Four Classes of Bivariate Permutation Polynomials over Finite Fields of Even Characteristic

Changhui CHEN[^1], Nonmember, Haibin KAN[^2,††††††], Member, Jie PENG[^2*,††], and Li WANG[^2††††], Nonmembers

SUMMARY Permutation polynomials have important applications in cryptography, coding theory and combinatorial designs. In this letter, we construct four classes of permutation polynomials over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$, where $\mathbb{F}_2$ is the finite field with $2^n$ elements.

Key words: finite field, vectorial Boolean function, binomial, bivariate, permutation polynomial

1. Introduction

A mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called a vectorial Boolean function, also known as an $(n,m)$-function. When $n = 1$, $f$ reduces to a Boolean function. In this letter, we limit our study to the $(n,m)$-functions where $n = m$. Let $\mathbb{F}_{2^n}$ be the finite field with $2^n$ elements, and $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n}\backslash \{0\}$ be the multiplicative group of $\mathbb{F}_{2^n}$. By identifying the vector space $\mathbb{F}_{2^n}^*$ with the additive structure of $\mathbb{F}_{2^n}$, $f$ can be viewed as a mapping from $\mathbb{F}_{2^n}$ to itself. If the mapping $f : c \mapsto f(c)$ is a bijection on $\mathbb{F}_{2^n}$, then $f(x)$ is called a permutation polynomial over $\mathbb{F}_{2^n}$. Due to its important applications in cryptography, coding theory and combinatorial designs (see [8], [13], [14] for instance), permutation polynomials have been intensively studied in the past. The study can be generalized from the case of univariate to bivariate. Let $f_1(x,y), f_2(x,y) \in \mathbb{F}_{2^n}[x,y]$, then $F(x,y) = (f_1(x,y), f_2(x,y))$ is called a permutation polynomial over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ if the corresponding mapping of $F(x,y)$ is a bijection of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

Though the number of papers on univariate permutation polynomials over $\mathbb{F}_{2^n}$ is very large so far [7], the results on bivariate permutation polynomials are not so many. In recent years, to construct permutation polynomials with good cryptographic properties such as low differential uniformity, many researchers investigated permutation polynomials over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ with the form of butterfly structure and obtained several constructions (see for instance [1], [3], [4], [6], [11]). Very recently, Göloğlu [2] classified fractional projective permutations over finite fields, which generalized the results of permutations in the form of (1). In addition, it is worth noting that permutation polynomials can be also utilized for constructing bent functions, which are regarded as maximally nonlinear Boolean functions. For further details, we refer the reader to [5], [9], [10].

In this letter, our aim is to construct explicitly more new bivariate permutation polynomials over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ by using orthogonal system of equations. In our new method, we divide the set $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ into two parts, and verify that the polynomial is injective on each part and the corresponding image sets are disjoint, then it is a permutation polynomial. Finally, we obtain four new classes of such permutation polynomials.

2. Preliminaries

In this section, we introduce some notations and auxiliary results which are useful in the sequel.

Let $n$ be any positive integer and $m \mid n$, we denote by

$$\text{Tr}_{m/n}(x) = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{n-1}}$$

the trace mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$.

The following lemma is directly from Lemma 2.3 of [12].

Lemma 2.1 Let $n, i$ be any positive integers and $x \neq y$ be two elements of $\mathbb{F}_{2^n}$. Then

$$(x^i y + xy^i)^{2^i} = \sum_{x=0}^{i-1} (x^i y)^{2^{i-1}}.$$ 

Throughout this letter, we denote the image set of a polynomial $F(x,y)$ over $\mathbb{A} \times \mathbb{B} \subseteq \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ as $\text{Im}(F(A, B))$.

3. Constructions of Bivariate Permutation Polynomials

In this section, we propose four classes of permutation polynomials over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$.

The first class of permutation polynomials is given as follows.

