum_{u=1}^{n}\beta_u\mathrm{Tr}(\theta_u x)$, and $(\mathrm{Tr}(\theta_1 x),\ldots,\mathrm{Tr}(\theta_n x))$ runs through $\mathbb{F}_q^n$ if and only if $(\mathrm{Tr}(\theta_1 x)^2,\ldots,\mathrm{Tr}(\theta_n x)^2)$ runs through $\mathbb{F}_q^n$. Therefore, Corollary 2 is equivalent to Theorems 1 to 3, and thus Theorem 7 is a generalization of the results in [17, 28, 30].

We next give another important result of this paper, which generalizes the sufficient condition in Theorem 7 for $Q(x)$ to be a DOPP.

Theorem 8. *Let $\{\beta_1,\beta_2,\ldots,\beta_n\}$ be any basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where q is even. For any subset S of $\{1,2,\ldots,n\}$ with $\#S\ge 2$, define an upper triangular matrix $\Psi = [\psi_{uv}]_{n\times n}$ over $\mathbb{F}_{q^n}$ as follows:*

$$\psi_{uv} = \begin{cases}\beta_u & \text{if } u=v,\\ \gamma_{uv} & \text{if } u,v\in S \text{ and } u<v,\\ 0 & \text{otherwise,}\end{cases} \tag{15}$$

where $\gamma_{uv}\in\mathbb{F}_{q^n}$. Let $\Gamma = \{\gamma_{uv} : u,v\in S \text{ and } u<v\}$ and $\Upsilon = \{\beta_i : i\in\{1,2,\ldots,n\}\setminus S\}$. If $\Gamma\subseteq \mathrm{span}(\Upsilon)$, then Ψ is a DOPM over $\mathbb{F}_{q^n}$ and

$$Q(x) := \sum_{u,v\in S,\, u<v}\gamma_{uv}\,\mathrm{Tr}(\theta_u x)\mathrm{Tr}(\theta_v x) + \sum_{1\le u\le n}\beta_u(\mathrm{Tr}(\theta_u x))^2 \tag{16}$$

is a DOPP of $\mathbb{F}_{q^n}$, where $\{\theta_1,\theta_2,\ldots,\theta_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Proof. By Theorem 5, we need only prove that Ψ is a DOPM. Let $T = \{1, 2, \ldots, n\} \setminus S$. Then $\Upsilon = \{\beta_t : t \in T\}$ and so

$$\text{span}(\Upsilon) = \Big\{ \sum_{t \in T} a_t \beta_t : a_t \in \mathbb{F}_q \Big\}.$$

(When $S = \{1, 2, \ldots, n\}$, Υ is an empty set and $\text{span}(\Upsilon) = \{0\}$ by Definition 3.) If $\gamma_{uv} \in \text{span}(\Upsilon)$ for all $u, v \in S$ and $u < v$, then

$$\gamma_{uv} = \sum_{t \in T} b_{uvt} \beta_t \quad \text{for some } b_{uvt} \in \mathbb{F}_q.$$

Since $S \cup T = \{1, 2, \ldots, n\}$, we have

$$\begin{aligned} V &= \Big\{ \overline{X} \Psi \overline{X}^T : \ \overline{X} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n \Big\} \\ &= \Big\{ \sum_{s \in S} \beta_s x_s^2 + \sum_{t \in T} \beta_t x_t^2 + \sum_{u < v \in S} \gamma_{uv} x_u x_v : x_1, x_2, \ldots, x_n \in \mathbb{F}_q \Big\} \\ &= \Big\{ \sum_{s \in S} \beta_s x_s^2 + \sum_{t \in T} \beta_t \Big(x_t^2 + \sum_{u < v \in S} b_{uvt} x_u x_v \Big) : x_1, x_2, \ldots, x_n \in \mathbb{F}_q \Big\}. \end{aligned}$$

Since $T = \{1, 2, \ldots, n\} \setminus S$ and q is even, for any fixed $x_u, x_v \in \mathbb{F}_q$,

$$x_t^2 + \sum_{u < v \in S} b_{uvt} x_u x_v$$

runs through all the elements of $\mathbb{F}_q$ when x_t runs over $\mathbb{F}_q$. Hence $\#V = q^n$, and so Ψ is a DOPM over $\mathbb{F}_{q^n}$. □

Theorem 8 provides a simple method for constructing DOPMs and DOPPs. Next we give an example to illustrate this method.

