Turkish Journal of Mathematics

Volume 43 | Number 5 Article 6

1-1-2019

Some permutations and complete permutation polynomials over finite fields

PINAR ONGAN

BURCU GÜLMEZ TEMÜR

TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2019) 43: 2154 – 2160
© TÜBİTAK
doi:10.3906/mat-1806-83

Some permutations and complete permutation polynomials over finite fields

Pınar ONGAN[1], **Burcu GÜLMEZ TEMÜR**[2*]
[1]Institute of Applied Mathematics, Middle East Technical University
[2]Department of Mathematics, Faculty of Sciences, Atılım University, Ankara, Turkey

Received: 19.06.2018 • **Accepted/Published Online:** 26.06.2019 • **Final Version:** 28.09.2019

Abstract: In this paper we determine $b \in \mathbb{F}_{q^n}^*$ for which the polynomial $f(x) = x^{s+1} + bx \in \mathbb{F}_{q^n}[x]$ is a permutation polynomial and determine $b \in \mathbb{F}_{q^n}^*$ for which the polynomial $f(x) = x^{s+1} + bx \in \mathbb{F}_{q^n}[x]$ is a complete permutation polynomial where $s = \frac{q^n-1}{t}, t \in \mathbb{Z}^+$ such that $t \mid q^n - 1$.

Key words: Permutation polynomials, complete permutation polynomials, finite fields

1. Introduction

Let q be a power of a prime number and let $\mathbb{F}_q$ be a 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 on $\mathbb{F}_q$ (i.e. the mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$). The explicit constructions of permutation polynomials are studied extensively since they have many theoretical and practical applications in finite fields. They also have important applications in cryptography, coding theory, and combinatorial design theory. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a complete permutation polynomial (CPP) if both $f(x)$ and $f(x) + x$ are permutations of $\mathbb{F}_q$. These polynomials were introduced by Niederreiter and Robinson in [6]. Finding new PPs and CPPs of finite fields is a hard problem and there are few classes of CPPs known. For further studies of CPPs see [4, 5, 7]. The simplest polynomials are monomials. For a positive integer d and $\alpha \in \mathbb{F}_q^*$, the monomial αx^d over $\mathbb{F}_q$ is a CPP if and only if d satisfies $\gcd(d, q-1) = 1$ and the binomial $\alpha x^d + x$ is a PP. Such an integer d is called a CPP exponent over $\mathbb{F}_q$.

Let p be the characteristic of $\mathbb{F}_q$, $n \in \mathbb{N}$ and $s = \frac{q^n-1}{t}$, where $t \in \mathbb{Z}^+$ such that $t \mid q^n - 1$. The main interest of this study is the following question:

Question 1.1 *When does a polynomial of the form $f(x) = x^{s+1} + bx \in \mathbb{F}_{q^n}[x]$ become a CPP of $\mathbb{F}_{q^n}$?*

A subcase of this question in which $t = q - 1$ is answered for the cases $n = 2$ and $n = 3$ in [2], for the case $n = 4$ in [9] and [3], and for the case $n = 6$ in [1].

In this paper we determine b for which the polynomial $f(x) = x^{s+1} + bx \in \mathbb{F}_{q^n}[x]$ is a PP and determine b for which the polynomial $f(x) = x^{s+1} + bx \in \mathbb{F}_{q^n}[x]$ is a CPP, where $s = \frac{q^n-1}{t}$ with $t \in \mathbb{Z}^+$ such that $t \mid q^n - 1$.

*Correspondence: burcu.temur@atilim.edu.tr

2. Main results

Let p be the characteristic of $\mathbb{F}_q$, $n \in \mathbb{N}$ and $s = \frac{q^n-1}{t}$, where $t \in \mathbb{Z}^+$ such that $t \mid q^n-1$. Throughout the paper, let γ be a fixed primitive element of $\mathbb{F}_{q^n}$ and $\zeta = \gamma^s$ be a primitive tth root of unity of $\mathbb{F}_{q^n}$. Let $ind_\gamma(a)$ denote the discrete logarithm of $a \in \mathbb{F}_{q^n}^*$, which is an integer between 0 and q^n-2.

