Finite Fields and Their Applications 89 (2023) 102193

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

A general construction of permutation polynomials of $\mathbb{F}_{q^2}$

Xiang-dong Hou [*], Vincenzo Pallozzi Lavorante [1]

Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620, United States of America

ARTICLE INFO

Article history:
Received 29 June 2022
Received in revised form 31 January 2023
Accepted 13 February 2023
Available online xxxx
Communicated by Gary L. Mullen

MSC:
11T06
11T30
11T55

Keywords:
Finite field
Permutation polynomial
Self-dual polynomial

ABSTRACT

Let r be a positive integer, $h(X) \in \mathbb{F}_{q^2}[X]$, and μ_{q+1} be the subgroup of order $q+1$ of $\mathbb{F}_{q^2}^*$. It is well known that $X^r h(X^{q-1})$ permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(r, q-1) = 1$ and $X^r h(X)^{q-1}$ permutes μ_{q+1}. There are many ad hoc constructions of permutation polynomials of $\mathbb{F}_{q^2}$ of this type such that $h(X)^{q-1}$ induces monomial functions on the cosets of a subgroup of μ_{q+1}. We give a general construction that can generate, through an algorithm, *all* permutation polynomials of $\mathbb{F}_{q^2}$ with this property, including many which are not known previously. The construction is illustrated explicitly for permutation binomials and trinomials.

* Corresponding author.
E-mail addresses: xhou@usf.edu (X.-d. Hou), vincenzop@usf.edu (V. Pallozzi Lavorante).

[1] The research of Vincenzo Palozzi Lavorante was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM) and the National Science Foundation under Grant No. 2127742.

https://doi.org/10.1016/j.ffa.2023.102193
1071-5797/

1. Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements. A polynomial $f(X) \in \mathbb{F}_q[X]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a permutation of $\mathbb{F}_q$. Let r be a positive integer, $d \mid q-1$, and $h(X) \in \mathbb{F}_q[X]$. It is well known [10,12,16] that $X^r h(X^{(q-1)/d})$ is a PP of $\mathbb{F}_q$ if and only if $\gcd(r,(q-1)/d) = 1$ and $X^r h(X)^{(q-1)/d}$ permutes the multiplicative group $\mu_d := \{x \in \mathbb{F}_q^* : x^d = 1\}$. (In general, we use μ_m to denote a multiplicative group of order m of a finite field.) Replacing q with q^2 and d with $q+1$, we see that for $h(X) \in \mathbb{F}_{q^2}[X]$, $X^r h(X^{q-1})$ is a PP of $\mathbb{F}_{q^2}$ if and only if $\gcd(r, q-1) = 1$ and $X^r h(X)^{q-1}$ permutes μ_{q+1}. To facilitate the constructions of permutations of μ_{q+1} of the form $X^r h(X)^{q-1}$, the following idea has been used by several authors [1,6,7,11,15]: Let H be a subgroup of μ_{q+1} of small index. Construct a polynomial $h(X) \in \mathbb{F}_{q^2}[X]$ such that $h(X)^{q-1}$ induces monomial functions on each coset of H in μ_{q+1}. With such a property, $X^r h(X)^{q-1}$ permutes μ_{q+1} if and only if some simple number theoretic conditions on the parameters are satisfied. This method has produced many results. However, these results only deal with specific situations, leaving a unified treatment to be desired.

In the present paper, we take a general approach to the question. The main result is an algorithm (Algorithm 2.4) that produces *all* PPs of $\mathbb{F}_{q^2}$ of the form $X^r h(X^{q-1})$ such that $h(X)^{q-1}$ induces monomial functions on the cosets of a subgroup in μ_{q+1}. The order of an element a in a group is denoted by $o(a)$. Let $d \mid q+1$ and $\epsilon \in \mathbb{F}_{q^2}^*$ be such that $o(\epsilon) = d$. Define

$$A_k = \{x \in \mu_{q+1} : x^{(q+1)/d} = \epsilon^k\}, \quad 0 \le k < d. \tag{1.1}$$

Then $A_0 = \mu_{(q+1)/d}$, and $A_0, \ldots, A_{d-1}$ are the cosets of $\mu_{(q+1)/d}$ in μ_{q+1}, whence

$$\mu_{q+1} = \bigsqcup_{k=0}^{d-1} A_k. \tag{1.2}$$

Since $X^{n_1(q-1)} \equiv X^{n_2(q-1)} \pmod{X^{q^2-1}-1}$ whenever $n_1 \equiv n_2 \pmod{q+1}$, it suffices to consider $h \in \mathbb{F}_{q^2}[X]$ with $\deg h \le q$. Write

$$h(X) = \sum_{\substack{0 \le i < (q+1)/d \\ 0 \le j < d}} a_{ij} X^{i+j(q+1)/d}. \tag{1.3}$$

The objective is to find conditions on $a_{ij} \in \mathbb{F}_{q^2}$ such that for every $0 \le k < d$,

$$x^r h(x)^{q-1} = \lambda_k x^{e_k} \text{ for all } x \in A_k, \tag{1.4}$$

where $e_k \in \mathbb{Z}$ and $\lambda_k \in \mu_{q+1}$, say $\lambda_k \in A_{\pi(k)}$.

Theorem 1.1. *Assume that* (1.4) *is satisfied for all* $0 \le k < d$. *Then* $X^r h(X)^{q-1}$ *permutes* μ_{q+1} *if and only if*

$$\gcd\Big(e_k, \frac{q+1}{d}\Big) = 1, \quad 0 \le k < d,$$

and

$$k \mapsto \pi(k) + e_k k$$

is a permutation of $\mathbb{Z}/d\mathbb{Z}$.

Proof. By (1.4), $X^r h(X)^{q-1}$ maps A_k to $A_{\pi(k)+e_k k}$. This map is one-to-one on A_k if and only if $\gcd(e_k, (q+1)/d) = 1$. Hence the conclusion is true. □

Therefore, the crucial question is to determine the polynomials $h(X)$ satisfying (1.4). In Section 2, we will resolve this question and we will describe an algorithm that produces all PPs of the form $X^r h(X^{q-1})$ of $\mathbb{F}_{q^2}$ satisfying (1.4). In Section 3, we determine all permutation binomials of $\mathbb{F}_{q^2}$ resulting from this algorithm and it turns out that these permutation binomials were all known previously. In Section 4, we determine all permutation trinomials of $\mathbb{F}_{q^2}$ resulting from the algorithm. There are four classes such permutation trinomials, excluding those that were previously known. These four classes, in their generality, appear to be new, although many special cases have been discovered by other authors. Additional examples of the algorithm are given in Section 5. Overall, this approach reveals many PPs that were not known previously.

Remark. In the present paper, we investigate polynomials $h(X) \in \mathbb{F}_{q^2}[X]$ such that $h(X)^{q-1}$ induces monomial functions on the cosets of a subgroup of μ_{q+1} and permutes μ_{q+1} as a whole. Before this approach became popular in recent years, people had explored a similar method for PPs of $\mathbb{F}_q$. Several authors [2,9,12–14] had studied PPs of $\mathbb{F}_q$ which induce monomial functions on the cosets of a subgroup of $\mathbb{F}_q^*$.

2. The construction

For $a \in \mathbb{F}_{q^2}$, define $\bar{a} = a^q$; for $f(X) = \sum_{i=0}^n a_i X^i \in \mathbb{F}_{q^2}[X]$ with $a_n \neq 0$, define

$$\bar{f}(X) = \sum_{i=0}^n \bar{a}_i X^i$$

and

$$\tilde{f}(X) = X^n \bar{f}(X^{-1}) = \sum_{i=0}^n \bar{a}_i X^{n-i}.$$

Obviously, $\bar{\bar{f}} = f$ and $\tilde{\tilde{f}} = f$. If $\tilde{f} = cf$ for some $c \in \mathbb{F}_{q^2}^*$, f is said to be *self-dual*; in this case, it is necessary that $c \in \mu_{q+1}$. Self-dual polynomials were first introduced in [4] for a different purpose; they will also play an important role in the present paper.

We follow the notation of Section 1. Let $h(X)$ be given in (1.3) and assume that h has no roots in μ_{q+1}. For $x \in A_k$, where $0 \le k < d$, we have

$$h(x) = \sum_{i,j} a_{ij} \epsilon^{jk} x^i = \sum_i M_{ik} x^i, \tag{2.1}$$

where

$$M_{ik} = \sum_j a_{ij} \epsilon^{jk}. \tag{2.2}$$

Note that the $((q+1)/d) \times d$ matrices $[M_{ik}]$ and $[a_{ij}]$ are related by the $d \times d$ Vandermonde matrix $[\epsilon^{jk}]$:

$$[M_{ik}] = [a_{ij}]\,[\epsilon^{jk}], \qquad [a_{ij}] = \frac{1}{d}\,[M_{ik}]\,[\epsilon^{-kj}].$$

By (2.1), for $x \in \mu_{q+1}$,

$$x^r h(x)^{q-1} = x^r \frac{h(x)^q}{h(x)} = x^r \frac{\sum_i \overline{M}_{ik}\, x^{-i}}{\sum_i M_{ik}\, x^i}. \tag{2.3}$$

Write

$$\sum_i M_{ik} X^i = X^s L(X), \tag{2.4}$$

where $L(X) \in \mathbb{F}_{q^2}[X]$, $L(0) \ne 0$, $\deg L = t$, $s + t < (q+1)/d$. Then (2.3) becomes

$$x^r h(x)^{q-1} = x^r \frac{x^{-s} \bar{L}(x^{-1})}{x^s L(x)} = x^{r-2s-t} \frac{\tilde{L}(x)}{L(x)}. \tag{2.5}$$

The following lemma is crucial.

Lemma 2.1. *Let $L(X) \in \mathbb{F}_{q^2}[X]$ be such that $L(0) \ne 0$, $\deg L = t < (q+1)/d$, and $L(X)$ has no roots in A_k.*

(i) *Assume that there exist $0 \le \tau < (q+1)/d$ and $\lambda \in \mu_{q+1}$ such that*

$$\frac{\tilde{L}(x)}{L(x)} = \lambda x^\tau \quad \text{for all } x \in A_k. \tag{2.6}$$

Then either $\tau = 0$ or $(q+1)/d - t \le \tau \le t$.

(ii) *When* $\tau = 0$, (2.6) *is satisfied if and only if*

$$\tilde{L}(X) = \lambda L(X). \tag{2.7}$$

(iii) *When* $(q+1)/d - t \le \tau \le t$, (2.6) *is satisfied if and only if*

$$L(X) = P(X) + X^{(q+1)/d-\tau} Q(X), \tag{2.8}$$

where $P, Q \in \mathbb{F}_{q^2}[X]$, $\deg P = t - \tau$, $\tilde{P} = \lambda P$, $\deg Q = \tau + t - (q+1)/d$, $\tilde{Q} = \lambda \epsilon^k Q$.

Proof. (ii) Since $\deg(\tilde{L} - \lambda L) \le t < (q+1)/d = |A_k|$,

$$\tilde{L}(x) = \lambda L(x) \text{ for all } x \in A_k \;\Leftrightarrow\; \tilde{L}(X) - \lambda L(X) = 0.$$

(iii) ($\Rightarrow$) We have $X^{(q+1)/d} - \epsilon^k \mid \tilde{L}(X) - \lambda X^\tau L(X)$, say

$$\tilde{L}(X) - \lambda X^\tau L(X) = g(X)(\epsilon^k - X^{(q+1)/d}), \tag{2.9}$$

where $g(X) \in \mathbb{F}_{q^2}[X]$ with $\deg g = \tau + t - (q+1)/d$. In (2.9),

$$\begin{aligned}
\widetilde{\tilde{L} - \lambda X^\tau L} &= X^{\tau+t}\big(\tilde{\tilde{L}}(X^{-1}) - \bar{\lambda} X^{-\tau} \bar{L}(X^{-1})\big) \\
&= X^\tau \tilde{\tilde{L}} - \bar{\lambda} \tilde{L} \\
&= X^\tau L - \bar{\lambda} \tilde{L} \\
&= -\bar{\lambda}(\tilde{L} - \lambda X^\tau L).
\end{aligned}$$

Hence

$$\widetilde{g(X)(\epsilon^k - X^{(q+1)/d})} = -\bar{\lambda} g(X)(\epsilon^k - X^{(q+1)/d}),$$

i.e.,

$$\tilde{g}(X)(\epsilon^{-k} X^{(q+1)/d} - 1) = -\bar{\lambda} g(X)(\epsilon^k - X^{(q+1)/d}),$$

whence $\tilde{g} = \bar{\lambda} \epsilon^k g$. Therefore, (2.9) becomes

$$\tilde{L} - \lambda X^\tau L = \lambda \tilde{g} - X^{(q+1)/d} g. \tag{2.10}$$

Let $L = a_0 + \cdots + a_t X^t$ and $g = b_0 + \cdots + b_v X^v$, where $v = \deg g = \tau + t - (q+1)/d$. The coefficients of $\tilde{L} - \lambda X^\tau L$ and $\lambda \tilde{g} - X^{(q+1)/d} g$ are illustrated in Fig. 1. It follows from (2.10) and Fig. 1 that $a_i = 0$ for $t - \tau < i < t - v$, $a_{t-\tau} \neq 0$, and

$$\begin{aligned}
L &= a_0 + \cdots + a_{t-\tau} X^{t-\tau} + X^{(q+1)/d-\tau}(a_{t-v} + \cdots + a_t X^v) \\
&= P(X) + X^{(q+1)/d-\tau} Q(X),
\end{aligned}$$

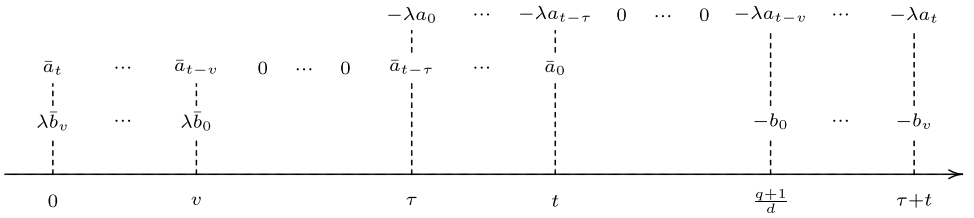

Fig. 1. The coefficients of $-\lambda X^\tau L$, $\tilde{L}$ and $\lambda\tilde{g} - X^{(q+1)/d}g$ (from top to bottom).