Corollary 3. *Let $n = 5$ and $\{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5\}$ be any basis of $\mathbb{F}_{q^5}$ over $\mathbb{F}_q$. Define four square matrices of size 5 over $\mathbb{F}_{q^5}$ as follows:*

$$\Psi_1 = \begin{bmatrix} \beta_1 & \psi_{12} & \psi_{13} & \psi_{14} & 0 \\ 0 & \beta_2 & \psi_{23} & \psi_{24} & 0 \\ 0 & 0 & \beta_3 & \psi_{34} & 0 \\ 0 & 0 & 0 & \beta_4 & 0 \\ 0 & 0 & 0 & 0 & \beta_5 \end{bmatrix}, \quad \Psi_2 = \begin{bmatrix} \beta_1 & \psi_{12} & \psi_{13} & 0 & 0 \\ 0 & \beta_2 & \psi_{23} & 0 & 0 \\ 0 & 0 & \beta_3 & 0 & 0 \\ 0 & 0 & 0 & \beta_4 & 0 \\ 0 & 0 & 0 & 0 & \beta_5 \end{bmatrix},$$

$$\Psi_3 = \begin{bmatrix} \beta_1 & \psi_{12} & \psi_{13} & 0 & \psi_{15} \\ 0 & \beta_2 & \psi_{23} & 0 & \psi_{25} \\ 0 & 0 & \beta_3 & 0 & \psi_{35} \\ 0 & 0 & 0 & \beta_4 & 0 \\ 0 & 0 & 0 & 0 & \beta_5 \end{bmatrix}, \quad \Psi_4 = \begin{bmatrix} \beta_1 & 0 & \psi_{13} & 0 & \psi_{15} \\ 0 & \beta_2 & 0 & 0 & 0 \\ 0 & 0 & \beta_3 & 0 & \psi_{35} \\ 0 & 0 & 0 & \beta_4 & 0 \\ 0 & 0 & 0 & 0 & \beta_5 \end{bmatrix}.$$

Then the following statements hold:

(1) *If $\psi_{ij} \in \text{span}(\{\beta_5\})$ for all $1 \le i < j \le 4$, then Ψ_1 is a DOPM;*

(2) *If* $\psi_{ij} \in \operatorname{span}(\{\beta_4, \beta_5\})$ *for all* $1 \le i < j \le 3$, *then* Ψ_2 *is a DOPM;*
(3) *If* $\psi_{ij} \in \operatorname{span}(\{\beta_4\})$ *for all* $i, j \in \{1, 2, 3, 5\}$ *and* $i < j$, *then* Ψ_3 *is a DOPM;*
(4) *If* $\psi_{ij} \in \operatorname{span}(\{\beta_2, \beta_4\})$ *for all* $i, j \in \{1, 3, 5\}$ *and* $i < j$, *then* Ψ_4 *is a DOPM.*

Since $\{\theta_1, \theta_2, \dots, \theta_n\}$ and $\{\beta_1, \beta_2, \dots, \beta_n\}$ are arbitrary bases, we can assume that the first one is a polynomial basis and the other is the dual basis. In this case, the expression of $Q(x)$ becomes very explicit.

Example 1. *Let* $\{1, g, g^2, g^3, g^4, g^5, g^6, g^7\}$ *be a basis of* $\mathbb{F}_{2^8}$ *over* $\mathbb{F}_2$, *where* g *is a root of* $x^8 + x^4 + x^3 + x^2 + 1$. *Then its dual basis is* $\{g^{252}, g^{251}, g^{45}, g^{98}, g, 1, g^{254}, g^{253}\}$. *Define*

$$Q(x) = \gamma_{12} \operatorname{Tr}(x)\operatorname{Tr}(gx) + \gamma_{13} \operatorname{Tr}(x)\operatorname{Tr}(g^2x) + \gamma_{23} \operatorname{Tr}(gx)\operatorname{Tr}(g^2x) + x,$$

where $\operatorname{Tr}(x) = \sum_{k=0}^{7} x^{2^k}$. *Then* $Q(x)$ *is a DOPP of* $\mathbb{F}_{2^8}$ *if*

$$\{\gamma_{12}, \gamma_{13}, \gamma_{23}\} \subseteq \operatorname{span}(\{g^{98}, g, 1, g^{254}, g^{253}\}).$$