Lemma 2.1 *[8, Theorem 1] Let $a_0, a_1, ..., a_{t-1} \in \mathbb{F}_{q^n}^*$. The polynomial*

$$P(x) = \frac{1}{t}\sum_{i=0}^{t-1}\sum_{j=0}^{t-1} a_i \zeta^{-ji} x^{r_i+js} \in \mathbb{F}_{q^n}[x] \tag{2.1}$$

is a PP of $\mathbb{F}_{q^n}$ if and only if the following statements are satisfied:

i. $\gcd(r_i, s) = 1$ *for any* $i \in \mathbb{Z}$ *such that* $0 \le i \le t-1$.

ii. $\{ind_\gamma(a_i) + ir_i \mid i = 0, 1, ..., t-1\}$ *is a complete set of residues modulo* t.

Moreover, the inverse of $P(x)$ is

$$P^{-1}(x) = \frac{1}{t}\sum_{k=0}^{t-1}\sum_{j=0}^{t-1} b_k \zeta^{-jk} x^{r_k{}'+js}, \tag{2.2}$$

where

- $k := \varphi(i) \equiv ind_\gamma(a_i) + ir_i \,(mod\, t)$,
- $r_k{}' \equiv {r_i}^{-1} \,(mod\, s)$,
- $b_k = {a_i}^{-r_k{}'} \gamma^{i(1-r_i r_k{}')}$,

for each $i \in \mathbb{Z}$ such that $0 \le i \le t-1$.

Proof It comes directly as a result of Theorem 1 in [8] for the field $\mathbb{F}_{q^n}$ instead of $\mathbb{F}_q$. □

If $f(x)$ and $f(x)+x$ are written in the form (2.1), then an answer for Question 1.1 in the introduction section can be obtained by using Lemma 2.1. The following lemma gives the representation of $f(x)$ in the form (2.1). Before going further, we need to prove a proposition that will be used in the proof of Lemma 2.3. Denote the following Vandermonde matrix by $M_k(\omega)$:

$$M_k(\omega) = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{(k-1)} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(k-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{(k-1)} & \omega^{2(k-1)} & \dots & \omega^{(k-1)(k-1)} \end{bmatrix},$$

where ω is a kth root of unity of $\mathbb{F}_{q^n}$.

Proposition 2.2 *Let ω be a kth root of unity of $\mathbb{F}_{q^n}$ and the matrices $M_k(\omega)$ and $M_k(\omega^{-1})$ be defined as above. Then the following identity holds:*

$$M_k(\omega)M_k(\omega^{-1}) = kI,$$

where I is the identity matrix.

Proof Consider the (ij)th entry of the product $M_k(\omega)M_k(\omega^{-1})$. It is equal to

$$\begin{aligned}\left(1,\omega^{(i-1)},\omega^{2(i-1)},...,\omega^{(k-1)(i-1)}\right)\cdot\left(1,\omega^{-(j-1)},\omega^{-2(j-1)},...,\omega^{-(k-1)(j-1)}\right)&\\ = 1+\omega^{(i-1)-(j-1)}+\omega^{2(i-1)-2(j-1)}+...+\omega^{(k-1)(i-1)-(k-1)(j-1)}&\\ = \sum_{l=0}^{k-1}\omega^{l[(i-1)-(j-1)]} = \sum_{l=0}^{k-1}\omega^{l(i-j)}. \quad (2.3)&\end{aligned}$$