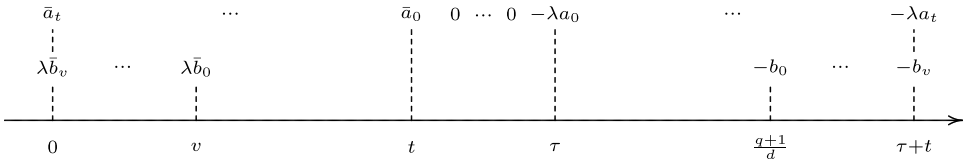

Fig. 2. The coefficients of $\tilde{L} - \lambda X^\tau L$ (top) and $\lambda\tilde{g} - X^{(q+1)/d}g$ (bottom).

where $P(X) = a_0 + \cdots + a_{t-\tau}X^{t-\tau}$, which satisfies $\tilde{P} = \lambda P$, and $Q(X) = a_{t-v} + \cdots + a_t X^v = -\bar{\lambda}g(X)$, which satisfies $\tilde{Q} = -\lambda\tilde{g} = -\lambda\bar{\lambda}\epsilon^k g = \lambda\epsilon^k Q$.

($\Leftarrow$) We have

$$\begin{aligned}
\tilde{L} - \lambda X^\tau L &= \widetilde{(P + X^{(q+1)/d-\tau}Q)} - \lambda X^\tau (P + X^{(q+1)/d-\tau}Q) \\
&= X^t\big(\bar{P}(X^{-1}) + X^{-((q+1)/d-\tau)}\bar{Q}(X^{-1})\big) - \lambda X^\tau (P + X^{(q+1)/d-\tau}Q) \\
&= X^t\bar{P}(X^{-1}) + X^v\bar{Q}(X^{-1}) - \lambda X^\tau (P + X^{(q+1)/d-\tau}Q) \\
&= X^\tau\tilde{P} + \tilde{Q} - \lambda X^\tau (P + X^{(q+1)/d-\tau}Q) \\
&= X^\tau\lambda P + \lambda\epsilon^k Q - \lambda X^\tau (P + X^{(q+1)/d-\tau}Q) \\
&= \lambda Q(\epsilon^k - X^{(q+1)/d}).
\end{aligned}$$

Hence

$$\frac{\tilde{L}(x)}{L(x)} = \lambda x^\tau \quad \text{for all } x \in A_k.$$

(i) Assume $\tau > 0$. By the proof of (iii) ($\Rightarrow$), $\tau + t - (q+1)/d = \deg g \geq 0$, whence $\tau \geq (q+1)/d - t$. It remains to show that $\tau \leq t$. Assume to the contrary that $\tau > t$. Then Fig. 1 is replaced by Fig. 2. Then $a_0 = 0$, which is a contradiction. □

Definition 2.2. Let $0 \leq k < d$, $0 \leq t < (q+1)/d$ and $\lambda \in \mu_{q+1}$. Define

$$\mathcal{L}_k(t, 0; \lambda) = \{L \in \mathbb{F}_{q^2}[X] : \deg L = t,\ \tilde{L} = \lambda L,\ \gcd(L, X^{(q+1)/d} - \epsilon^k) = 1\}, \qquad (2.11)$$

and for $(q+1)/d - t \leq \tau \leq t$, define

$$\mathcal{L}_k(t,\tau;\lambda) = \{L = P + X^{(q+1)/d-\tau}Q : P, Q \in \mathbb{F}_{q^2}[X], \quad (2.12)$$
$$\deg P = t-\tau,\ \tilde{P} = \lambda P,\ \deg Q = \tau + t - (q+1)/d,$$
$$\tilde{Q} = \lambda\epsilon^k Q,\ \gcd(L, X^{(q+1)/d} - \epsilon^k) = 1\}.$$

It follows from (2.4), (2.5) and Lemma 2.1 that $X^r h(X)^{q-1}$ is a monomial function on A_k if and only if there exist $s, t \geq 0$ with $s + t < (q+1)/d$, $\lambda \in \mu_{q+1}$, and integer $\tau \in \{0\} \cup [(q+1)/d - t, t]$ such that $\sum_i M_{ik} X^i = X^s L(X)$, where $L \in \mathcal{L}_k(t,\tau;\lambda)$. When this happens,

$$x^r h(x)^{q-1} = \lambda x^{r-2s-t+\tau} \quad \text{for all } x \in A_k. \quad (2.13)$$

Combining the above statement with Theorem 1.1, we obtain the main theorem of the paper:

Theorem 2.3. *Let $h(X)$ be given by (1.3) and $[M_{ik}]$ be given by (2.2). Then $X^r h(X^{q-1})$ is a PP of $\mathbb{F}_{q^2}$ such that $X^r h(X)^{q-1}$ is a monomial function on A_k for every $0 \leq k < d$ if and only if the following conditions are satisfied.*

(i) *For each $0 \leq k < d$, there exist $s_k, t_k \geq 0$ with $s_k + t_k < (q+1)/d$, $\pi(k) \in \mathbb{Z}/d\mathbb{Z}$, $\lambda_k \in A_{\pi(k)}$ and $\tau_k \in \{0\} \cup [(q+1)/d - t_k, t_k]$ such that $\sum_i M_{ik} X^i = X^{s_k} L_k(X)$, where $L_k \in \mathcal{L}_k(t_k, \tau_k; \lambda_k)$.*

(ii) $\gcd(r, q-1) = 1$ *and* $\gcd(e_k, (q+1)/d) = 1$ *for all $0 \leq k < d$, where*

$$e_k = r - 2s_k - t_k + \tau_k.$$

(iii) *The map $k \mapsto \pi(k) + e_k k$ permutes $\mathbb{Z}/d\mathbb{Z}$.*

Theorem 2.3 can be stated as an algorithm.

Algorithm 2.4. Let r be a positive integer such that $\gcd(r, q-1) = 1$ and let $d \mid q+1$.

Input: Sequences s_k, t_k, τ_k, $\pi(k)$, λ_k, $0 \leq k < d$, described below.
Output: A PP of $\mathbb{F}_{q^2}$ of the form $X^r h(X^{q-1})$ such that $X^r h(X)^{q-1}$ is a monomial function on each A_k, $0 \leq k < d$.
Note: All PPs of $\mathbb{F}_{q^2}$ with such properties can be produced by this algorithm.
Step 1: Choose integer sequences $s_k, t_k, \tau_k \geq$, $0 \leq k < d$, such that $s_k + t_k < (q+1)/d$, $\tau_k \in \{0\} \cup [(q+1)/d - t_k, t_k]$, and $e_k := r - 2s_k - t_k + \tau_k$ satisfies $\gcd(e_k, (q+1)/d) = 1$.
Step 2: Choose a sequence $\pi(k) \in \mathbb{Z}/d\mathbb{Z}$, $0 \leq k < d$, such that $k \mapsto \pi(k) + e_k k$ permutes $\mathbb{Z}/d\mathbb{Z}$.
Step 3: For each $0 \leq k < d$, choose $\lambda_k \in A_{\pi(k)}$ and $L_k \in \mathcal{L}_k(t_k, \tau_k; \lambda_k)$.

Step 4: Compute the $((q+1)/d) \times d$ matrix $[M_{ik}]$ such that

$$X^{s_k} L_k = \sum_i M_{ik} X^i,$$

and compute the $((q+1)/d) \times d$ matrix

$$[a_{ij}] = \frac{1}{d}[M_{ik}][\epsilon^{-kj}].$$

Step 5: Let

$$h(X) = \sum_{i,j} a_{ij} X^{i+j(q+1)/d}.$$

Then $X^r h(X^{q-1})$ is the output PP of $\mathbb{F}_{q^2}$.

Remark 2.5. In Step 3, when choosing $L_k \in \mathcal{L}_k(t_k, \tau_k; \lambda_k)$, it is required that $\gcd(L_k, X^{(q+1)/d} - \epsilon^k) = 1$. However, this condition is automatically satisfied if $h(X)$ in Step 5 satisfies $\gcd(h, X^{q+1} - 1) = 1$. In fact, $\gcd(L_k, X^{(q+1)/d} - \epsilon^k) = 1$ for all $0 \le k < d$ if and only if $\gcd(h, X^{q+1} - 1) = 1$.

There are two ways to use this algorithm: forward or backward. In the forward approach, we simply proceed from Step 1 through Step 5. The advantage of this approach is that there are few restrictions on the choices of the sequences; the drawback is that we have little control over the appearance of the resulting PP. A few examples of the forward approach are given in Section 5. In the backward approach, we first impose conditions on $[a_{ij}]$. (For example, we may require $h(X)$ to be a binomial of a trinomial.) We then compute $[M_{ik}]$ and determine if the sequences L_k, s_k, t_k, τ_k, $\pi(k)$, λ_k exist. The benefit of this approach is that we have more control over the appearance of the resulting PP. However, the conditions for the aforementioned sequences to be existent could be complicated. In Sections 3 and 4, we use the backward approach to determine the permutation binomials and trinomials obtainable from the algorithm.

For $0 \le t < (q+1)/d$, $\tau \in \{0\} \cup [(q+1)/d - t, t]$, $\lambda \in \mu_{q+1}$ and $0 \le k < d$, write $\lambda = a^{1-q}$, where $a \in \mathbb{F}_{q^2}^*$, and $\epsilon^k = b^{(q+1)/d}$, where $b \in \mu_{q+1}$. Then it is easy to see that the map

$$\begin{array}{ccc} \mathcal{L}_k(t, \tau; \lambda) & \longrightarrow & \mathcal{L}_0(t, \tau; 1) \\ L(X) & \longmapsto & aL(bX) \end{array}$$

is a bijection. Set $l(t, \tau) = |\mathcal{L}_0(t, \tau; 1)|$. Then $|\mathcal{L}_k(t, \tau; \lambda)| = l(t, \tau)$, which is independent of k and λ.

Let

$$\Omega = \{(s, t, \tau) \in \mathbb{N}^3 : s + t < (q+1)/d,\ \tau \in \{0\} \cup [(q+1)/d - t, t],$$

$$\gcd(r-2s-t+\tau,(q+1)/d)=1\}.$$

In Step 2 of Algorithms 2.4, the number of choices for the sequence $\pi(k)$ is $d!$. In Step 3, the number of choices for λ_k is $(q+1)/d$ and the number of choices for L_k is $l(t_k,\tau_k)$. Therefore, the total number of PPs produced by the algorithm is

$$\begin{aligned}&\sum_{(s_0,t_0,\tau_0),\ldots,(s_{d-1},t_{d-1},\tau_{d-1})\in\Omega} d!\prod_{k=0}^{d-1}\Big(\frac{q+1}{d}l(t_k,\tau_k)\Big) \\ &= d!\Big(\frac{q+1}{d}\Big)^d\Big(\sum_{(s,t,\tau)\in\Omega} l(t,\tau)\Big)^d \\ &= d!\Big(\frac{q+1}{d}\Big)^d\Big(\sum_{\substack{0\le t<(q+1)/d\\ \tau\in\{0\}\cup[(q+1)/d-t,t]}} m(t,\tau)l(t,\tau)\Big)^d,\end{aligned} \tag{2.14}$$

where

$$m(t,\tau)=|\{(0\le s<(q+1)/d-t:\gcd(r-2s-t+\tau,(q+1)/d)=1\}|. \tag{2.15}$$

When $\tau=0$, $l(t,0)$ is determined by the following lemma.

Lemma 2.6. *For $0\le t<(q+1)/d$,*

$$l(t,0)=(q^2-1)\sum_{i=0}^{t-1}(-1)^i\binom{(q+1)/d}{i}q^{t-i-1}+(-1)^t(q-1)\binom{(q+1)/d}{t}.$$

Proof. Let Λ_t denote the number of monic self-dual polynomials of degree t in $\mathbb{F}_{q^2}[X]$. It is known that [4]

$$\Lambda_t=\begin{cases}1 & \text{if } t=0,\\ (q+1)q^{t-1} & \text{if } t>0.\end{cases}$$

For $Y\subset\mu_{q+1}$, let

$$\mathcal{L}_Y=\Big\{L\in\mathbb{F}_{q^2}[X] \text{ monic, self-dual, } \deg L=t,\ \prod_{y\in Y}(X-y)\mid L\Big\}$$

and

$$\mathcal{L}=\{L\in\mathbb{F}_{q^2}[X] \text{ monic, self-dual, } \deg L=t,\ \gcd(L,X^{(q+1)/d}-1)=1\}.$$

Then $|\mathcal{L}_Y|=\Lambda_{t-|Y|}$ (which is 0 if $t-|Y|<0$). By inclusion-exclusion,

$$\begin{aligned}|\mathcal{L}| &= \sum_{i=0}^{t}(-1)^i\binom{(q+1)/d}{i}\Lambda_{t-i}\\ &= \sum_{i=0}^{t-1}(-1)^i\binom{(q+1)/d}{i}(q+1)q^{t-i-1}+(-1)^t\binom{(q+1)/d}{t}.\end{aligned}$$

On the other hand, we have

$$(q^2-1)|\mathcal{L}| = (q+1)l(t,0),$$

since both sides count the number of self-dual polynomials of degree t in $\mathbb{F}_{q^2}[X]$ that are relatively prime to $X^{(q+1)/d}-1$. Hence $l(t,0)=(q-1)|\mathcal{L}|$ and the conclusion follows. □

However, for $\tau>0$, we have not found an explicit formula for $l(t,\tau)$.

Question 2.7. For $(q+1)/d-t\le\tau\le t<(q+1)/d$, determine

$$\begin{aligned}l(t,\tau) = |\{&L=P+X^{(q+1)/d-\tau}Q : P,Q\in\mathbb{F}_{q^2}[X],\ \deg P=t-\tau,\\ &\deg Q=\tau+t-(q+1)/d,\ \tilde{P}=P,\ \tilde{Q}=Q,\ \gcd(L,X^{(q+1)/d}-1)=1\}|.\end{aligned}$$

3. Permutation binomials

We follow the notation of Algorithm 2.4. Assume that the polynomial $h(X)$ resulting from Algorithm 2.4 is a binomial, i.e., the matrix $[a_{ij}]$ has precisely two nonzero entries. Without loss of generality, assume that

$$[a_{ij}] = \begin{array}{c} \\ 0 \\ u \end{array}\begin{array}{c} \begin{array}{cc} 0 & v \end{array} \\ \begin{bmatrix} 1 & \\ & a \end{bmatrix} \end{array},$$

where $a\in\mathbb{F}_{q^2}^*$, $0\le u<(q+1)/d$, $0\le v<d$, $(u,v)\neq(0,0)$. We remind the reader that the rows of the matrix $[a_{ij}]$ are labeled by integers $0,\dots,(q+1)/d-1$ and the columns are labeled by $0,\dots,d-1$.