Theorem 3.1 Let $n, d$ be positive integers such that $\gcd(d, 2^n - 1) = 1$. Let $a \neq b \in \mathbb{F}_{2^n}, f(x,y) \in \mathbb{F}_{2^n}[x,y]$ be a homogeneous polynomial of degree $d$ such that $f(0,y) \neq 0$, $f(x,0) \neq 0$, etc.
Proof. In order to prove that \( F \) is a permutation, one only needs to show that if the system of equations
\[
\begin{align*}
f(x) &= f(1, y) \text{ is a permutation polynomial over } \mathbb{F}_{p^2}.
\end{align*}
\]
Then
\[
\begin{align*}
F(x, y) &= f(x, y) + ax^2 + bx^3
\end{align*}
\]
permutes \( \mathbb{F}_{p^2}^2 \).

**Proof.** To prove that \( F(x, y) = (f_1(x, y), f_2(x, y)) \) permutes \( \mathbb{F}_{p^2}^2 \), one only needs to show under the assumption that for all \( c_1, c_2 \in \mathbb{F}_{p^2}^2 \) the system
\[
\begin{align*}
x^{2+2+2} + x^{2+1} + x^{2+1} + y^2 + y + x^{2+1} + y^2 + x^{2+1} + y^2 + y^2 + y^2 + 2 + 2 + 2 + 2 + 2,
\end{align*}
\]
has a solution \((x_0, y_0) \in \mathbb{F}_{p^2}^2 \), then it must be unique. Firstly, we consider the case that \((x_0, y_0) \in \mathbb{F}_{p^2}^2 \), then this solution is unique. Next we assume that \((x_0, y_0) \in \mathbb{F}_{p^2}^2 \times \mathbb{F}_{p^2}^2 \). Let \( y_0 = s x_0 \) with \( s \in \mathbb{F}_{p^2}^2 \). Then System (4) can be rewritten as
\[
\begin{align*}
x^{2+2+2} + x^{2+2} + y^{2+2} + s^{2+2} + s^{2+1} + s + 1 = c_1,
\end{align*}
\]
and
\[
\begin{align*}
x^{2+2+2} + s^{2+2} + s^{2+1} + s^{2+2} + s^{2+1} + s = c_2.
\end{align*}
\]
Note that if \( c_2 = 0 \), then \( s = 0 \) or \( 2^{2+2+2} + 2^{2+2} + 2^{2+1} + 2^{2+2} + 2^{2+1} + 2^{2+1} + 2^{2+1} = 0 \). For the former, we have \( x_0 = c_1^{2+2+2} \) as \( \gcd(n, 3) = 1 \).

Thus, \((c_1^{2+2+2}, 0)\) is the unique solution of (4). For the latter, one has
\[
\begin{align*}
0 = \text{Tr}((2^{2+2+2} + 2^{2+2} + 2^{2+1} + 2^{2+2} + 2^{2+1} + 2^{2+1} + 2^{2+1})) = \text{Tr}(1),
\end{align*}
\]
which contradicts to \( n \) being odd. Therefore, if \( c_2 \neq 0 \) and let \( c = \frac{c_2}{c_1} \), then System (5) is equivalent to
\[
\begin{align*}
(2^{2+2+2} + 2^{2+2} + 2^{2+1} + 2^{2+2} + 2^{2+1} + 2^{2+1} + 2^{2+1}) \equiv 0
\end{align*}
\]
which implies that \( s = c \). Therefore we have the unique solution \((x_0, y_0) = ((\frac{c_1}{2^{2+2+2}} c_1^{2+2+2}, \frac{c_2}{2^{2+2+2}} c_1^{2+2+2})) \) for (4).

Secondly, for the case \((x_0, y_0) \in \{0\} \times \mathbb{F}_{p^2}^2 \), we get \( y_0 = c_1^{2+2+2} \). This completes the proof.

**Example 3.4** Let \( n = 5 \) and \( i = 1 \), then \( F(x, y) = (x^2 + y + x^2 y + x^2 y + x^2 y + y + x^2 + x^2 y + y + y) \) is a permutation polynomial over \( \mathbb{F}_{p^2}^2 \).