Thus, (2.3) will be equal to k in the case $i=j$ and in all other cases it will be equal to

$$\sum_{l=0}^{k-1}\left(\omega^{(i-j)}\right)^l = \frac{\left(\omega^{(i-j)}\right)^k-1}{\omega^{(i-j)}-1} = \frac{\left(\omega^k\right)^{i-j}-1}{\omega^{(i-j)}-1} = 0$$

since ω is a kth root of unity of $\mathbb{F}_{q^n}$. □

Lemma 2.3 *$f(x)=x^{s+1}+bx\in\mathbb{F}_{q^n}[x]$ can be written in the form*

$$P(x) = \frac{1}{t}\sum_{i=0}^{t-1}\sum_{j=0}^{t-1}\left(b+\zeta^i\right)\zeta^{-ji}x^{js+1}\in\mathbb{F}_{q^n}[x].$$

Proof Choosing $r_0=r_1=r_2=...=r_{t-1}=1$ in (2.1), then

$$\begin{aligned}P(x) = &\left(\frac{a_0}{t}+\frac{a_1}{t}+\frac{a_2}{t}+\cdots+\frac{a_{t-1}}{t}\right)x\\ &+\left(\frac{a_0}{t}+\frac{a_1\zeta^{-1}}{t}+\frac{a_2\zeta^{-2}}{t}+\cdots+\frac{a_{t-1}\zeta^{-(t-1)}}{t}\right)x^{s+1}\\ &+\left(\frac{a_0}{t}+\frac{a_1\zeta^{-2}}{t}+\frac{a_2\zeta^{-4}}{t}+\cdots+\frac{a_{t-1}\zeta^{-2(t-1)}}{t}\right)x^{2s+1}+\cdots\\ &+\left(\frac{a_0}{t}+\frac{a_1\zeta^{-(t-1)}}{t}+\frac{a_2\zeta^{-2(t-1)}}{t}+\cdots+\frac{a_{t-1}\zeta^{-(t-1)(t-1)}}{t}\right)x^{(t-1)s+1},\end{aligned}$$

and this polynomial is equal to $f(x)=x^{s+1}+bx$ if and only if the following system of equations is satisfied:

$$b = \frac{a_0}{t}+\frac{a_1}{t}+\frac{a_2}{t}+...+\frac{a_{t-1}}{t}$$

$$1 = \frac{a_0}{t}+\frac{a_1\zeta^{-1}}{t}+\frac{a_2\zeta^{-2}}{t}+...+\frac{a_{t-1}\zeta^{-(t-1)}}{t}$$

$$0 = \frac{a_0}{t} + \frac{a_1\zeta^{-2}}{t} + \frac{a_2\zeta^{-4}}{t} + ... + \frac{a_{t-1}\zeta^{-2(t-1)}}{t}$$
$$...$$
$$0 = \frac{a_0}{t} + \frac{a_1\zeta^{-(t-1)}}{t} + \frac{a_2\zeta^{-2(t-1)}}{t} + ... + \frac{a_{t-1}\zeta^{-(t-1)(t-1)}}{t}$$

In fact, this system of equations can also be represented as follows:

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta^{-1} & \zeta^{-2} & \dots & \zeta^{-(t-1)} \\ 1 & \zeta^{-2} & \zeta^{-4} & \dots & \zeta^{-2(t-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{-(t-1)} & \zeta^{-2(t-1)} & \dots & \zeta^{-(t-1)(t-1)} \end{bmatrix} \begin{bmatrix} \frac{a_0}{t} \\ \frac{a_1}{t} \\ \frac{a_2}{t} \\ \vdots \\ \frac{a_{t-1}}{t} \end{bmatrix} = \begin{bmatrix} b \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{2.4}$$

Note that the matrix on the left in (2.4) can also be denoted by $M_t\left(\zeta^{-1}\right)$ since ζ is a primitive tth root of unity. Therefore, we get

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{t-1} \end{bmatrix} = t\left(M_t\left(\zeta^{-1}\right)\right)^{-1} \begin{bmatrix} b \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{2.5}$$

On the other hand, Proposition 2.2 gives us the equality

$$M_t(\zeta)\, M_t\left(\zeta^{-1}\right) = tI,$$

which is directly implying

$$\left(M_t\left(\zeta^{-1}\right)\right)^{-1} = \frac{1}{t} M_t(\zeta).$$

Thus, we conclude from (2.5) that

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{t-1} \end{bmatrix} = M_t(\zeta) \begin{bmatrix} b \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} b+1 \\ b+\zeta \\ b+\zeta^2 \\ \vdots \\ b+\zeta^{(t-1)} \end{bmatrix}.$$