Case 1. Assume that $u=0$. Then

$$X^r h(X^{q-1}) = X^r(1+aX^{v(q^2-1)/d}).$$

It is well known, as stated in the introduction, that $X^r(1+aX^{v(q^2-1)/d})$ is a PP of $\mathbb{F}_{q^2}$ if and only if $\gcd(r,(q^2-1)/d)=1$ and $X^r(1+aX^v)^{(q^2-1)/d}$ permutes μ_d.

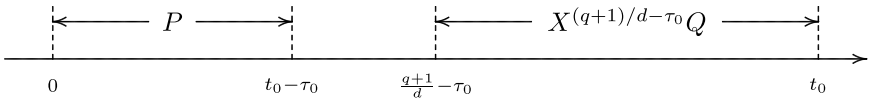

Fig. 3. When $P + X^{(q+1)/d-\tau_0}Q$ is a binomial.

Case 2. Assume that $u > 0$. Then

$$[M_{ik}] = \begin{array}{c} \\ 0 \\ u \end{array} \begin{bmatrix} 1 & \cdots & 1 \\ a\epsilon^{v\cdot 0} & \cdots & a\epsilon^{v(d-1)} \end{bmatrix}$$

and

$$\sum_i M_{ik}X^i = 1 + a\epsilon^{vk}X^u, \quad s_k = 0,\ t_k = u, \quad 0 \le k < d.$$

In particular, $L_0 = 1 + aX^u \in \mathcal{L}_0(t_0, \tau_0; \lambda_0)$, where $\tau_0 \in \{0\} \cup [(q+1)/d - t_0, t_0]$.

First assume that $\tau_0 = 0$. By the definition of $\mathcal{L}_0(t_0, 0; \lambda_0)$, L_0 is self-dual. It follows that $a \in \mu_{q+1}$. We have $X^r h(X^{q-1}) = X^r(1 + aX^{l(q-1)})$, where $l = u + v(q+1)/d$. Because of the condition $a \in \mu_{q+1}$, such permutation binomials are well known. By [17, Corollary 5.3], $X^r(1 + aX^{l(q-1)})$ permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(r, q-1) = 1$, $\gcd(r - l, q + 1) = 1$ and $(-a)^{(q+1)/\gcd(q+1,l)} \neq 1$.

Next, assume that $\tau_0 \in [(q+1)/d - t_0, t_0]$. Since $L_0 \in \mathcal{L}_0(t_0, \tau_0; \lambda_0)$, we have $L_0 = P + X^{(q+1)/d-\tau_0}Q$, where $P, Q \in \mathbb{F}_{q^2}[X]$, $\deg P = t_0 - \tau_0$, $\deg Q = \tau_0 + t_0 - (q+1)/d$, $\gcd(L_0, X^{(q+1)/d} - 1) = 1$. Since $P + X^{(q+1)-\tau_0}Q$ is a binomial, we must have $t_0 = \tau_0$ and $(q+1)/d - \tau_0 = t_0$ (see Fig. 3). Hence $t_0 = \tau_0 = u = (q+1)/2d$. Then $h(X) = 1 + aX^{u+v(q+1)/d} = 1 + aX^{(1+2v)(q+1)/2d}$. Then $X^r h(X^{q-1}) = X^r(1 + aX^{(1+2v)(q^2-1)/2d})$ is a PP of $\mathbb{F}_{q^2}$ if and only if $\gcd(r, (q^2-1)/2d) = 1$ and $X^r(1 + aX^{1+2v})$ permutes μ_{2d}.

Summary for binomials. From the above two cases, we see that permutation binomials generated by Algorithm 2.4 were all previously known.

4. Permutation trinomials

Now assume that $h(X)$ in Algorithm 2.4 is a trinomial, i.e., the matrix $[a_{ij}]$ has precisely three nonzero entries. Without loss of generality, write

$$[a_{ij}] = \begin{array}{c} \\ 0 \\ i_1 \\ i_2 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & j_1 & j_2 \end{array} \\ \begin{bmatrix} 1 & & \\ & a & \\ & & b \end{bmatrix} \end{array}, \qquad a, b \in \mathbb{F}_{q^2}^*.$$

4.1. Three cases

Case 1. Assume that $i_1 = i_2 = 0$. Then

$$X^r h(X^{q-1}) = X^r(1 + aX^{j_1(q^2-1)/d} + bX^{j_2(q^2-1)/d}).$$

Such a trinomial is a PP of $\mathbb{F}_{q^2}$ if and only if $\gcd(r, (q^2-1)/d) = 1$ and $X^r(1 + aX^{j_1} + bX^{j_2})^{(q^2-1)/d}$ permutes μ_d.

Remark. If $i_1 = i_2 \neq 0$, then

$$\begin{aligned} X^r h(X^{q-1}) &= X^r(1 + aX^{(q-1)(i_1+j_1(q+1)/d)} + bX^{(q-1)(i_2+j_2(q+1)/d)}) \\ &\equiv X^{r+(q-1)(i_1+j_1(q+1)/d)}(a + bX^{(q-1)i_1'} + X^{(q-1)i_2'}) \pmod{X^{q^2} - X}, \end{aligned}$$

where $i_1' \equiv 0 \pmod{(q+1)/d}$ and $i_2' \not\equiv 0 \pmod{(q+1)/d}$. This situation is covered by the next case (Case 2).

Case 2. Assume that $i_1 = 0$ and $0 < i_2 < (q+1)/d$. Then

$$[M_{ik}] = \begin{array}{c} \\ 0 \\ i_2 \end{array} \begin{array}{c} \begin{array}{ccc} & \cdots & \end{array} \\ \begin{bmatrix} 1 + a\epsilon^{j_1 \cdot 0} & \cdots & 1 + a\epsilon^{j_1(d-1)} \\ b\epsilon^{j_2 \cdot 0} & \cdots & b\epsilon^{j_2(d-1)} \end{bmatrix} \end{array}$$

and

$$\sum_i M_{ik} X^i = 1 + a\epsilon^{j_1 k} + b\epsilon^{j_2 k} X^{i_2}. \tag{4.1}$$

Case 2.1. Assume that $1 + a\epsilon^{j_1 k} \neq 0$ for all $0 \leq k < d$. Then

$$L_k(X) = 1 + a\epsilon^{j_1 k} + b\epsilon^{j_2 k} X^{i_2}, \quad s_k = 0, \quad t_k = i_2.$$

Lemma 4.1. *The following statements hold in Case 2.1.*

(i) *If* $\tau_k = 0$ *for some* $0 \le k < d$, *then*

$$\Big(\frac{1 + a^q \epsilon^{-j_1 k}}{b}\Big)^{(q+1)/d} = \epsilon^{\alpha(k)} \tag{4.2}$$

for some $\alpha(k) \in \mathbb{Z}/d\mathbb{Z}$. *We have*

$$e_k = r - i_2 \quad \textit{and} \quad \pi(k) = -j_2 k \frac{q+1}{d} + \alpha(k).$$

(ii) *If* $\tau_k = 0$ *for all* $0 \le k < d$, *then* $j_1 = d/2$, $a^{q-1} = -1$, $(1-a)/b \in \mu_{q+1}$, $e_k = r - i_2$, *and*

$$\pi(k) + e_k k = \Big(-j_2 \frac{q+1}{d} + r - i_2\Big)k + \delta(k)v + u,$$

where

$$\Big(\frac{1-a}{b}\Big)^{(q+1)/d} = \epsilon^u, \quad \Big(\frac{1+a}{1-a}\Big)^{(q+1)/d} = \epsilon^v,$$

and

$$\delta(k) = \begin{cases} 0 & \textit{if } k \textit{ is even,} \\ 1 & \textit{if } k \textit{ is odd.} \end{cases}$$

Proof. (i) Clearly, $e_k = r - i_2$. Since $L_k \in \mathcal{L}_k(t_k, 0; \lambda_k)$, we have $\tilde{L}_k = \lambda_k L_k$, whence

$$\lambda_k = \frac{(1 + a\epsilon^{j_1 k})^q}{b\epsilon^{j_2 k}}.$$

Since

$$\epsilon^{\pi(k)} = \lambda_k^{(q+1)/d} = \Big(\frac{1 + a^q \epsilon^{-j_1 k}}{b\epsilon^{j_2 k}}\Big)^{(q+1)/d} = \epsilon^{-j_2 k(q+1)/d} \Big(\frac{1 + a^q \epsilon^{-j_1 k}}{b}\Big)^{(q+1)/d},$$

we have

$$\Big(\frac{1 + a^q \epsilon^{-j_1 k}}{b}\Big)^{(q+1)/d} = \epsilon^{\alpha(k)}$$

for some $\alpha(k) \in \mathbb{Z}/d\mathbb{Z}$ and $\pi(k) = -j_2 k(q+1)/d + \alpha(k)$.

(ii) By (4.2),

$$(1 + a^q \epsilon^{-j_1 k})^{q+1} = b^{q+1}, \tag{4.3}$$

i.e.,

$$(1+a\epsilon^{j_1 k})(1+a^q\epsilon^{-j_1 k}) = b^{q+1}.$$

Hence the quadratic equation $(1+ax)(1+a^q x^{-1}) = b^{q+1}$ has solutions $x = \epsilon^{j_1 k}$, $0 \le k < d$. Since the number of such solutions is ≤ 2 and since $0 < j_1 < d$, we must have $j_1 = d/2$, whence $\epsilon^{j_1} = -1$. It follows from (4.3), with $k = 0, 1$, that

$$(1+a^q)^{q+1} = (1-a^q)^{q+1}.$$

This happens if and only if $a^q = -a$. (Note that q is odd since $2 \mid d$.) Then

$$\Big(\frac{1-a}{b}\Big)^{q+1} = 1 \quad \text{and} \quad \Big(\frac{1+a}{1-a}\Big)^{q+1} = 1.$$

Write

$$\Big(\frac{1-a}{b}\Big)^{(q+1)/d} = \epsilon^u \quad \text{and} \quad \Big(\frac{1+a}{1-a}\Big)^{(q+1)/d} = \epsilon^v.$$

Then by (4.2),

$$\begin{aligned}\epsilon^{\alpha(k)} &= \Big(\frac{1-a(-1)^k}{b}\Big)^{(q+1)/d} = \Big(\frac{1-a}{b}\Big)^{(q+1)/d}\Big(\frac{1-a(-1)^k}{1-a}\Big)^{(q+1)/d} \\ &= \begin{cases} \epsilon^u & \text{if } k \text{ is even,} \\ \epsilon^{u+v} & \text{if } k \text{ is odd.} \end{cases}\end{aligned}$$

Thus $\alpha(k) = u + \delta(k)v$, and by (i),

$$\begin{aligned}\pi(k) + e_k k &= -j_2 k\frac{q+1}{d} + u + \delta(k)v + (r-i_2)k \\ &= \Big(-j_2\frac{q+1}{d} + r - i_2\Big)k + \delta(k)v + u. \quad \square\end{aligned}$$

If $\tau_k \in [(q+1)/d - t_k, t_k]$ for some $0 \le k < d$, applying the argument in the last paragraph in Case 2 of Section 3 to $L_k \in \mathcal{L}_k(t_k, \tau_k; \lambda_k)$, we have $t_k = \tau_k = i_2 = (q+1)/2d$. Therefore,

$$\begin{aligned}X^r h(X^{q-1}) &= X^r(1 + aX^{(q-1)\cdot j_1(q+1)/d} + bX^{(q-1)((q+1)/2d + j_2(q+1)/d)}) \\ &= X^r(1 + aX^{j_1(q^2-1)/d} + bX^{(2j_2+1)(q^2-1)/2d}).\end{aligned}$$

This trinomial permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(r, (q^2-1)/2d) = 1$ and $X^r(1 + aX^{2j_1} + bX^{2j_2+1})^{(q^2-1)/2d}$ permutes μ_{2d}.

Case 2.2. Assume that $1 + a\epsilon^{j_1 k} = 0$ for some $0 \le k < d$. Write $\epsilon^k = \lambda^{(q+1)/d}$ for some $\lambda \in \mu_{q+1}$. Then

$$\begin{aligned} h(\lambda X) &= 1 + a(\lambda X)^{j_1(q+1)/d} + b(\lambda X)^{i_2 + j_2(q+1)/d} \\ &= 1 - X^{j_1(q+1)/d} + b\lambda^{i_2}\epsilon^{j_2 k} X^{i_2 + j_2(q+1)/d}. \end{aligned}$$

Hence we may assume that $a = -1$. By (4.1),

$$L_k(X) = \begin{cases} b\epsilon^{j_2 k} & \text{if } j_1 k \equiv 0 \pmod d, \\ 1 - \epsilon^{j_1 k} + b\epsilon^{j_2 k} X^{i_2} & \text{if } j_1 k \not\equiv 0 \pmod d, \end{cases}$$

$$s_k = \begin{cases} i_2 & \text{if } j_1 k \equiv 0 \pmod d, \\ 0 & \text{if } j_1 k \not\equiv 0 \pmod d, \end{cases} \tag{4.4}$$

$$t_k = \begin{cases} 0 & \text{if } j_1 k \equiv 0 \pmod d, \\ i_2 & \text{if } j_1 k \not\equiv 0 \pmod d. \end{cases} \tag{4.5}$$

Lemma 4.2. *If $j_1 k \equiv 0 \pmod d$, then $\tau_k = 0$, $e_k = r - 2i_2$, and*

$$\pi(k) = -2j_2 k \frac{q+1}{d} + \beta,$$

where $b^{(q^2-1)/d} = \epsilon^\beta$.