The third class of permutation polynomials is constructed from linear bivariate binomials and quadrinomials of algebraic degree 2.

**Theorem 3.5** Let \( i < n \) be positive integers, \( k = \gcd(n, i) \) and \( f_1(x, y) = (x + ay)^i \), \( f_2(x, y) = x^{2+i} + bx^{2+i} + cxy^{2+i} + dy^{2+i} \in \mathbb{F}_{p^2}[x] \). Let
\[
\begin{align*}
\theta_0 &= a + b,
\theta_1 &= a^2 + c,
\theta_2 &= a^{2+i} + d + a^2 b + ac,
\theta_3 &= a^{2+i} + d,
\theta_4 &= a^{2+i} + d + a^2 c,
\theta_5 &= a^{2+i} + d + a^2 b + ad
\end{align*}
\]
then \( F(x, y) = (f_1(x, y), f_2(x, y)) \) permutes \( \mathbb{F}_{p^2}^2 \).

**Proof.** One only needs to show that if \( F(x_1, y_1) = (x_2, y_2) \), i.e.,
\[
\begin{align*}
\begin{cases}
(x_1 + ay_1)^i = (x_2 + ay_2)^i,

x_1^{2+i} + bx_1^{2+i} + cxy_1^{2+i} + dy_1^{2+i} = x_2^{2+i} + bx_2^{2+i} + cxy_2^{2+i} + dy_2^{2+i}.
\end{cases}
\end{align*}
\]
then $x_1 = x_2$ and $y_1 = y_2$, say $F$ is injective. Firstly, we prove that $F(x, y)$ is injective on $F_{2^n} \times F_{2^n}$. Suppose that (7) holds for some $(x_1, y_1)$ and $(x_2, y_2) \in F_{2^n} \times F_{2^n}$. There exist some $s, r \in F_{2^n}$ such that $y_1 = sx_1$ and $y_2 = rx_2$. Thus, System (7) can be rewritten as

\[
\begin{align*}
(x_1^2 + s + 1)^{2i} &= x_2^2(2r + 1)^{2i}, \\
\left( x_2^{2i + 1}(d + c + b + s + 1) \\ &= x_1^{2i + 1}(d + c + b + r + 1).
\end{align*}
\]

(8a) and (8b)

Raising (8a) and (8b) to $(2^i - 1)$-th power and $2^i$-th power, respectively, and eliminating $x_1$ and $x_2$, one has

\[(as + 1)^{2i + 1}(d + c + b + 1)^{2i}
\]

which is equivalent to

\[(d + c + b + 1)^{2i + 1}(a(r + 1)^{2i + 1} + (ar + 1)^{2i + 1})
\]

since $gcd(2^i - 1, 2^i - 1) = 1$. By expanding (9), we have then

\[
\begin{align*}
&\theta_0(s + r) + \theta_2(s + r)^2 + \theta_3(s + r)^3 s r^2 + \theta_4(s + r)^4 + \theta_5(s^2 + r + s r^2).
\end{align*}
\]

If $s \neq r$, then by the assumptions that $\theta_0 \neq 0$, $\theta_2 \neq 0$, and $\theta_5 \neq 0$, the above equation is equivalent to

\[
\begin{align*}
&\left( \theta_2 + s r \right)^{2i} + \theta_2 + \theta_3 s r + \frac{\theta_4}{\theta_5} (s + r)^{2i - 1} = 0.
\end{align*}
\]

Note that $\left( \frac{s + r}{(s + r)^{2i - 1}} \right)^{2i} = \sum_{i=0}^{i-1} \frac{r}{(s + r)^{2i - 1}}$ by Lemma 2.1 and $\frac{s + r}{(s + r)^{2i - 1}} = \frac{s + r}{(s + r)^{2i - 1}}$. Applying $Tr^2_{F_{2^n}}$ on both sides of the above equation, then we can get

\[
Tr^2_{F_{2^n}} \left( \frac{s + r}{(s + r)^{2i - 1}} \right)^{2i} = 0,
\]

which contradicts to $Tr^2_{F_{2^n}} \left( \frac{s + r}{(s + r)^{2i - 1}} \right)^{2i} = 1$. Therefore, we must have $s = r$, which implies from (7) that

\[
\begin{align*}
(x_1^2 + s + 1)^{2i} &= 0, \\
(d + c + b + s + 1) &= 0.
\end{align*}
\]

Hence if (11) does not hold, then $x_1 = x_2$ and thus $y_1 = y_2$, so that $F(x, y)$ is indeed injective on $F_{2^n} \times F_{2^n}$.