4. Comparison with known DO permutation polynomials

To show a permutation f is new, one usually has to prove that f is not affine equivalent (Definition 2) to known permutations, see for example [4, 9, 22]. In this section, we also use affine equivalence to show that our DOPPs are new. Obviously, the affine equivalence class of DOPPs are also DOPPs. Therefore, we need only show that DOPPs constructed in this paper are new compared to other DOPPs. To this end, we list all infinite classes of DOPPs we know in Table 1.

In the third column of Table 1, each n has an odd divisor or $n \equiv 4 \pmod 8$ for $1 \le i \le 15$. However, n is arbitrary positive integer for $i = 16, 17$ by Corollary 1 and Theorem 8, and Theorem 7 contains the following new DOPPs over $\mathbb{F}_{2^n}$ with $n = 8$.

Example 2. *Let* $\{\beta_1, \beta_2, \dots, \beta_8\}$ *and* $\{\theta_1, \theta_2, \dots, \theta_8\}$ *be two bases of* $\mathbb{F}_{2^8}$ *over* $\mathbb{F}_2$. *For any* $\gamma \in \mathbb{F}_{2^8}$ *and fixed* $i, j \in \{1, 2, \dots, 8\}$ *with* $i \ne j$, *define*

$$Q(x) = \gamma \operatorname{Tr}(\theta_i x)\operatorname{Tr}(\theta_j x) + \sum_{1 \le u \le 8} \beta_u \operatorname{Tr}(\theta_u x),$$

where $\operatorname{Tr}(x) = \sum_{k=0}^{7} x^{2^k}$. *Then* $Q(x)$ *is a DOPP of* $\mathbb{F}_{2^8}$ *if and only if*

$$\gamma \in \operatorname{span}(\{\beta_1, \beta_2, \dots, \beta_8\} \setminus \{\beta_i, \beta_j\}).$$