Proof. Clearly, $\tau_k = 0$ and $e_k = r - 2i_2$. Since $L_k = b\epsilon^{j_2 k} \in \mathcal{L}_k(t_k, 0; \lambda_k)$, we have $\tilde{L}_k = \lambda_k L_k$, whence $\lambda_k = (b\epsilon^{j_2 k})^{q-1} = b^{q-1}\epsilon^{-2j_2 k}$. Since

$$\lambda_k^{(q+1)/d} = b^{(q^2-1)/d}\epsilon^{-2j_2 k(q+1)/d} = \epsilon^{-2j_2 k(q+1)/d + \beta},$$

we have $\pi(k) = -2j_2 k(q+1)/d + \beta$. □

If $\tau_k \in [(q+1)/d - t_k, t_k]$ for some $0 \le k < d$ with $j_1 k \not\equiv 0 \pmod d$, applying the argument in the last paragraph in Case 2 of Section 3 to $L_k \in \mathcal{L}_k(t_k, \tau_k; \lambda_k)$, we have $t_k = \tau_k = i_2 = (q+1)/2d$. Then

$$X^r h(X^{q-1}) = X^r(1 + aX^{j_1(q^2-1)/d} + bX^{(2j_2+1)(q^2-1)/2d}),$$

which permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(r, (q^2-1)/2d) = 1$ and $X^r(1 + aX^{2j_1} + bX^{2j_2+1})^{(q^2-1)/2d}$ permutes μ_{2d}. Therefore, we assume that $\tau_k = 0$ for all $0 \le k < d$ with $j_1 k \not\equiv 0 \pmod d$. This assumption combined with Lemma 4.2 means that $\tau_k = 0$ for all $0 \le k < d$.

Lemma 4.3. *Assume that $\tau_k = 0$ for all $0 \le k < d$ in Case 2.2. Then $o(\epsilon^{j_1}) = 2$ or 3.*

(i) *If $o(\epsilon^{j_1}) = 2$, then*

$$s_k = \begin{cases} i_2 & \text{if } k \equiv 0 \pmod 2, \\ 0 & \text{if } k \not\equiv 0 \pmod 2, \end{cases}$$

$$t_k = \begin{cases} 0 & \text{if } k \equiv 0 \pmod 2, \\ i_2 & \text{if } k \not\equiv 0 \pmod 2, \end{cases}$$

$$e_k = \begin{cases} r - 2i_2 & \text{if } k \equiv 0 \pmod 2, \\ r - i_2 & \text{if } k \not\equiv 0 \pmod 2, \end{cases}$$

$$\pi(k) = \begin{cases} -2j_2 k\dfrac{q+1}{d} + 2\theta & \text{if } k \equiv 0 \pmod 2, \\ -j_2 k\dfrac{q+1}{d} + \theta & \text{if } k \not\equiv 0 \pmod 2, \end{cases}$$

where $(2/b)^{(q+1)/d} = \epsilon^{\theta}$.

(ii) *If* $o(\epsilon^{j_1}) = 3$, *then*

$$s_k = \begin{cases} i_2 & \text{if } k \equiv 0 \pmod 3, \\ 0 & \text{if } k \not\equiv 0 \pmod 3, \end{cases}$$

$$t_k = \begin{cases} 0 & \text{if } k \equiv 0 \pmod 3, \\ i_2 & \text{if } k \not\equiv 0 \pmod 3, \end{cases}$$

$$e_k = \begin{cases} r - 2i_2 & \text{if } k \equiv 0 \pmod 3, \\ r - i_2 & \text{if } k \not\equiv 0 \pmod 3, \end{cases}$$

$$\pi(k) = \begin{cases} -(2j_2 k + j_1)\dfrac{q+1}{d} + 2\eta + \dfrac{q+1}{\gcd(2,d)} & \text{if } k \equiv 0 \pmod 3, \\ -(j_2 k + j_1)\dfrac{q+1}{d} + \eta + \dfrac{q+1}{\gcd(2,d)} & \text{if } k \not\equiv 0 \pmod 3, \end{cases}$$

where

$$\Big(\frac{1-\epsilon^{j_1}}{b}\Big)^{(q+1)/d} = \epsilon^{\eta}.$$

Proof. If $j_1 k \not\equiv 0 \pmod d$, then $L_k = 1 - \epsilon^{j_1 k} + b\epsilon^{j_2 k} X^{i_2} \in \mathcal{L}_k(t_k, 0, \lambda_k)$. Since $\tilde{L}_k = \lambda_k L_k$, we have

$$\frac{(1-\epsilon^{j_1 k})^q}{b\epsilon^{j_2 k}} = \lambda_k.$$

It follows that

$$1 = \Big(\frac{(1-\epsilon^{j_1 k})^q}{b\epsilon^{j_2 k}}\Big)^{q+1} = \Big(\frac{1-\epsilon^{j_1 k}}{b}\Big)^{q+1},$$

i.e.,

$$(1-\epsilon^{j_1 k})(1-\epsilon^{-j_1 k}) = b^{q+1}. \tag{4.6}$$

Therefore, $\epsilon^{j_1 k}$ is a root of

$$(1-x)(1-x^{-1}) = b^{q+1} \tag{4.7}$$

whenever $\epsilon^{j_1 k} \neq 1$. Since (4.7) has at most two solutions, we have $o(\epsilon^{j_1}) \leq 3$.

(i) Assume that $o(\epsilon^{j_1}) = 2$, i.e., $\epsilon^{j_1} = -1$. The formulas for s_k and t_k follow from (4.4) and (4.5), and the formula for e_k is obvious. It remains to prove the formula for $\pi(k)$.

For $k \not\equiv 0 \pmod 2$,

$$\epsilon^{\pi(k)} = \lambda_k^{(q+1)/d} = \Big(\frac{2}{b\epsilon^{j_2 k}}\Big)^{(q+1)/d} = \Big(\frac{2}{b}\Big)^{(q+1)/d} \epsilon^{-j_2 k(q+1)/d} = \epsilon^{-j_2 k(q+1)/d + \theta},$$

where $(2/b)^{(q+1)/d} = \epsilon^{\theta}$. Hence

$$\pi(k) = -j_2 k \frac{q+1}{d} + \theta.$$

For $k \equiv 0 \pmod 2$, by Lemma 4.2

$$\pi(k) = -2j_2 k \frac{q+1}{d} + \beta,$$

where $b^{(q^2-1)/d} = \epsilon^{\beta}$. Since

$$\epsilon^{-2\theta} = \epsilon^{\theta(q-1)} = b^{-(q^2-1)/d} = \epsilon^{-\beta},$$

we have $\beta = 2\theta$.

(ii) Assume that $o(\epsilon^{j_1}) = 3$ and write $\epsilon^{j_1} = \omega$. Again, we only have to prove the formula for $\pi(k)$.

For $k \not\equiv 0 \pmod 3$,

$$\begin{aligned}\epsilon^{\pi(k)} &= \Big(\frac{1-\omega^k}{b\epsilon^{j_2 k}}\Big)^{(q+1)/d} = \Big(\frac{1-\omega^k}{1-\omega}\Big)^{(q+1)/d} \Big(\frac{1-\omega}{b}\Big)^{(q+1)/d} \epsilon^{-j_2 k(q+1)/d} \\ &= \Big(\frac{1-\omega^k}{1-\omega}\Big)^{(q+1)/d} \epsilon^{-j_2 k(q+1)/d + \eta},\end{aligned}$$

where $((1-\omega)/b)^{(q+1)/d} = \epsilon^{\eta}$. Note that

$$\Big(\frac{1-\omega^{-1}}{1-\omega}\Big)^{(q+1)/d} = (-\omega^{-1})^{(q+1)/d} = (-1)^{(q+1)/d} \epsilon^{-j_1(q+1)/d},$$

where

$$(-1)^{(q+1)/d} = \left\{\begin{array}{ll} \epsilon^{(q+1)/2} & \text{if } d \text{ is even} \\ 1 & \text{if } d \text{ is odd} \end{array}\right\} = \epsilon^{(q+1)/\gcd(2,d)}.$$

Hence

$$\pi(k) = -(j_2 k + j_1)\frac{q+1}{d} + \eta + \frac{q+1}{\gcd(2,d)}.$$

For $k \equiv 0 \pmod 3$, by Lemma 4.2,

$$\pi(k) = -2j_2 k\frac{q+1}{d} + \beta,$$

where $b^{(q^2-1)/d} = \epsilon^{\beta}$. Since

$$\begin{aligned}\epsilon^{-2\eta} &= \epsilon^{\eta(q-1)} = \Big(\frac{1-\omega}{b}\Big)^{(q^2-1)/d} = \epsilon^{-\beta}\Big(\frac{1-\omega^{-1}}{1-\omega}\Big)^{(q+1)/d} \\ &= \epsilon^{-\beta - j_1(q+1)/d}(-1)^{(q+1)/d} = \epsilon^{-\beta - j_1(q+1)/d + (q+1)/\gcd(2,d)},\end{aligned}$$

we have

$$\beta = -j_1\frac{q+1}{d} + 2\eta + \frac{q+1}{\gcd(2,d)}. \quad \square$$

Case 3. Assume that $0 < i_1 < i_2 < (q+1)/d$. Then

$$[M_{ik}] = \begin{array}{c} 0 \\ i_1 \\ i_2 \end{array}\!\!\begin{bmatrix} 1 & \cdots & 1 \\ a\epsilon^{j_1\cdot 0} & \cdots & a\epsilon^{j_1(d-1)} \\ b\epsilon^{j_2\cdot 0} & \cdots & b\epsilon^{j_2(d-1)} \end{bmatrix},$$

$$L_k(X) = 1 + a\epsilon^{j_1 k}X^{i_1} + b\epsilon^{j_2 k}X^{i_2},$$

$$s_k = 0, \quad t_k = i_2.$$

Lemma 4.4. *If $\tau_k = 0$, then $i_1 = i_2/2$, $e_k = r - i_2$, and*

$$\pi(k) = -2j_1 k\frac{q+1}{d} + \alpha,$$

where $a^{(q^2-1)/d} = \epsilon^{\alpha}$ and $b = a^{1-q}\epsilon^{(2j_1 - j_2)k}$.

Proof. Clearly, $e_k = r - i_2$. Since $\tilde{L}_k = \lambda_k L_k$, i.e.,

$$\overline{b\epsilon^{j_2 k}} + \overline{a\epsilon^{j_1 k}}X^{i_2 - i_1} + X^{i_2} = \lambda_k(1 + a\epsilon^{j_1 k}X^{i_1} + b\epsilon^{j_2 k}X^{i_2}),$$

we have $i_1 = i_2/2$ and $(\overline{b\epsilon^{j_2 k}}, \overline{a\epsilon^{j_1 k}}, 1) = \lambda_k(1, a\epsilon^{j_1 k}, b\epsilon^{j_2 k})$. Hence

$$\lambda_k = \overline{b\epsilon^{j_2 k}} = b^q \epsilon^{-j_2 k}$$

and

$$\overline{a\epsilon^{j_1 k}} \cdot b\epsilon^{j_2 k} = a\epsilon^{j_1 k}, \quad \text{i.e.,} \quad b = a^{1-q}\epsilon^{(2j_1 - j_2)k}.$$

We have

$$\begin{aligned}\epsilon^{\pi(k)} &= \lambda_k^{(q+1)/d} = (b^q \epsilon^{-j_2 k})^{(q+1)/d} = ((a^{q-1}\epsilon^{-(2j_1-j_2)k} \cdot \epsilon^{-j_2 k})^{(q+1)/d} \\ &= a^{(q^2-1)/d}\epsilon^{-2j_1 k(q+1)/d} = \epsilon^{-2j_1 k(q+1)/d + \alpha},\end{aligned}$$

where $a^{(q^2-1)/d} = \epsilon^{\alpha}$. Hence

$$\pi(k) = -2j_1 k\frac{q+1}{d} + \alpha. \quad \square$$

Remark. If $\tau_k = 0$ for all $0 \le k < d$, then by Lemma 4.4, $i_1 = i_2/2$, $2j_1 - j_2 \equiv 0 \pmod d$ and $b = a^{1-q}$. Consequently,

$$\begin{aligned}h(X) &= 1 + aX^{i_1 + j_1(q+1)/d} + bX^{i_2 + j_2(q+1)/d} \\ &\equiv 1 + aX^{i_1 + j_1(q+1)/d} + bX^{2(i_1 + j_1(q+1)/d)} \pmod{X^{q+1} - 1} \\ &= h_1(X),\end{aligned}$$

where

$$h_1(X) = 1 + aX^l + bX^{2l}, \quad l = i_1 + j_1(q+1)/d.$$

Hence

$$X^r h(X^{q-1}) \equiv X^r h_1(X^{q-1}) \pmod{X^{q^2-1} - 1}.$$

Since $b = a^{1-q}$, $h_1(X)$ is self-dual. In general, when $h_1(X)$ is self dual, PPs of $\mathbb{F}_{q^2}$ of the form $X^r h_1(X^{q-1})$ are known; see Example 5.1.

Lemma 4.5. *If $\tau_k \in [(q+1)/d - t_k, t_k]$, then precisely one of the following occurs.*
(i)

$$t_k = \tau_k = \frac{1}{2}\Big(\frac{q+1}{d} + 1\Big), \quad i_1 = \frac{1}{2}\Big(\frac{q+1}{d} - 1\Big), \quad i_2 = \frac{1}{2}\Big(\frac{q+1}{d} + 1\Big),$$
$$a = b^q \epsilon^{-(j_1 + j_2 + 1)k}, \quad e_k = r, \quad \pi(k) = 0.$$

(ii)
$$t_k = \frac{1}{2}\Big(\frac{q+1}{d} + 1\Big), \quad \tau_k = \frac{1}{2}\Big(\frac{q+1}{d} - 1\Big), \quad i_1 = 1, \quad i_2 = \frac{1}{2}\Big(\frac{q+1}{d} + 1\Big),$$

$$a = b^{1-q}\epsilon^{(2j_2-j_1+1)k}, \quad b^{(q^2-1)/d} = \epsilon^{\beta}, \quad e_k = r-1,$$
$$\pi(k) = -(2j_2+1)k\frac{q+1}{d} + \beta.$$

Proof. Since

$$L_k = 1 + a\epsilon^{j_1 k}X^{i_1} + b\epsilon^{j_2 k}X^{i_2} = P + X^{(q+1)/d-\tau_k}Q$$

is a trinomial, where $\deg P = t_k - \tau_k$ and $\deg Q = \tau_k + t_k - (q+1)/d$ (see Fig. 4), we have

$$\begin{cases} t_k - \tau_k = 0, \\ t_k = \dfrac{q+1}{d} - \tau_k + 1, \\ i_1 = \dfrac{q+1}{d} - \tau_k, \\ i_2 = t_k, \end{cases} \quad \text{or} \quad \begin{cases} t_k - \tau_k = 1, \\ t_k = \dfrac{q+1}{d} - \tau_k, \\ i_1 = 1, \\ i_2 = t_k, \end{cases}$$

i.e.,

$$\begin{cases} t_k = \tau_k = \dfrac{1}{2}\Big(\dfrac{q+1}{d} + 1\Big), \\ i_1 = \dfrac{1}{2}\Big(\dfrac{q+1}{d} - 1\Big), \\ i_2 = \dfrac{1}{2}\Big(\dfrac{q+1}{d} + 1\Big), \end{cases} \tag{4.8}$$

or

$$\begin{cases} t_k = \dfrac{1}{2}\Big(\dfrac{q+1}{d} + 1\Big), \\ \tau_k = \dfrac{1}{2}\Big(\dfrac{q+1}{d} - 1\Big), \\ i_1 = 1, \\ i_2 = \dfrac{1}{2}\Big(\dfrac{q+1}{d} + 1\Big). \end{cases} \tag{4.9}$$

(i) Assume (4.8). First, note that $e_k = r - t_k + \tau_k = r$. In this case,

$$L_k = 1 + X^{\frac{1}{2}(\frac{q+1}{d}-1)}(a\epsilon^{j_1 k} + b\epsilon^{j_2 k}X),$$

where $P = 1$ and $Q = a\epsilon^{j_1 k} + b\epsilon^{j_2 k}X$. We have $\lambda_k = \tilde{P}/P = 1$ and

$$\lambda_k\epsilon^k = \frac{\tilde{Q}}{Q} = \frac{\overline{b\epsilon^{j_2 k}} + \overline{a\epsilon^{j_1 k}}X}{a\epsilon^{j_1 k} + b\epsilon^{j_2 k}X}.$$

Hence

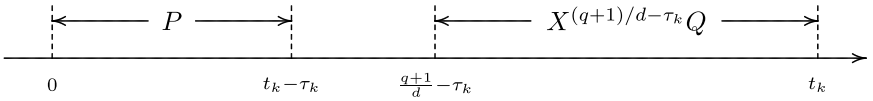

Fig. 4. When $P + X^{(q+1)/d-\tau_k}Q$ is a trinomial.

$$\frac{\overline{b\epsilon^{j_2 k}}}{a\epsilon^{j_1 k}} = \epsilon^k,$$

i.e., $a = b^q \epsilon^{-(j_1+j_2+1)k}$. Clearly, $\pi(k) = 0$.