On the other hand, it is easy to see that $F(0, y) = (ay)^{2i + 1}$ is injective on $0 \times F_{2^n}$.

Therefore, we only need to show that

\[
F(F_{2^n} \times F_{2^n}) \cap F(0, F_{2^n}) = 0,
\]

and that (11) does not hold. Assume that $(x_1, y_1) \in F_{2^n} \times F_{2^n}$ and $(x_2, y_2) \in \{0 \times F_{2^n}$ such that $F(x_1, y_1) = F(x_2, y_2)$. Let $y_1 = sx_1$, then (7) can be rewritten as

\[
\begin{align*}
\left( x_1^2 + s + 1 \right)^{2i} &= (ay)^{2i}, \\
\left( x_1^{2i + 1}(d + c + s r + b + 1) \right) \cdot (dy)^{2i + 1}.
\end{align*}
\]

(12a) and (12b)

Raising (12a) and (12b) to $(2^i - 1)$-th power and $2^i$-th power, respectively, and then computing $(d + c + s r + b + 1)$, one gets

\[
\theta_5 s^2 + \theta_6 s + \theta_4 = 0.
\]

Dividing $\theta_5$ and applying $Tr^2_{F_{2^n}}$ on both sides of the above equation, we obtain

\[
Tr^2_{F_{2^n}} \left( \frac{s + r}{(s + r)^{2i - 1}} \right) = 0,
\]

which contradicts to $Tr^2_{F_{2^n}} \left( \frac{s + r}{(s + r)^{2i - 1}} \right) \neq 0$. Thus, one gets $F(F_{2^n} \times F_{2^n}) \cap F(0, F_{2^n}) = 0$. Moreover, it is also easy to check that (11) does not hold by the above discussion.

Thus, $F(x, y)$ permutes $F_{2^n}$.

This completes the proof.

Example 3.6 Let $n = 3$ and $w$ be a primitive element of $F_{2^n}$. Then it can be checked by Magma that $a = b = c = 1$, $d = w$, $i = 3$ and $j = 2$ satisfy all the conditions of Theorem 3.5. Therefore, $F(x, y) = (x^4 + y^4, x^3 + x^2 + y^2 + w^3 y^2 + w^4 y^2)$ is a permutation polynomial over $F_{2^n}$.

Remark 3.7 For $n \leq 5$ and $F(x, y)$ on $F_{2^n} \times F_{2^n}$, we can check by Magma software that the conditions of Theorem 3.5 are also necessary. For example, there are in total 31744 different triples $(a, b, c, d) \in (F_{2^n})^4$ which satisfy the conditions of Theorem 3.5 and the corresponding polynomials are exactly all those $F(x, y) \in F_{2^n} \times F_{2^n}$ permuting $F_{2^n}$.

The fourth class of permutation polynomials is constructed by some bivariate trinomials and quadrinomials of algebraic degree 3.

Theorem 3.8 Let $n = \text{odd}$, $f_1(x, y) = x^4 + x^2 y^2 + x + y$, and $f_2(x, y) = x^4 + x^3 y + xy^2 + y^4$, then $F(x, y) = (f_1(x, y), f_2(x, y))$ permutes $F_{2^n}$.