Therefore, if one chooses

$$a_i := b + \zeta^i, \quad \text{for all } 0 \le i \le t-1,$$

then she will obtain the polynomial $f(x)$ of the form (2.1). □

Theorem 2.4 *$f(x) = x^{s+1} + bx \in \mathbb{F}_{q^n}[x]$ is a PP of $\mathbb{F}_{q^n}$ if and only if $b \in \mathbb{F}_{q^n}^*$ satisfies the identities $b \neq -\gamma^{si}$, for any $0 \le i \le t-1$ and*

$$b \neq -\gamma^{sj} + \frac{\gamma^{si} - \gamma^{sj}}{\gamma^{j-i+rt} - 1},$$

for every distinct elements i and j of the set $\{0, 1, ..., t-1\}$ and $0 \le r \le s-1$.

Proof If $b=-\gamma^{si}$, for some $0\leq i\leq t-1$ we then have $f(x)=x^{s+1}+bx=x(x^s+b)=x(x^s-\gamma^{si})=0$ whenever $x=\gamma^i$ or $x=0$, which implies that $f(x)$ is not a PP. Therefore, we must have $b\neq-\gamma^{si}$, for any $0\leq i\leq t-1$.

Lemmas 2.1 and 2.3 imply that $f(x)=x^{s+1}+bx\in\mathbb{F}_{q^n}[x]$ is a PP of $\mathbb{F}_{q^n}$ if and only if

$$\left\{ind_\gamma(b+\zeta^i)+i \mid i=0,1,...,t-1\right\}$$

is a complete set of residues modulo t and this is possible if and only if

$$ind_\gamma(b+\zeta^i)+i\not\equiv ind_\gamma(b+\zeta^j)+j,\ \forall\, 0\leq i<j\leq t-1, \tag{2.6}$$

modulo t. Suppose that $ind_\gamma(b+\zeta^i)+i=ind_\gamma(b+\zeta^j)+j+rt$, for some i,j with $0\leq i<j\leq t-1$ and $0\leq r\leq s-1$. It means there exists $k\in\mathbb{Z}^+$ such that

$$k-i=ind_\gamma(b+\zeta^i)\ \text{ and } k-j-rt=ind_\gamma(b+\zeta^j).$$

Therefore, k is the least positive integer greater than j satisfying

$$\gamma^{k-i}=b+\zeta^i\ \text{ and }\gamma^{k-j}=\gamma^{rt}\left(b+\zeta^j\right). \tag{2.7}$$

Since $b+\zeta^i=\gamma^{k-i}=\gamma^{j-i}\gamma^{k-j}=\gamma^{j-i}\gamma^{rt}\left(b+\zeta^j\right)$, (2.7) can also be written as

$$b+\zeta^i=\gamma^{j-i+rt}\left(b+\zeta^j\right),$$

which directly implies that

$$b=\frac{\gamma^{si}-\gamma^{sj+j-i+rt}}{\gamma^{j-i+rt}-1}=-\gamma^{sj}+\frac{\gamma^{si}-\gamma^{sj}}{\gamma^{j-i+rt}-1}.$$

Therefore, (2.6) is satisfied if and only if

$$b\neq-\gamma^{sj}+\frac{\gamma^{si}-\gamma^{sj}}{\gamma^{j-i+rt}-1},$$

for any $0\leq i<j\leq t-1$ and $0\leq r\leq s-1$. □

Corollary 2.5 *$f(x)=x^{s+1}+bx\in\mathbb{F}_{q^n}[x]$ is a CPP of $\mathbb{F}_{q^n}$ if and only if $b+1\neq-\gamma^{si}$, for any $0\leq i\leq t-1$ and both $b\in\mathbb{F}_{q^n}^*$ and $b+1\in\mathbb{F}_{q^n}^*$ are not equal to*

$$-\gamma^{sj}+\frac{\gamma^{si}-\gamma^{sj}}{\gamma^{j-i+rt}-1},$$

for any $0\leq i<j\leq t-1$ and $0\leq r\leq s-1$.