(ii) Assume (4.9). First, note that $e_k = r - t_k + \tau_k = r - 1$. In this case,

$$L_k = 1 + a\epsilon^{j_1 k} X + X^{\frac{1}{2}(\frac{q+1}{d}+1)} \cdot b\epsilon^{j_2 k},$$

where $P = 1 + a\epsilon^{j_1 k} X$ and $Q = b\epsilon^{j_2 k}$. Since $\tilde{P} = \lambda_k P$ and $\tilde{Q} = \lambda_k \epsilon^k Q$, we have

$$(a\epsilon^{j_1 k})^q = \lambda_k \qquad \text{and} \qquad (b\epsilon^{j_2 k})^{q-1} = \lambda_k \epsilon^k.$$

It follows that

$$a = \lambda_k^{-1} \epsilon^{-j_1 k} = \epsilon^k (b\epsilon^{j_2 k})^{1-q} \cdot \epsilon^{-j_1 k} = b^{1-q} \epsilon^{(2j_2 - j_1 + 1)k}.$$

Since

$$\begin{aligned} \lambda_k^{(q+1)/d} &= (a^q \epsilon^{-j_1 k})^{(q+1)/d} = (b^{q-1} \epsilon^{-(2j_2 - j_1 + 1)k} \epsilon^{-j_1 k})^{(q+1)/d} \\ &= b^{(q^2-1)/d} \epsilon^{-(2j_2+1)k(q+1)/d} = \epsilon^{-(2j_2+1)k(q+1)/d + \beta}, \end{aligned}$$

where $b^{(q^2-1)/d} = \epsilon^\beta$, we have

$$\pi(k) = -(2j_2 + 1)k\frac{q+1}{d} + \beta. \quad \square$$

Remark. In Lemma 4.5, if (i) occurs for all $0 \le k < d$, then $j_1 + j_2 + 1 \equiv 0 \pmod d$ and $a = b^q$. We have

$$\begin{aligned} h(X) &= 1 + aX^{\frac{1}{2}(\frac{q+1}{d}-1)+j_1\frac{q+1}{d}} + bX^{\frac{1}{2}(\frac{q+1}{d}+1)+j_2\frac{q+1}{d}} \\ &\equiv 1 + aX^{\frac{1}{2}(\frac{q+1}{d}-1)+j_1\frac{q+1}{d}} + bX^{q+1-(\frac{1}{2}(\frac{q+1}{d}-1)+j_1\frac{q+1}{d})} \pmod{X^{q+1}-1} \\ &\equiv X^{q+1-l} h_1(X) \pmod{X^{q+1}-1}, \end{aligned}$$

where

$$l = \frac{1}{2}\Big(\frac{q+1}{d} - 1\Big) + j_1\frac{q+1}{d}$$

and

$$h_1(X) = b + X^l + aX^{2l}.$$

Since $a = b^q$, $h_1(X)$ is self-dual. We have

$$X^r h(X^{q-1}) \equiv X^{r+(q+1-l)(q-1)} h_1(X^{q-1}) \pmod{X^{q^2-1} - 1},$$

and PPs of $\mathbb{F}_{q^2}$ of this type are known (Example 5.1).

Similarly, if (ii) occurs for all $0 \le k < d$ in Lemma 4.5, then $2j_2 - j_1 + 1 \equiv 0 \pmod d$ and $a = b^{1-q}$. We have

$$\begin{aligned} h(X) &= 1 + aX^{1+j_1\frac{q+1}{d}} + bX^{\frac{1}{2}(\frac{q+1}{d}+1)+j_2\frac{q+1}{d}} \\ &\equiv 1 + aX^{2(\frac{1}{2}(\frac{q+1}{d}+1)+j_2\frac{q+1}{d})} + bX^{\frac{1}{2}(\frac{q+1}{d}+1)+j_2\frac{q+1}{d}} \pmod{X^{q+1} - 1} \\ &= h_1(X), \end{aligned}$$

where

$$h_1(X) = 1 + bX^l + aX^{2l}, \quad l = \frac{1}{2}\Big(\frac{q+1}{d} + 1\Big) + j_2\frac{q+1}{d}.$$

Since $a = b^{1-q}$, $h_1(X)$ is self-dual. We have

$$X^r h(X^{q-1}) \equiv X^r h_1(X^{q-1}) \pmod{X^{q^2-1} - 1},$$

and PPs of $\mathbb{F}_{q^2}$ of this type are known.

Lemma 4.6. *If $(q+1)/d \neq 3$, then either Lemma 4.4 occurs for all $0 \le k < d$, or Lemma 4.5 (i) occurs for all $0 \le k < d$, or Lemma 4.5 (ii) occurs for all $0 \le k < d$.*

Proof. In Lemma 4.4, Lemma 4.5 (i) and Lemma 4.5 (ii), we have

$$i_1 = \frac{i_2}{2}, \quad \begin{cases} i_1 = \frac{1}{2}\Big(\frac{q+1}{d} - 1\Big), \\ i_2 = \frac{1}{2}\Big(\frac{q+1}{d} + 1\Big), \end{cases} \quad \text{and} \quad \begin{cases} i_1 = 1 \\ i_2 = \frac{1}{2}\Big(\frac{q+1}{d} + 1\Big), \end{cases}$$

respectively. Any two of these three conditions imply that $(q+1)/d = 3$. □

Partition $\mathbb{Z}/d\mathbb{Z}$ as

$$\mathbb{Z}/d\mathbb{Z} = K_0 \sqcup K_1 \sqcup K_2, \tag{4.10}$$

where Lemma 4.4 occurs for $k \in K_0$, Lemma 4.5 (i) occurs for $k \in K_1$, and Lemma 4.5 (ii) occurs for $k \in K_2$. Assume that at least two of K_0, K_1, K_2 are nonempty. Then $(q+1)/d = 3$, $i_1 = 1$ and $i_2 = 2$. Since $\gcd(e_k, 3) = \gcd(e_k, (q+1)/d) = 1$, it follows from Lemmas 4.4 and 4.5 that one of K_0, K_1, K_2 must be empty:

$$\begin{cases} \text{if } r \equiv 0 \pmod 3, \text{ then } K_1 = \emptyset; \\ \text{if } r \equiv 1 \pmod 3, \text{ then } K_2 = \emptyset; \\ \text{if } r \equiv -1 \pmod 3, \text{ then } K_0 = \emptyset. \end{cases}$$

It also follows from Lemmas 4.4 and 4.5 that

$$\begin{cases} \text{if } k_0 \in K_0, \text{ then } b = a^{1-q}\epsilon^{(2j_1-j_2)k_0}; \\ \text{if } k_1 \in K_1, \text{ then } a = b^q\epsilon^{-(j_1+j_2+1)k_1}; \\ \text{if } k_2 \in K_2, \text{ then } a = b^{1-q}\epsilon^{(2j_2-j_1+1)k_2}. \end{cases} \tag{4.11}$$

Any combination of two of the above three equations allow us to determine a and b up to a third root of unity.

Lemma 4.7. *We have the following equivalences:*

$$\begin{cases} b = a^{1-q}\epsilon^{(2j_1-j_2)k_0} \\ a = b^q\epsilon^{-(j_1+j_2+1)k_1} \end{cases} \Leftrightarrow \begin{cases} a^3 = \epsilon^{-(2j_1-j_2)k_0-(j_1+j_2+1)k_1} \\ b = a^2\epsilon^{(2j_1-j_2)k_0} \end{cases} \tag{4.12}$$

$$\begin{cases} b = a^{1-q}\epsilon^{(2j_1-j_2)k_0} \\ a = b^{1-q}\epsilon^{(2j_2-j_1+1)k_2} \end{cases} \Leftrightarrow \begin{cases} a^3 = \epsilon^{-2(2j_1-j_2)k_0-(2j_2-j_1+1)k_2} \\ b = a^2\epsilon^{(2j_1-j_2)k_0} \end{cases} \tag{4.13}$$

$$\begin{cases} a = b^q\epsilon^{-(j_1+j_2+1)k_1} \\ a = b^{1-q}\epsilon^{(2j_2-j_1+1)k_2} \end{cases} \Leftrightarrow \begin{cases} b^3 = \epsilon^{-(j_1+j_2+1)k_1-(2j_2-j_1+1)k_2} \\ a = b^{-1}\epsilon^{-(j_1+j_2+1)k_1} \end{cases} \tag{4.14}$$

Proof. We only prove (4.12). (The proofs of (4.13) and (4.14) are similar.)

($\Rightarrow$) We have

$$b^{q+1} = (a^{1-q}\epsilon^{(2j_1-j_2)k_0})^{q+1} = 1,$$

and hence

$$a^{q+1} = (b^q\epsilon^{-(j_1+j_2+1)k_1})^{q+1} = 1.$$

Now

$$b = a^{1-q}\epsilon^{(2j_1-j_2)k_0} = a^2\epsilon^{(2j_1-j_2)k_0},$$

and

$$a = b^q\epsilon^{-(j_1+j_2+1)k_1} = (a^2\epsilon^{(2j_1-j_2)k_0})^q\epsilon^{-(j_1+j_2+1)k_1} = a^{-2}\epsilon^{-(2j_1-j_2)k_0-(j_1+j_2+1)k_1},$$

i.e.,

$$a^3 = \epsilon^{-(2j_1-j_2)k_0-(j_1+j_2+1)k_1}.$$

($\Leftarrow$) First, since $(q+1)/d = 3$, it is clear that $a^{q+1} = b^{q+1} = 1$. The rest is obvious. □

Lemma 4.8. *Assume that $K_0 \neq \emptyset$ and $K_1 \neq \emptyset$ in (4.10) and hence $(q+1)/d = 3$, $i_1 = 1$, $i_2 = 2$, and $r \equiv 1 \pmod 3$. Then d is even, and K_0 and K_1 form the two cosets of $2\mathbb{Z}/d\mathbb{Z}$ in $\mathbb{Z}/d\mathbb{Z}$. Moreover, $a^3 = -1$, $b = \pm a^2$,*

$$\begin{cases} 2j_1 - j_2 \equiv \dfrac{d}{2} \pmod d, \\ j_1 + j_2 + 1 \equiv \dfrac{d}{2} \pmod d, \end{cases} \tag{4.15}$$

and $\pi(k) + e_k k = rk$ for $k \in \mathbb{Z}/d\mathbb{Z}$. More precisely, either

$$q \equiv 11 \pmod{18} \quad \text{and} \quad h(X) = 1 + aX^{(q+1)/3} + bX^{(q+1)/6}$$

or

$$q \equiv 5 \pmod{18} \quad \text{and} \quad h(X) = 1 + aX^{2(q+1)/3} + bX^{5(q+1)/6}.$$

Proof. If $2j_1 - j_2 \equiv 0 \pmod d$, then by (4.11), $b = a^{1-q}$. Moreover, by the proof of Lemma 4.4, for all $k \in \mathbb{Z}/d\mathbb{Z}$, $L_k \in \mathcal{L}_k(2, 0; \lambda_k)$ with $\lambda_k = b^q \epsilon^{-j_2 k}$. This means that Lemma 4.4 occurs for all $k \in \mathbb{Z}/d\mathbb{Z}$, i.e., $K_0 = \mathbb{Z}/d\mathbb{Z}$, which is a contradiction since $K_1 \neq \emptyset$. Similarly, if $j_1 + j_2 + 1 \equiv 0 \pmod d$, then by (4.11), $a = b^q$. Moreover, by the proof of Lemma 4.5 (i), for all $k \in \mathbb{Z}/d\mathbb{Z}$, $L_k \in \mathcal{L}_k(2, 2; 1)$. This means that Lemma 4.5 (i) occurs for all $k \in \mathbb{Z}/d\mathbb{Z}$, i.e., $K_1 = \mathbb{Z}/d\mathbb{Z}$, which is also a contradiction. Hence $2j_1 - j_2 \neq 0 \pmod d$ and $j_1 + j_2 + 1 \neq 0 \pmod d$.