Table 1: Infinite classes of DO permutation polynomials over $\mathbb{F}_{2^n}$

i	f_i	Conditions	Ref.
1	x^{2^m+1}	$n/\gcd(m,n)$ is odd	[6]
2	$x^{2^m+2}+ax$	$n=2m$, m is odd, $a\in\mathbb{F}_{2^n}^*$, and $\mathrm{ord}(a^{q-1})=3$	[31]
3	$x^{2^{2m}+2^{m+s}}+a^{1-2^m}x^{2^s+1}$	$n=3m$, $3\nmid m$, $3\mid m+s$, $\mathbb{F}_{2^n}^*=\langle a\rangle$, $\gcd(n,s)\mid m$, and $m/\gcd(n,s)$ is odd	[2]
4	$x^{2^{m+1}+1}+x^3+x$	$n=2m+1$	[5]
5	$x^{2^{2m}+1}+x^{2^m+1}+ax$	$n=3m$, $a\in\mathbb{F}_{2^m}\setminus\{0,1\}$	[23]
6	$x^{2^{m+2}+1}+x^{2^m+4}+x^5$	$n=2m$, m is odd	[7]
7	$x^{2^{m+2}+2^m}+x^{2^m+4}+x^5$	$n=2m$, $m\equiv 2\ (\mathrm{mod} 4)$	[29]
8	$x^{2^{m+2}+2^m}+x^{2^{m+2}+1}+x^5$	$n=2m$, $m\equiv 2\ (\mathrm{mod} 4)$	[29]
9	$bx^{2^{m+1}+1}+ax^{2^m+2}+x^3$	$n=2m$, m is odd, $a,b\in\mathbb{F}_{2^m}^*$, and others	[20]
10	$x^{2^{m+1}+2^m}+bx^{2^m+2}+cx^3$	$n=2m$, m is odd, $b,c\in\mathbb{F}_{2^m}^*$, and others	[19, 29]
11	$cx^{2^{m+1}+2^m}+bx^{2^{m+1}+1}+x^3$	$n=2m$, m is odd, $b,c\in\mathbb{F}_{2^m}^*$, and others	[20, 29]
12	$x^{2^{m+k}}(c_0x^{2^m}+c_1x)+x^{2^k}(c_2x^{2^m}+c_3x)$	$n=2m$, m is odd, $c_i\in\mathbb{F}_{2^n}$, and others	[10, 11, 14–16, 24–27]
13	$x(\mathrm{Tr}(x)+ax)$	$n=k\ell$, k is odd, $a\in\mathbb{F}_{2^\ell}\setminus\{0,1\}$	[1]
14	$x(L(\mathrm{Tr}(x))+a\mathrm{Tr}(x)+ax)$	$n=k\ell$, k is odd, $a\in\mathbb{F}_{2^\ell}^*$, $xL(x)$ permutes $\mathbb{F}_{2^\ell}$	[12]
15	$x(L(\mathrm{Tr}(x))+a\mathrm{Tr}(x)+ax+b)$	$n=k\ell$, $k>1$ is odd, $a\in\mathbb{F}_{2^\ell}^*$, $b\in\mathbb{F}_{2^\ell}$, and $x(L(x)+b)$ permutes $\mathbb{F}_{2^\ell}$	[22]
16	$\gamma\,\mathrm{Tr}(\alpha^{2^i}x)\mathrm{Tr}(\alpha^{2^j}x)+x$	n is arbitrary, $\gamma\in\mathrm{span}(\{\beta,\beta^2,\ldots,\beta^{2^{n-1}}\}\setminus\{\beta^{2^i},\beta^{2^j}\})$	Corollary 1
17	$Q(x)$ in Theorem 8	see Theorem 8	Theorem 8

* Note that f_{16} is a special case of f_{17}.

† In Lines 13 to 15, $\mathrm{Tr}(x)=\sum_{j=0}^{k-1}x^{2^{j\ell}}$ and $L(x)=\sum_{t=0}^{\ell-1}a_tx^{2^t}\in\mathbb{F}_{2^\ell}[x]$.

Conflict of Interest The authors declared that they have no conflicts of interest.
Data Availability The authors do not have any research data outside the manuscript.

References

[1] A. Blokhuis, R. S. Coulter, M. Henderson, and C. M. O'Keefe. Permutations amongst the Dembowski–Ostrom polynomials. In D. Jungnickel and H. Niederreiter, editors, *Finite Fields and Applications: Proceedings of the Fifth International Conference on Finite Fields and Applications*, pages 37–42, 2001.

[2] C. Bracken, C. H. Tan, and Y. Tan. Binomial differentially 4 uniform permutations with high nonlinearity. *Finite Fields Appl.*, 18(3):537–546, 2012.

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

[4] L. E. Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Part I. *Ann. Math.*, 11: 65–120, 1896.

[5] H. Dobbertin. Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: the Welch case. *IEEE Trans. Inf. Theory*, 45(4):1271–1275, 1999.

[6] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Trans. Inf. Theory*, IT-14(1):154–156, Jan. 1968.

[7] R. Gupta and R. K. Sharma. Some new classes of permutation trinomials over finite fields with even characteristic. *Finite Fields Appl.*, 41:89–96, 2016.

[8] X.-D. Hou. Affinity of permutations of $\mathbb{F}_2^n$. *Discrete Appl. Math.*, 154(2):313–325, 2006.

[9] X.-D. Hou. Permutation polynomials over finite fields—a survey of recent advances. *Finite Fields Appl.*, 32:82–119, 2015.

[10] K. H. Kim, S. Mesnager, J. H. Choe, D. N. Lee, S. Lee, and M. C. Jo. On permutation quadrinomials with boomerang uniformity 4 and the best-known nonlinearity. *Des. Codes Cryptogr.*, 90:1437–1461, 2022.