Proof. Let $(x_1, y_1), (x_2, y_2) \in F_{2^n}$ such that $F(x_1, y_1) = F(x_2, y_2)$, i.e.,

\[
\begin{align*}
(x_1^4 + x_1^2 y_1^2 + x_1 + y_1 = x_2^4 + x_2^2 y_2^2 + x_2 + y_2, \\
x_1^4 + x_1^2 y_1 + x_1 + y_1 = x_2^4 + x_2^2 y_2 + x_2 + y_2.
\end{align*}
\]

(13)

one needs to show $(x_1, y_1) = (x_2, y_2)$.

Firstly, assume that $(x_1, y_1), (x_2, y_2) \in F_{2^n} \times F_{2^n}$. Write $y_1 = sx_1$ and $y_2 = rx_2$ for some $s, r \in F_{2^n}$. Then (13) can be rewritten as

\[
\begin{align*}
(x_1^4 + s^2 + 1) = x_2^4 + r^2 + 1, \\
x_1^4 (s^4 + s + 1) = x_2^4 (r^4 + r^3 + r + 1),
\end{align*}
\]

(14)

which gives

\[
(s^2 + s + 1)(r^4 + r^3 + r + 1) = (r^4 + r^3 + r + 1)(s^4 + s + 1).
\]

(15)
By expanding (15), we have then
\[
s^2r^2(s + r)^2 + srm(s + r)^3 + sr(s + r)^2 + (s + r)^3 + (s + r)^2 = 0.
\] (16)

Suppose that \( s \neq r \). Let \( v = sr \) and \( u = s + r \), the above equation is equivalent to
\[
v^2 + (u + 1)v + u^2 + u + 1 = 0.
\] (17)

Note that
\[
\text{Tr}_1\left(\frac{u^2 + u + 1}{u + 1}\right) = \text{Tr}_1((1) + \frac{u}{u + 1})^2 = 1,
\]
since \( n \) is odd. It means that (17) has no solution in \( \mathbb{F}_{2^n} \).

Therefore, it must hold
\[
s = r.
\]

Note that (18) does not hold, since \( s^2 + s + 1 = 0 \) has no solution in \( \mathbb{F}_{2^n} \). Then we get \( x_1 = x_2 \) and \( y_1 = y_2 \).

On the other hand, since \( F(0, y_1) = (0, y'_1) \), it is obvious that
\[
F(0, y_1) = F(0, y_2)
\]
indicates \( y_1 = y_2 \).

At last, we need to show that (13) cannot hold if
\[
(x_1, y_1) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, (x_2, y_2) \in [0] \times \mathbb{F}_{2^n}.
\]
Assume that there exist some \( (x_1, y_1) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \) and \( (x_2, y_2) \in [0] \times \mathbb{F}_{2^n} \) satisfying (13). Then there is some \( s \in \mathbb{F}_{2^n} \) such that \( y_1 = sx_1 \), and (13) can be rewritten as
\[
\begin{cases}
\chi^n_1(s^2 + s + 1) = 0, \\
\chi^n_1(s^3 + s + 1) = y_2.
\end{cases}
\]

Since \( n \) is odd and \( s^2 + s + 1 \) is irreducible over \( \mathbb{F}_2 \), \( s^2 + s + 1 = 0 \) has no solution in \( \mathbb{F}_{2^n} \), a contradiction.

Therefore, \( F(x, y) \) permutes \( \mathbb{F}_{2^n}^2 \). This completes the proof.

Acknowledgments

This work was supported in part by the National Key Research and Development Program of China under Grant 2019YFB2101703; in part by the National Natural Science Foundation of China under Grants 61972258, 62272107 and U19A2066; in part by the Innovation Action Plan of Shanghai Science and Technology under Grants 20511102200 and 21511102200; in part by the Key Research and Development Program of Guangdong Province under Grant 2020B0101090001, and in part by Open Research Program of Shanghai Key Lab of Intelligent Information Processing under Grant IIPL201902.

References

[12] L. Wang and B. Wu, “General constructions of permutation polynomials of the form \( x^2 + x + \delta x^{2^{n-1}+1} + x \) over \( \mathbb{F}_{2^n}^2 \),” Finite Fields Their Appl., vol.52, pp.137–155, July 2018.