By (4.11), there exist $u, v \in \mathbb{Z}/d\mathbb{Z}$ such that

$$\begin{cases} (2j_1 - j_2)k \equiv u \pmod d & \text{for all } k \in K_0, \\ (j_1 + j_2 + 1)k \equiv v \pmod d & \text{for all } k \in K_1. \end{cases}$$

Since $2j_1 - j_2 \neq 0 \pmod d$ and $j_1 + j_2 + 1 \neq 0 \pmod d$ and $K_0 \cup K_1 = \mathbb{Z}/d\mathbb{Z}$, we must have

$$\begin{cases} 2j_1 - j_2 \equiv \dfrac{d}{2} \pmod d, \\ j_1 + j_2 + 1 \equiv \dfrac{d}{2} \pmod d, \end{cases}$$

$\{u, v\} = \{0, d/2\}$, and

$$K_0 = \{k \in \mathbb{Z}/d\mathbb{Z} : (2j_1 - j_2)k \equiv u \pmod d\},$$
$$K_1 = \{k \in \mathbb{Z}/d\mathbb{Z} : (j_1 + j_2 + 1)k \equiv v \pmod d\}.$$

It follows from (4.12) that $a^3 = \epsilon^{-u-v} = \epsilon^{d/2} = -1$ and $b = a^2\epsilon^u = \pm a^2$.

By Lemma 4.4 and Lemma 4.5 (i), we have

$$\pi(k) + e_k k = \begin{cases} (r - 2 - 6j_1)k & \text{if } k \in K_0, \\ rk & \text{if } k \in K_1. \end{cases}$$

By (4.15), $3j_1 + 1 \equiv 0 \pmod{d}$, hence $\pi(k) + e_k k = rk$ for $k \in \mathbb{Z}/d\mathbb{Z}$.

System (4.15) is equivalent to

$$\begin{cases} 1 + 3j_1 \equiv 0 \pmod{d}, \\ 2 + 3j_2 \equiv \dfrac{d}{2} \pmod{d}. \end{cases}$$

Since $0 \le j_1, j_2 < d$, we have

$$\begin{cases} 1 + 3j_1 = d, \\ 2 + 3j_2 = \dfrac{d}{2}, \end{cases} \quad \text{or} \quad \begin{cases} 1 + 3j_1 = 2d, \\ 2 + 3j_2 = \dfrac{5d}{2}. \end{cases}$$

In the first case, $d \equiv 4 \pmod 6$, whence $q = 3d - 1 \equiv 11 \pmod{18}$, and

$$h(X) = 1 + aX^{1+3j_1} + bX^{2+3j_2} = 1 + aX^{(q+1)/3} + bX^{(q+1)/6}.$$

In the second case, $d \equiv 2 \pmod 6$, whence $q = 3d - 1 \equiv 5 \pmod{18}$, and

$$h(X) = 1 + aX^{1+3j_1} + bX^{2+3j_2} = 1 + aX^{2(q+1)/3} + bX^{5(q+1)/6}. \quad \square$$

Lemma 4.9. *Assume that $K_0 \neq \emptyset$ and $K_2 \neq \emptyset$ in (4.10) and hence $(q+1)/d = 3$, $i_1 = 1$, $i_2 = 2$, and $r \equiv 0 \pmod 3$. Then d is even, and K_0 and K_2 form the two cosets of $2\mathbb{Z}/d\mathbb{Z}$ in $\mathbb{Z}/d\mathbb{Z}$. Moreover, $a^3 = \pm 1$, $b = -a^{-1}$,*

$$\begin{cases} 2j_1 - j_2 \equiv \dfrac{d}{2} \pmod{d}, \\ 2j_2 - j_1 + 1 \equiv \dfrac{d}{2} \pmod{d}, \end{cases} \tag{4.16}$$

and $\pi(k) + e_k k = rk$ for $k \in \mathbb{Z}/d\mathbb{Z}$. More precisely, either

$$q \equiv 5 \pmod{18} \quad \textit{and} \quad h(X) = 1 + aX^{(q+1)/6} + bX^{5(q+1)/6}$$

or

$$q \equiv 11 \pmod{18} \quad \textit{and} \quad h(X) = 1 + aX^{5(q+1)/6} + bX^{(q+1)/6}.$$

Proof. By the same argument in the proof of Lemma 4.8, we have

$$\begin{cases} 2j_1 - j_2 \equiv \dfrac{d}{2} \pmod{d}, \\ 2j_2 - j_1 + 1 \equiv \dfrac{d}{2} \pmod{d}, \end{cases}$$

and

$$K_0 = \{k \in \mathbb{Z}/d\mathbb{Z} : (2j_1 - j_2)k \equiv u \pmod{d}\},$$
$$K_2 = \{k \in \mathbb{Z}/d\mathbb{Z} : (2j_2 - j_1 + 1)k \equiv v \pmod{d}\},$$

where $\{u, v\} = \{0, d/2\}$. It follows from (4.13) that $a^3 = \epsilon^v = \pm 1$ and $b = a^2\epsilon^u = -a^2\epsilon^v = -a^5 = -a^{-1}$. By Lemma 4.4 and Lemma 4.5 (ii), we have

$$\pi(k) + e_k k = \begin{cases} (r - 2 - 6j_1)k & \text{if } k \in K_0, \\ (r - 4 - 6j_2)k & \text{if } k \in K_2. \end{cases}$$

By (4.16), $6j_1 \equiv -2 \pmod{d}$ and $6j_2 \equiv -4 \pmod{d}$, hence $\pi(k) + e_k k = rk$ for $k \in \mathbb{Z}/d\mathbb{Z}$.

System (4.16) is equivalent to

$$\begin{cases} 1 + 3j_1 \equiv \dfrac{d}{2} \pmod{d}, \\ 2 + 3j_2 \equiv \dfrac{d}{2} \pmod{d}, \end{cases}$$

i.e.,

$$\begin{cases} 1 + 3j_1 = \dfrac{d}{2}, \\ 2 + 3j_2 = \dfrac{5d}{2}, \end{cases} \quad \text{or} \quad \begin{cases} 1 + 3j_1 = \dfrac{5d}{2}, \\ 2 + 3j_2 = \dfrac{d}{2}. \end{cases}$$

In the first case, $d \equiv 2 \pmod{6}$, whence $q = 3d - 1 \equiv 5 \pmod{18}$, and

$$h(X) = 1 + aX^{(q+1)/6} + bX^{5(q+1)/6}.$$

In the second case, $d \equiv 4 \pmod{6}$, whence $q = 3d - 1 \equiv 11 \pmod{18}$, and

$$h(X) = 1 + aX^{5(q+1)/6} + bX^{(q+1)/6}. \quad \square$$

Lemma 4.10. *Assume that $K_1 \neq \emptyset$ and $K_2 \neq \emptyset$ in (4.10) and hence $(q+1)/d = 3$, $i_1 = 1$, $i_2 = 2$, and $r \equiv -1 \pmod{3}$. Then d is even, and K_1 and K_2 form the two cosets of $2\mathbb{Z}/d\mathbb{Z}$ in $\mathbb{Z}/d\mathbb{Z}$. Moreover, $b^3 = -1$, $a = \pm b^{-1}$,*

$$\begin{cases} j_1 + j_2 + 1 \equiv \dfrac{d}{2} \pmod{d}, \\ 2j_2 - j_1 + 1 \equiv \dfrac{d}{2} \pmod{d}, \end{cases} \tag{4.17}$$

and $\pi(k) + e_k k = rk$ *for* $k \in \mathbb{Z}/d\mathbb{Z}$. *More precisely, either*

$$q \equiv 5 \pmod{18} \quad \textit{and} \quad h(X) = 1 + aX^{(q+1)/6} + bX^{(q+1)/3}$$

or

$$q \equiv 11 \pmod{18} \quad \textit{and} \quad h(X) = 1 + aX^{5(q+1)/6} + bX^{2(q+1)/3}.$$

Proof. Again, by the argument in the proof of Lemma 4.8, we have

$$\begin{cases} j_1 + j_2 + 1 \equiv \dfrac{d}{2} \pmod{d}, \\ 2j_2 - j_1 + 1 \equiv \dfrac{d}{2} \pmod{d}, \end{cases}$$

and

$$K_1 = \{k \in \mathbb{Z}/d\mathbb{Z} : (j_1 + j_2 + 1)k \equiv u \pmod{d}\},$$
$$K_2 = \{k \in \mathbb{Z}/d\mathbb{Z} : (2j_2 - j_1 + 1)k \equiv v \pmod{d}\},$$

where $\{u, v\} = \{0, d/2\}$. It follows from (4.14) that $b^3 = \epsilon^{u+v} = -1$ and $a = b^{-1}\epsilon^u = \pm b^{-1}$. By Lemma 4.5 (i) and (ii), we have

$$\pi(k) + e_k k = \begin{cases} rk & \text{if } k \in K_1, \\ (r - 4 - 6j_2)k & \text{if } k \in K_2. \end{cases}$$

By (4.17), $6j_2 \equiv -4 \pmod{d}$, hence $\pi(k) + e_k k = rk$ for $k \in \mathbb{Z}/d\mathbb{Z}$.

System (4.17) is equivalent to

$$\begin{cases} 1 + 3j_1 \equiv \dfrac{d}{2} \pmod{d}, \\ 2 + 3j_2 \equiv 0 \pmod{d}, \end{cases}$$

i.e.,

$$\begin{cases} 1 + 3j_1 = \dfrac{d}{2}, \\ 2 + 3j_2 = d, \end{cases} \quad \text{or} \quad \begin{cases} 1 + 3j_1 = \dfrac{5d}{2}, \\ 2 + 3j_2 = 2d. \end{cases}$$

In the first case, $d \equiv 2 \pmod 6$, whence $q = 3d - 1 \equiv 5 \pmod{18}$, and

$$h(X) = 1 + aX^{(q+1)/6} + bX^{(q+1)/3}.$$

In the second case, $d \equiv 4 \pmod 6$, whence $q = 3d - 1 \equiv 11 \pmod{18}$, and

$$h(X) = 1 + aX^{5(q+1)/6} + bX^{2(q+1)/3}. \quad \square$$

Remark 4.11. In Lemmas 4.8 – 4.10, it is easy to see that the polynomial $h(X)$ satisfies

$$\gcd(h(X),\, X^{q+1} - 1) = 1.$$

For example, in Lemma 4.8, with $q \equiv 11 \pmod{18}$, we have

$$h(X) = 1 + aX^{(q+1)/3} \pm a^2 X^{(q+1)/6},$$

where $a^3 = -1$. Assume to the contrary that $h(X)$ and $X^{q+1} - 1$ have a common root $x \in \mathbb{F}_{q^2}$. Then $a^2 x^{(q+1)/6}$ is a common root of $1 \pm X - X^2$ and $X^6 - 1$. This is impossible since $\gcd(1 \pm X - X^2, X^6 - 1) = 1$.

4.2. Four classes

All permutation trinomials resulting from Algorithm 2.4 have been determined in Section 4.1. These permutation trinomials, excluding those that were previously known, can be categorized into four classes. Each class covers a situation described in a lemma or several lemmas in Section 4.1. Theorem 2.3 is applied to the situation to set the conditions on the parameters. More precisely, these conditions are

- $\gcd(r, q - 1) = 1$;
- $\gcd(e_k, (q + 1)/d) = 1$ for all $0 \le k < d$;
- $\gcd(h(X), X^{q+1} - 1) = 1$ (cf. Remark 2.5);
- the map $k \mapsto \pi(k) + e_k k$ permutes $\mathbb{Z}/d\mathbb{Z}$.

In Class 4, which covers Lemmas 4.8 – 4.10, the condition $\gcd(e_k, (q + 1)/d) = 1$ $(0 \le k < d)$ is satisfied by the choice of $r \pmod 3$, and the condition $\gcd(h(X), X^{q+1} - 1) = 1$ is automatically satisfied by Remark 4.11.

In each class, the permutation trinomial is

$$X^r h(X^{q-1}),$$

where

$$h(X) = 1 + aX^{i_1 + j_1(q+1)/d} + bX^{i_2 + j_2(q+1)/d}.$$

Class 1. (Case 2.1, Lemma 4.1 (ii))

Conditions: $i_1 = 0 < i_2 < (q+1)/d$, $j_1 = d/2$, $0 \le j_2 < d$, $a^{q-1} = -1$, $(1-a)/b \in \mu_{q+1}$,

$$\gcd(1 + aX^{(q+1)/2} + bX^{i_2+j_2(q+1)/d},\ X^{q+1} - 1) = 1,$$

$\gcd(r, q-1) = 1$, $\gcd(r - i_2, (q+1)/d) = 1$, and

$$k \mapsto \Big(-j_2\frac{q+1}{d} + r - i_2\Big)k + \delta(k)v$$

permutes $\mathbb{Z}/d\mathbb{Z}$, where

$$\Big(\frac{1+a}{1-a}\Big)^{(q+1)/d} = \epsilon^v$$

and

$$\delta(k) = \begin{cases} 0 & \text{if } k \text{ is even,} \\ 1 & \text{if } k \text{ is odd.} \end{cases}$$

PP: $X^r(1 + aX^{(q^2-1)/2} + bX^{(q-1)(i_2+j_2(q+1)/d)})$.

Class 2. (Case 2.2, Lemma 4.3 (i))

Conditions: $i_1 = 0 < i_2 < (q+1)/d$, $j_1 = d/2$, $0 \le j_2 < d$, $a = -1$, $(2/b)^{(q+1)/d} = \epsilon^\theta$ for some $\theta \in \mathbb{Z}/d\mathbb{Z}$,

$$\gcd(1 - X^{(q+1)/2} + bX^{i_2+j_2(q+1)/d},\ X^{q+1} - 1) = 1,$$

$\gcd(r, q-1) = 1$, $\gcd(r - i_2, (q+1)/d) = \gcd(r - 2i_2, (q+1)/d) = 1$, and

$$k \mapsto \begin{cases} \Big(-2j_2\frac{q+1}{d} + r - 2i_2\Big)k + 2\theta & \text{if } k \equiv 0 \pmod 2, \\ \Big(-j_2\frac{q+1}{d} + r - i_2\Big)k + \theta & \text{if } k \not\equiv 0 \pmod 2 \end{cases}$$

permutes $\mathbb{Z}/d\mathbb{Z}$.

PP: $X^r(1 - X^{(q^2-1)/2} + bX^{(q-1)(i_2+j_2(q+1)/d)})$.