[11] K. H. Kim, S. Mesnager, C. H. Kim, and M. C. Jo. Completely characterizing a class of permutation quadrinomials. *Finite Fields Appl.*, 87:102155, 2023.

[12] Y. Laigle-Chapuy. A note on a class of quadratic permutations over $\mathbb{F}_{2^n}$. In S. Boztaş and H.-F. Lu, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium, AAECC-17*, volume 4851 of *LNCS*, pages 130–137, 2007.

[13] K. Li, L. Qu, B. Sun, and C. Li. New results about the boomerang uniformity of permutation polynomials. *IEEE Trans. Inf. Theory*, 65(11):7542–7553, Nov. 2019.

[14] K. Li, L. Qu, C. Li, and H. Chen. On a conjecture about a class of permutation quadrinomials. *Finite Fields Appl.*, 66:101690, 2020.

[15] K. Li, C. Li, T. Helleseth, and L. Qu. Cryptographically strong permutations from the butterfly structure. *Des. Codes Cryptogr.*, 89:737–761, 2021.

[16] N. Li, M. Xiong, and X. Zeng. On permutation quadrinomials and 4-uniform BCT. *IEEE Trans. Inf. Theory*, 67(7):4845–4855, 2021.

[17] S. Ling and L. Qu. A note on linearized polynomials and the dimension of their kernels. *Finite Fields Appl.*, 18:56–62, 2012.

[18] S. Mesnager, C. Tang, and M. Xiong. On the boomerang uniformity of quadratic permutations. *Des. Codes Cryptogr.*, 88:2233–2246, 2020.

[19] F. Özbudak and B. G. Temür. Classification of permutation polynomials of the form $x^3g(x^{q-1})$ of $\mathbb{F}_{q^2}$ where $g(x) = x^3 + bx + c$ and $b, c \in \mathbb{F}_q^*$. *Des. Codes Cryptogr.*, 90: 1537–1556, 2022.

[20] F. Özbudak and B. G. Temür. Complete characterization of some permutation polynomials of the form $x^r(1 + ax^{s_1(q-1)} + bx^{s_2(q-1)}$ over $\mathbb{F}_{q^2}$. *Cryptogr. Commun.*, 15:775–793, 2023.

[21] J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In U. Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, volume 1070 of *LNCS*, pages 33–48, 1996.

[22] S. Samardjiska and D. Gligoroski. Quadratic permutations, complete mappings and mutually orthogonal Latin squares. *Math. Slovaca*, 67(5):1129–1146, 2017.

[23] Z. Tu, X. Zeng, and L. Hu. Several classes of complete permutation polynomials. *Finite Fields Appl.*, 25:182–193, 2014.

[24] Z. Tu, X. Zeng, and T. Helleseth. New permutation quadrinomials over $\mathbb{F}_{2^{2m}}$. *Finite Fields Appl.*, 50:304–318, 2018.

[25] Z. Tu, X. Liu, and X. Zeng. A revisit to a class of permutation quadrinomials. *Finite Fields Appl.*, 59:57–85, 2019.

[26] Z. Tu, N. Li, X. Zeng, and J. Zhou. A class of quadrinomial permutations with boomerang uniformity four. *IEEE Trans. Inf. Theory*, 66(6):3753–3765, 2020.

[27] Y. Wu, L. Wang, N. Li, X. Zeng, and X. Tang. On the boomerang uniformity of a class of permutation quadrinomials over finite fields. *Discrete Math.*, 345(10): 113000, 2022.

[28] P. Yuan and X. Zeng. A note on linear permutation polynomials. *Finite Fields Appl.*, 17(5):488–491, 2011.

[29] Z. Zha, L. Hu, and S. Fan. Further results on permutation trinomials over finite fields with even characteristic. *Finite Fields Appl.*, 45:43–52, 2017.

[30] K. Zhou. A remark on linear permutation polynomials. *Finite Fields Appl.*, 14: 532–536, 2008.

[31] M. E. Zieve. Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal Latin squares. arXiv:1312.1325v3, 2013.