Proof If $b+1=-\gamma^{si}$, for some $0\leq i\leq t-1$ we then have $f(x)+x=x^{s+1}+(b+1)x=x(x^s+b+1)=x(x^s-\gamma^{si})=0$ whenever $x=\gamma^i$ or $x=0$, which implies that $f(x)$ is not a PP. Therefore, we must have $b+1\neq-\gamma^{si}$, for any $0\leq i\leq t-1$.

Similar to the proof of Lemma 2.3, $f(x)+x=x^{s+1}+x(b+1)$ can be written in the form (2.1) if one chooses a_i as follows:

$$a_i := b+1+\zeta^i, \quad \text{for all } 0 \leq i \leq t-1.$$

By Lemma 2.1, we know that $f(x)+x=x^{s+1}+(b+1)x \in \mathbb{F}_{q^n}[x]$ is a PP of $\mathbb{F}_{q^n}$ if and only if

$$\left\{ind_\gamma(b+1+\zeta^i)+i \mid i=0,1,...,t-1\right\}$$

is a complete set of residues modulo t, which is possible if and only if

$$ind_\gamma(b+1+\zeta^i)+i \not\equiv ind_\gamma(b+1+\zeta^j)+j, \forall\, 0 \leq i < j \leq t-1, \tag{2.8}$$

modulo t. Consider the case $ind_\gamma(b+1+\zeta^i)+i = ind_\gamma(b+1+\zeta^j)+j+rt$, for some $0 \leq i < j \leq t-1$ and $0 \leq r \leq s-1$. Similar to the proof of Theorem 2.4, we get the identity

$$b = -\left(\gamma^{sj}+1\right)+\frac{\gamma^{si}-\gamma^{sj}}{\gamma^{j-i+rt}-1}.$$

Therefore, (2.8) is satisfied if and only if

$$b+1 \neq -\gamma^{sj}+\frac{\gamma^{si}-\gamma^{sj}}{\gamma^{j-i+rt}-1},$$

for any $0 \leq i < j \leq t-1$ and $0 \leq r \leq s-1$. □

Acknowledgments

We want to thank to Q. Wang for his valuable suggestions and ideas. We also thank the anonymous referee for the valuable suggestions and comments.

References

[1] Bartoli D, Zini G. On monomial complete permutation polynomials. Finite Fields and Their Applications 2016; 41: 132-158.

[2] Bassalygo LA, Zinoviev VA. Permutation and complete permutation polynomials. Finite Fields and Their Applications 2015; 33: 198-211.

[3] Bassalygo LA, Zinoviev VA. On one class of permutation polynomials over finite fields of characteristic two. Moscow Mathematical Journal 2015; 15 (4): 703-713.

[4] Laigle-Chapuy Y. Permutation polynomials and applications to coding theory. Finite Fields and Their Applications 2007; 13 (1): 58-70.

[5] Mullen GL, Niederreiter H. Dickson polynomials over finite fields and complete mappings. Canadian Mathematical Bulletin 1987; 30 (1): 19-27.

[6] Niederreiter H, Robinson KH. Complete mappings of finite fields. Journal of the Australian Mathematical Society (Series A) 1982; 33: 197-212.

[7] Wan D. On a problem of Niederreiter and Robinson about finite fields. Journal of the Australian Mathematical Society (Series A) 1986; 41 (3): 336-338.

[8] Wang Q. A note on inverses of cyclotomic mapping permutation polynomials over finite fields. Finite Fields and Their Applications 2017; 45: 422-427.

[9] Wu G, Li N, Helleseth T, Zhang Y. Some classes of complete permutation polynomials over $\mathbb{F}_q$. Science China Mathematics 2015; 58 (10): 2081-2094.