Class 3. (Case 2.2, Lemma 4.3 (ii))

Conditions: $i_1 = 0 < i_2 < (q+1)/d$, $j_1 = d/3$ or $2d/3$, $0 \le j_2 < d$, $a = -1$, $((1-\epsilon^{j_1})/b)^{(q+1)/d} = \epsilon^\eta$ for some $\eta \in \mathbb{Z}/b\mathbb{Z}$,

$$\gcd(1 - X^{j_1(q+1)/d} + bX^{i_2+j_2(q+1)/d},\ X^{q+1} - 1) = 1,$$

$\gcd(r, q-1) = 1$, $\gcd(r - i_2, (q+1)/d) = \gcd(r - 2i_2, (q+1)/d) = 1$, and

$$k \mapsto \begin{cases} \left(-2j_2\frac{q+1}{d} + r - 2i_2\right)k - j_1\frac{q+1}{d} + \frac{q+1}{\gcd(2,d)} + 2\eta & \text{if } k \equiv 0 \pmod 3, \\ \left(-j_2\frac{q+1}{d} + r - i_2\right)k - j_1\frac{q+1}{d} + \frac{q+1}{\gcd(2,d)} + \eta & \text{if } k \not\equiv 0 \pmod 3 \end{cases}$$

permutes $\mathbb{Z}/d\mathbb{Z}$.

PP: $X^r(1 - X^{j_1(q^2-1)/d} + bX^{(q-1)(i_2+j_2(q+1)/d)})$.

Remark. All permutation trinomials in [11, §2] are covered by Class 2 up to equivalence. All permutation trinomials in [11, §3] are covered by Class 3 (with even q) up to equivalence.

Class 4. (Case 3, Lemmas 4.8 – 4.10) Conditions on q and r and the expressions of $h(X)$ in this class are given in Table 1. There are six cases in Table 1 according to $q \pmod{18}$ and $r \pmod 3$. However, the resulting PP, $X^r h(X^{q-1})$, modulo $X^{q^2-1} - 1$, has only two cases according to $q \pmod{18}$. More precisely, let q, r and $h(X)$ be from Table 1 and let $m = (q^2-1)/6$. If $q \equiv 5 \pmod{18}$, then

$$X^r h(X^{q-1}) \equiv uX^s(1 + cX^m - c^2X^{2m}) \pmod{X^{q^2-1} - 1},$$

for some $s \equiv -1 \pmod 3$, $u \in \mathbb{F}_{q^2}^*$ and $c \in \mu_6$. If $q \equiv 11 \pmod{18}$, then

$$X^r h(X^{q-1}) \equiv uX^s(1 + cX^m - c^2X^{2m}) \pmod{X^{q^2-1} - 1},$$

for some $s \equiv 1 \pmod 3$, $u \in \mathbb{F}_{q^2}^*$ and $c \in \mu_6$.

To verify the above claim, let $l = (q+1)/6$. When $q \equiv 5 \pmod{18}$ and $r \equiv 0 \pmod 3$,

$$h(X) \equiv 1 + aX^l - a^{-1}X^{5l} \equiv -a^{-1}X^{5l}(1 + cX^l - c^2X^{2l}) \pmod{X^{q+1} - 1},$$

where $c = -a \in \mu_6$. Hence

$$X^r h(X^{q-1}) \equiv -a^{-1}X^{r+5l(q-1)}(1 + cX^m - c^2X^{2m}) \pmod{X^{q^2-1} - 1},$$

where $r + 5l(q-1) \equiv -1 \pmod 3$.

When $q \equiv 5 \pmod{18}$ and $r \equiv 1 \pmod 3$,

$$h(X) \equiv 1 + aX^{4l} \pm a^2X^{5l} \equiv aX^{4l}(1 + cX^l - c^2X^{2l}) \pmod{X^{q+1} - 1},$$

where $c = \pm a \in \mu_6$. Hence

$$X^r h(X^{q-1}) \equiv aX^{r+4l(q-1)}(1 + cX^m - c^2X^{2m}) \pmod{X^{q^2-1} - 1},$$

where $r + 4l(q-1) \equiv -1 \pmod 3$.

For the remaining cases in Table 1, the claim is verified similarly.

Table 1
q, r and $h(X)$ in Class 4.

q	r	$h(X)$
$q \equiv 5 \pmod{18}$	$r \equiv 0 \pmod 3$ $\gcd(r, q-1) = 1$	$h(X) = 1 + aX^{(q+1)/6} - a^{-1}X^{5(q+1)/6}$ $a^3 = \pm 1$
	$r \equiv 1 \pmod 3$ $\gcd(r, q-1) = 1$	$h(X) = 1 + aX^{2(q+1)/3} \pm a^2X^{5(q+1)/6}$ $a^3 = -1$
	$r \equiv -1 \pmod 3$ $\gcd(r, q-1) = 1$	$h(X) = 1 \pm b^2X^{(q+1)/6} + bX^{(q+1)/3}$ $b^3 = -1$
$q \equiv 11 \pmod{18}$	$r \equiv 0 \pmod 3$ $\gcd(r, q-1) = 1$	$h(X) = 1 + aX^{5(q+1)/6} - a^{-1}X^{(q+1)/6}$ $a^3 = \pm 1$
	$r \equiv 1 \pmod 3$ $\gcd(r, q-1) = 1$	$h(X) = 1 + aX^{(q+1)/3} \pm a^2X^{(q+1)/6}$ $a^3 = -1$
	$r \equiv -1 \pmod 3$ $\gcd(r, q-1) = 1$	$h(X) = 1 \pm b^2X^{5(q+1)/6} + bX^{2(q+1)/3}$ $b^3 = -1$

4.3. Examples

We give an example in each of the first three classes in Section 4.2. (Note that Class 4 is already explicit.) These are rather simple examples and their primary purpose is to show that none of these classes is empty. Interested readers may explore more elaborate examples as they wish.

Example 4.12 *(Class 1).* Let $q \equiv 1 \pmod 4$, $d = 2$, $i_1 = 0$, $i_2 = 1$, $j_1 = 1$, $j_2 = 0$. Let $a \in \mathbb{F}_{q^2}^*$ be such that $a^{q-1} = -1$ and

$$\left(\frac{1+a}{1-a}\right)^{(q+1)/2} = -1.$$

To see that such a exists, first choose $a_0 \in \mathbb{F}_{q^2}^*$ such that $a_0^{q-1} = -1$ and let $a = ta_0$, $t \in \mathbb{F}_q^*$. Since $((1+a)/(1-a))^{q+1} = 1$, we have $((1+a)/(1-a))^{(q+1)/2} = \pm 1$, i.e.,

$$\left(\frac{1+ta_0}{1-ta_0}\right)^{(q+1)/2} = \pm 1.$$

The equation

$$\left(\frac{1+ta_0}{1-ta_0}\right)^{(q+1)/2} = 1$$

has at most $(q+1)/2$ solutions for t, where $(q+1)/2 < q-1$. Hence there exists $t \in \mathbb{F}_q^*$ such that

$$\left(\frac{1+ta_0}{1-ta_0}\right)^{(q+1)/2} = -1.$$

Let $b \in \mathbb{F}_{q^2}^*$ be such that $(1-a)/b = -1$. Assume that $\gcd(r, q-1) = 1$ and $\gcd(r-1, (q+1)/2) = 1$ ($q = 5$ and $r = 3$ satisfy these conditions). We have

$$h(X) = 1 + aX^{i_1 + j_1(q+1)/2} + bX^{i_2 + j_2(q+1)/2} = 1 + aX^{(q+1)/2} - (1-a)X.$$

We claim that $\gcd(h(X), X^{q+1} - 1) = 1$. Assume to the contrary that $h(X)$ and $X^{q+1} - 1$ have a common root x. Then $x^{(q+1)/2} = \pm 1$. If $x^{(q+1)/2} = 1$, then $x = (1+a)/(1-a)$, whence $x^{(q+1)/2} = ((1+a)/(1-a))^{(q+1)/2} = -1$, which is a contradiction. If $x^{(q+1)/2} = -1$, then $x = (1-a)/(1-a) = 1$, which is also a contradiction.

In the notation of Class 1,

$$k \mapsto \Big(-j_2 \frac{q+1}{d} + r - i_2\Big)k + \delta(k)v = k,$$

which permutes $\mathbb{Z}/2\mathbb{Z}$. Therefore,

$$X^r h(X^{q-1}) = X^r(1 + aX^{(q^2-1)/2} + (1-a)X^{q-1})$$

is a PP of $\mathbb{F}_{q^2}$.

Example 4.13 *(Class 2).* Let $q \equiv 1 \pmod 4$, $d = 2$, $i_1 = 0$, $0 < i_2 < (q+1)/2$, i_2 even, $j_1 = 1$, $j_2 = 0$. Let $a = -1$ and $b \in \mathbb{F}_{q^2}^*$ be such that $(2/b)^{(q+1)/2} = 1$. Assume that $\gcd(r, q-1) = 1$, $\gcd(r - i_2, (q+1)/2) = 1$ and $\gcd(r - 2i_2, (q+1)/2) = 1$ ($q = 5$, $r = 3$ and $i_2 = 2$ satisfy these conditions). We have

$$h(X) = 1 - X^{(q+1)/2} + bX^{i_2}.$$

We claim that $\gcd(h(X), X^{q+1} - 1) = 1$. Assume to the contrary that $h(X)$ and $X^{q+1} - 1$ have a common root x. Then $x^{(q+1)/2} = \pm 1$. If $x^{(q+1)/2} = 1$, then $0 = h(x) = bx^{i_2}$, which is a contradiction. If $x^{(q+1)/2} = -1$, then $x^{i_2} = -2/b$, whence $1 = (x^{(q+1)/2})^{i_2} = (x^{i_2})^{(q+1)/2} = (-2/b)^{(q+1)/2} = -1$, which is also a contradiction.

In the notation of Class 2,

$$k \mapsto \begin{cases} \Big(-2j_2 \dfrac{q+1}{d} + r - 2i_2\Big)k + 2\theta & \text{if } k \equiv 0 \pmod 2 \\ \Big(-j_2 \dfrac{q+1}{d} + r - i_2\Big)k + \theta & \text{if } k \not\equiv 0 \pmod 2 \end{cases} = k,$$

which permutes $\mathbb{Z}/2\mathbb{Z}$. Therefore,

$$X^r h(X^{q-1}) = X^r(1 - X^{(q^2-1)/2} + bX^{i_2(q-1)})$$

is a PP of $\mathbb{F}_{q^2}$.

Example 4.14 *(Class 3).* Let $q = 2^{2n+1}$, $d = 3$, $i_1 = 0$, $0 < i_2 < (q+1)/3$, $j_1 = 1$, $j_2 = 0$. Let $a = -1$ and $b \in \mathbb{F}_{q^2}^*$ be such that $((1-\epsilon)/b)^{(q+1)/3} = 1$, where ϵ is an element of $\mathbb{F}_{q^2}^*$ of order 3. Assume that $i_2 \not\equiv 0, r, (q+1)/3 \pmod 3$, $\gcd(r, q-1) = 1$, $\gcd(r-i_2, (q+1)/3) = 1$ and $\gcd(r-2i_2, (q+1)/3) = 1$ ($q = 2^3$, $r = 3$ and $i_2 = 1$ satisfy these conditions). We have

$$h(X) = 1 - X^{(q+1)/3} + bX^{i_2}.$$

We claim that $\gcd(h(X), X^{q+1}-1) = 1$. Assume to the contrary that $h(X)$ and $X^{q+1}-1$ have a common root x. Then $x^{(q+1)/3} = 1$, ϵ or ϵ^{-1}. If $x^{(q+1)/3} = 1$, then $0 = h(x) = bx^{i_2}$, which is a contradiction. If $x^{(q+1)/3} = \epsilon$, then $x^{i_2} = (1-\epsilon)/b$, whence $\epsilon^{i_2} = (x^{i_2})^{(q+1)/3} = ((1-\epsilon)/b)^{(q+1)/3} = 1$, which is a contradiction. If $x^{(q+1)/3} = \epsilon^{-1}$, then $x^{i_2} = (1-\epsilon^{-1})/b = \epsilon^{-1}(1-\epsilon)/b$, whence $\epsilon^{-i_2} = \epsilon^{-(q+1)/3}$, which is also a contradiction.

In the notation of Class 3,

$$\begin{aligned} k \mapsto & \begin{cases} \left(-2j_2\frac{q+1}{d} + r - 2i_2\right)k - j_1\frac{q+1}{d} + \frac{q+1}{\gcd(2,d)} + 2\eta & \text{if } k \equiv 0 \pmod 3 \\ \left(-j_2\frac{q+1}{d} + r - i_2\right)k - j_1\frac{q+1}{d} + \frac{q+1}{\gcd(2,d)} + \eta & \text{if } k \not\equiv 0 \pmod 3 \end{cases} \\ & = (r-i_2)k - j_1\frac{q+1}{3}, \end{aligned}$$

which permutes $\mathbb{Z}/3\mathbb{Z}$. Therefore,

$$X^r h(X^{q-1}) = X^r(1 - X^{(q^2-1)/3} + bX^{i_2(q-1)})$$

is a PP of $\mathbb{F}_{q^2}$.

4.4. Summary for trinomials

The permutation trinomials of $\mathbb{F}_{q^2}$ constructed in Section 4 are tabulated in Table 2.

Note. To see that the previous constructions of permutation trinomials are covered by the classes in Table 2 up to equivalence, simple transformations are usually needed. For example, [11, Theorem 2.1] gives a permutation trinomial

$$f = X^r(c + X^{(q-1)((q+3)/4+k)} + X^{(q-1)((q^2+3q)/4+k+1)})$$

of $\mathbb{F}_{q^2}$, where $q \equiv 1 \pmod 4$, $(c/2)^{(q+1)/2} = 1$, $\gcd(r, q^2-1) = 1$ and $\gcd(2r-2k-1, (q+1)/2) = 1$. We have

$$f \equiv X^{r+(q-1)((q+3)/4+k)}(1 + X^{(q^2-1)/2} + cX^{(q-1)(i_2+j_2(q+1)/2)}) \pmod{X^{q^2} - X},$$

where $i_2 + j_2(q+1)/2 \equiv -(q+3)/4 - k \pmod{q+1}$. Let $\delta \in \mathbb{F}_{q^2}$ be such that $\delta^{(q^2-1)/2} = -1$. Then

Table 2
Permutation trinomials of $\mathbb{F}_{q^2}$ by Algorithm 2.4.

class	PP	references for special cases
1	$X^r(1+aX^{(q^2-1)/2}+bX^{(q-1)(i_2+j_2(q+1)/d)})$ See 4.2 Class 1 for the conditions on the parameters.	
2	$X^r(1-X^{(q^2-1)/2}+bX^{(q-1)(i_2+j_2(q+1)/d)})$ See 4.2 Class 2 for the conditions on the parameters.	[5,6,11,15]
3	$X^r(1-X^{j_1(q^2-1)/d}+bX^{(q-1)(i_2+j_2(q+1)/d)})$ See 4.2 Class 3 for the conditions on the parameters.	[7,11]
4.1	$X^r(1+aX^{(q^2-1)/6}-a^{-1}X^{5(q^2-1)/6})$ $q\equiv 5 \pmod{18}, r\equiv 0 \pmod 3, \gcd(r,q-1)=1, a^3=\pm 1$.	
4.2	$X^r(1+aX^{5(q^2-1)/6}-a^{-1}X^{(q^2-1)/6})$ $q\equiv 11 \pmod{18}, r\equiv 0 \pmod 3, \gcd(r,q-1)=1, a^3=\pm 1$.	

$$\delta^{-r'}f(\delta X)\equiv X^{r'}(1-X^{(q^2-1)/2}+bX^{(q-1)(i_2+j_2(q+1)/2)}) \pmod{X^{q^2}-X},$$

where $r'=r+(q-1)((q+3)/4+k)$ and $b=c\delta^{(q-1)(i_2+j_2(q+1)/2)}$. This trinomial is covered by Class 2 with $d=2$.

5. Additional examples

In this section we give a few examples using the forward approach of Algorithm 2.4. We continue to follow the notation of Algorithm 2.4.

Example 5.1. Let r and q be such that $\gcd(r,q-1)=1$. Let $d=1$, $s_0=0$ (i.e., $h(0)\neq 0$), $0\le t_0<q+1$, $\tau_0=0$, and $e_0=r-t_0$ be such that $\gcd(e_0,q+1)=1$. Let $h\in\mathcal{L}_0(t_0,0;\lambda_0)$, that is, $h\in\mathbb{F}_{q^2}[X]$ is a self-dual polynomial of degree t_0 such that $\gcd(h,X^{q+1}-1)=1$. Then $X^rh(X^{q-1})$ is a PP of $\mathbb{F}_{q^2}$. This is the PP in [17, Theorem 5.1].

Example 5.2. Let r and q be such that $\gcd(r,q-1)=1$. Let $d=1$, $s_0=0$ (i.e., $h(0)\neq 0$), $0\le t_0<q+1$, $q+1-t_0\le\tau_0\le t_0$ and $e_0=r-t_0+\tau_0$ be such that $\gcd(e_0,q+1)=1$. Let $h\in\mathcal{L}_0(t_0,\tau_0;1)$, that is, $h=P+X^{q+1-\tau_0}Q$, where $P,Q\in\mathbb{F}_{q^2}[X]$, $\deg P=t_0-\tau_0$, $\tilde{P}=P$, $\deg Q=\tau_0+t_0-(q+1)$, $\tilde{Q}=Q$, $\gcd(h,X^{q+1}-1)=1$. Then $X^rh(X^{q-1})$ is a PP of $\mathbb{F}_{q^2}$. This construction does not seem to have appeared in the literature.

As an explicit instance of Example 5.2, let's consider the following situation: Let $q\ge 5$ be odd, $t_0=(q+5)/2$, $\tau_0=(q+1)/2$, $\gcd(r,q-1)=\gcd(r-2,q+1)=1$, $P=1+X^2$, $Q=a^q+aX^2$, where $a\in\mathbb{F}_{q^2}^*$ is such that $(1+a)^{(q^2-1)/2}=(1-a)^{(q^2-1)/2}=(-1)^{(q-1)/2}$. The number of such elements a is $(q^2-1)/4$; see Lemma 5.3 below. Let

$$h(X)=P(X)+X^{(q+1)/2}Q(X)=1+X^2+X^{(q+1)/2}(a^q+aX^2).$$

We claim that $\gcd(h(X),X^{q+1}-1)=1$. Assume to the contrary that $h(X)$ and $X^{q+1}-1$ have a common root x. Then

$$x^{(q+1)/2} = -\frac{1+x^2}{a^q + ax^2},$$

whence

$$1 = x^{q+1} = \Big(\frac{1+x^2}{a^q + ax^2}\Big)^2.$$

Thus

$$\frac{1+x^2}{a^q + ax^2} = \pm 1,$$

giving

$$x^2 = -\frac{1 \mp a^q}{1 \mp a} = -(1 \mp a)^{q-1}.$$

Therefore,

$$1 = (x^2)^{(q+1)/2} = \big(-(1 \mp a)^{q-1}\big)^{(q+1)/2} = (-1)^{(q+1)/2}(1 \mp a)^{(q^2-1)/2} = -1,$$

which is a contradiction.

Therefore,

$$X^r h(X^{q-1}) = X^r(1 + X^{2(q-1)} + a^q X^{(q^2-1)/2} + aX^{(q+5)(q-1)})$$

is a PP of $\mathbb{F}_{q^2}$.

Lemma 5.3. *Let q be odd and*

$$\mathcal{A} = \{a \in \mathbb{F}_{q^2}^* : (1+a)^{(q^2-1)/2} = (1-a)^{(q^2-1)/2} = (-1)^{(q-1)/2}\}.$$

Then $|\mathcal{A}| = (q^2-1)/4$.

Proof. Choose $u \in \mathbb{F}_{q^2}^*$ such that $u^{(q^2-1)/2} = (-1)^{(q-1)/2}$, and let

$$\mathcal{X} = \{(x,y) \in \mathbb{F}_{q^2}^2 : x^2 + y^2 = 2u\}.$$

By [3, Lemma 6.55] or [8, Lemma 6.24], $|\mathcal{X}| = q^2 - 1$. Note that for $a \in \mathbb{F}_{q^2}$,

$$(1+a)^{(q^2-1)/2} = (1-a)^{(q^2-1)/2} = (-1)^{(q-1)/2}$$
$$\Leftrightarrow \begin{cases} 1+a = u^{-1}x^2 \\ 1-a = u^{-1}y^2 \end{cases} \quad \text{for some } (x,y) \in \mathcal{X}.$$

If u is a nonsquare of $\mathbb{F}_{q^2}$, then

Table 3
Sequences in Example 5.4.

k	s_k	t_k	τ_k	$e_k = r - 2s_k - t_k + \tau_k$	$e_k k$	$\pi(k)$	λ_k
0	0	0	0	3	0	0	1
1	1	5	5	1	1	2	$\gamma^{46\cdot 2}$
2	2	2	0	-3	0	1	γ^{46}
3	0	5	3	1	3	1	γ^{46}
4	3	0	0	-3	0	2	$\gamma^{46\cdot 2}$
5	0	7	1	-3	3	2	$\gamma^{46\cdot 2}$

$$|\mathcal{A}| = \frac{1}{4}|\mathcal{X}| = \frac{1}{4}(q^2-1).$$

If u is a square of $\mathbb{F}_{q^2}$, partition $\mathcal{X}$ as $\mathcal{X} = \mathcal{X}_1 \sqcup \mathcal{X}_2 \sqcup \mathcal{X}_3$, where

$$\begin{aligned}
\mathcal{X}_1 &= \{(x,y) \in \mathcal{X} : x^2 \neq 0, u;\ y^2 \neq 0, u\},\\
\mathcal{X}_2 &= \{(x,y) \in \mathcal{X} : x^2 = y^2 = u\},\\
\mathcal{X}_3 &= \{(x,y) \in \mathcal{X} : x = 0 \text{ or } y = 0\}.
\end{aligned}$$

Then $|\mathcal{X}_1| + |\mathcal{X}_2| + |\mathcal{X}_3| = q^2 - 1$, $|\mathcal{X}_2| = 4$ and $|\mathcal{X}_3| = 4$. Hence

$$|\mathcal{A}| = \frac{1}{4}|\mathcal{X}_1| + \frac{1}{2}|\mathcal{X}_3| = \frac{1}{4}(q^2 - 1 - 8) + 2 = \frac{1}{4}(q^2-1). \quad \square$$

We conclude this section with a random concrete example.

Example 5.4. Let $q = 47$, $d = 6$, $r = 3$, so $(q+1)/d = 8$. Let γ be a primitive element of $\mathbb{F}_{47^2}$ with minimal polynomial $X^2 + X + 13$ over $\mathbb{F}_{47}$ and let $\epsilon = \gamma^{(q^2-1)/d} = \gamma^{46\cdot 8}$. Choose sequences s_k, t_k, τ_k, $\pi(k)$, and λ_k as shown in Table 3.

Choose

$$\begin{aligned}
L_0 &= 1 \in \mathcal{L}_0(0,0;1),\\
L_1 &= \gamma^2 + X^3(\gamma^{46\cdot 38} + X^2) \in \mathcal{L}_1(5,5;\gamma^{46\cdot 2}),\\
L_2 &= \gamma^{46\cdot 47} + X^2 \in \mathcal{L}_2(2,0;\gamma^{46}),\\
L_3 &= \gamma^{46\cdot 47} + X^2 + X^5 \cdot \gamma^{25} \in \mathcal{L}_3(5,3;\gamma^{46}),\\
L_4 &= \gamma^2 \in \mathcal{L}_4(0,0;\gamma^{46\cdot 2}),\\
L_5 &= \gamma^{46\cdot 46} + X^6 + X^7 \cdot \gamma^{42} \in \mathcal{L}_5(7,1;\gamma^{46\cdot 2}).
\end{aligned}$$

We have

$$\begin{aligned}
\sum_i M_{i0} X^i &= L_0 = 1,\\
\sum_i M_{i1} X^i &= X L_1 = \gamma^2 X + \gamma^{46\cdot 38} X^4 + X^6,
\end{aligned}$$

$$\sum_i M_{i2}X^i = X^2L_2 = \gamma^{46\cdot 47}X^2 + X^4,$$

$$\sum_i M_{i3}X^i = L_3 = \gamma^{46\cdot 47} + X^2 + \gamma^{25}X^5,$$

$$\sum_i M_{i4}X^i = X^3L_4 = \gamma^2X^3,$$

$$\sum_i M_{i5}X^i = L_5 = \gamma^{46\cdot 46} + X^6 + \gamma^{42}X^7.$$

Hence

$$[M_{ik}] = \begin{bmatrix} 1 & 0 & 0 & \gamma^{46\cdot 47} & 0 & \gamma^{46\cdot 46} \\ 0 & \gamma^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \gamma^{46\cdot 47} & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \gamma^2 & 0 \\ 0 & \gamma^{46\cdot 38} & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \gamma^{25} & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & \gamma^{42} \end{bmatrix}$$

and

$$\begin{aligned}[a_{ij}] &= \frac{1}{6}[M_{ik}][\gamma^{-46\cdot 8kj}] \\ &= \begin{bmatrix} 11+37\gamma & 11+25\gamma & 31+44\gamma & 5+10\gamma & 5+22\gamma & 32+3\gamma \\ 37+39\gamma & 12+32\gamma & 22+40\gamma & 10+8\gamma & 35+15\gamma & 25+7\gamma \\ 3\gamma & 19+32\gamma & 36+12\gamma & 31+3\gamma & 35+32\gamma & 20+12\gamma \\ 37+39\gamma & 35+15\gamma & 22+40\gamma & 37+39\gamma & 35+15\gamma & 22+40\gamma \\ 24+6\gamma & 24+18\gamma & 9+14\gamma & 39+41\gamma & 14+27\gamma & 31+35\gamma \\ 43+36\gamma & 4+11\gamma & 43+36\gamma & 4+11\gamma & 43+36\gamma & 4+11\gamma \\ 16 & 8 & 39 & 31 & 39 & 8 \\ 42+16\gamma & 27+24\gamma & 32+8\gamma & 5+31\gamma & 20+23\gamma & 15+39\gamma \end{bmatrix}. \end{aligned}$$

In conclusion,

$$X^3 \sum_{\substack{0\le i<8 \\ 0\le j<6}} a_{ij}X^{46(i+8j)}$$

is a PP of $\mathbb{F}_{47^2}$.

Data availability

No data was used for the research described in the article.

References

[1] X. Cao, X. Hou, J. Mi, S. Xu, More permutation polynomials with Niho exponents which permute $\mathbb{F}_{p^2}$, Finite Fields Appl. 62 (2020) 101626.
[2] N. Fernando, X. Hou, A piecewise construction of permutation polynomials over finite fields, Finite Fields Appl. 18 (2012) 1184–1194.
[3] X. Hou, Lectures on Finite Fields, Graduate Studies in Mathematics, vol. 190, American Mathematical Society, Providence, RI, 2018.
[4] X. Hou, Number of equivalence classes of rational functions over finite fields, preprint.
[5] G. Kyureghyan, M. Zieve, Permutation polynomials of the form $X+\gamma \mathrm{Tr}(X^k)$, in: Contemporary Developments in Finite Fields and Applications, World Sci. Publ., Hackensack, NJ, 2016, pp. 178–194.
[6] V.P. Lavorante, New families of permutation trinomials constructed by permutations of μ_{q+1}, arXiv: 2105.12012.
[7] K. Li, L. Qu, X. Chen, C. Li, Permutation polynomials of the form $cx+\mathrm{Tr}_{q^l/q}(x^a)$ and permutation trinomials over finite fields with even characteristic, Cryptogr. Commun. 10 (2018) 531–554.
[8] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[9] H. Niederreiter, A. Winterhof, Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields, Discrete Math. 295 (2005) 161–171.
[10] Y.H. Park, J.B. Lee, Permutation polynomials and group permutation polynomials, Bull. Aust. Math. Soc. 63 (2001) 67–74.
[11] X. Qin, L. Yan, Constructing permutation trinomials via monomials on the subsets of μ_{q+1}, AAECC, Published on April 10, 2021https://doi.org/10.1007/s00200-021-00505-8 .
[12] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, in: S.W. Golomb, G. Gong, T. Helleseth, H.-Y. Song (Eds.), Sequences, Subsequences, and Consequences, in: Lecture Notes in Comput. Sci., vol. 4893, Springer, Berlin, 2007, pp. 119–128.
[13] Q. Wang, Cyclotomy and permutation polynomials of large indices, Finite Fields Appl. 22 (2013) 57–69.
[14] Z. Zha, L. Hu, Two classes of permutation polynomials over finite fields, Finite Fields Appl. 18 (2012) 781–790.
[15] D. Zheng, M. Yuan, L. Yu, Two types of permutation polynomials with special forms, Finite Fields Appl. 56 (2019) 1–16.
[16] M.E. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, Proc. Am. Math. Soc. 137 (2009) 2209–2216.
[17] M.E. Zieve, Permutation polynomials on $\mathbb{F}_q$ induced from Rédei function bijections on subgroups of $\mathbb{F}_q^*$, arXiv:1310.0776.