

ON STRONG COMPLETE MONOMIALS AND ITS MULTIPLICATIVE ANALOGUE OVER FINITE FIELDS

AMELA MURATOVIĆ-RIBIĆ AND SHAIPI SURDULLI

ABSTRACT. We present an extended class of complete and strong complete monomials over a finite field. These monomials can also be viewed as generalized complete and strong complete mappings. In the second part of the article we give basic properties of polynomials induced by complete mappings, orthomorphisms and strong complete mappings over a multiplicative group of the finite field.

1. INTRODUCTION

Let $(G, *)$ be a group. A $\theta : G \rightarrow G$ mapping is called a complete mapping over the group $(G, *)$ if both $\theta(x)$ and $\theta(x) * x$ are bijections. A $\theta : G \rightarrow G$ mapping is called an orthomorphism if both $\theta(x)$ and $\theta(x) * x^{-1}$ are bijections. A $\theta : G \rightarrow G$ mapping is called a strong complete mapping if it is the complete mapping and the orthomorphism. The complete mappings have application in a construction of the mutually orthogonal Latin squares and strong complete mappings are applied in constructions of the Knut Vic designs, strong starters and group sequences (see [2]).

Let p be a prime, let m be a positive integer and $q = p^m$. Let $(\mathbb{F}_q, +, \cdot)$ be a finite field of order q . When underlying structure is a finite field complete mappings and orthomorphisms are considered over the additive group $(\mathbb{F}_q, +)$. A permutation $f(x)$ over \mathbb{F}_q is called a complete mapping if $f(x) + x$ is also permutation over finite field. A permutation $f(x)$ over \mathbb{F}_q is called an orthomorphism if $f(x) - x$ is a permutation over \mathbb{F}_q . A mapping that is both a complete mapping and an orthomorphism over a finite field is called a strong complete mapping. It is known that every mapping $\theta : \mathbb{F}_q \rightarrow \mathbb{F}_q$ can be represented by a polynomial $f(x) \in \mathbb{F}_q[x]$ with $\deg(f(x)) < q$ so that $\theta(s) = f(s)$ for every $s \in \mathbb{F}_q$. This polynomial can be evaluated by $f(x) = \sum_{s \in \mathbb{F}_q} [1 - (x - s)^{q-1}] \theta(s)$. If the mapping θ is a bijection over \mathbb{F}_q then its induced polynomial $f(x)$ is called a permutation polynomial. The polynomials which correspond to the complete (strong complete) mappings are called complete (strong complete) polynomials. More details on

2000 *Mathematics Subject Classification.* 11T06, 12Y05.

Key words and phrases. finite fields, complete mappings, strong complete mappings.

complete polynomials over the finite fields can be found in [6], [8], [10] and [11]. In [1] the strong complete mappings were called very complete mappings and many results were provided on this topic. In [5] generalized complete polynomials motivated by the application for check digit systems are introduced. Here, there is a requirement for the permutation polynomials $f(x)$ that all of $f(x) \pm x$ and $f^{(2)}(x) \pm x = f(f(x)) \pm x$ are also permutation polynomials. Furthermore, we will use notation $f \circ f = f^{(2)}, f \circ f \circ f = f^{(3)}$, ect. Let $\mathcal{K} = \{t_1, t_2, \dots, k_s\}$ be a set of positive integers. The mapping $f(x)$ is called a generalized \mathcal{K} -complete mapping if $f(x)$ and $x + \sum_{i=1}^s f^{(t_i)}(x)$ are both permutations over \mathbb{F}_q . In [9] polynomials with this property of the form $f(x) = \frac{a-b}{n} (\sum_{i=1}^{n-1} x^{i \frac{q-1}{n}}) + \frac{a+b(n-1)}{n} x$ were considered.

In this article we extend the class of monomials introduced by Harald Niederreiter and Karl H. Robinson [8] and we show that some of these monomials are such that $f(x)$, $f(x) \pm x$ and $f(x)^{(2)} \pm x$ are all permutations. An advantage of using monomials is their easy evaluation.

Furthermore, we introduce some basic properties of the polynomials induced by the complete and the strong complete mappings on the multiplicative group of the finite field that can be used in combinatorial designs. Even the multiplicative group of the finite field is cyclic and these type of mappings are well investigated in the theory of finite groups (see [2]), here an advantage is in the representation of the mapping by the polynomial.

2. STRONG COMPLETE MONOMIALS

Let p be a prime, let n be a positive integer and let $q = p^n$, Let \mathbb{F}_q be a finite field of order q . The class $ax^{(q+n-1)/n} + bx, q \equiv 1 \pmod{n}, n \geq 2$ of the permutation polynomials and complete polynomials was considered by Harald Niederreiter and Karl H. Robinson [8]. Wun-Seng Chou [1] considered strong complete polynomials of this form for $n = 2$.

We can easily modify results of H. Niederreiter and K.H. Robinson to obtain the criterion for the strong complete mappings. Define $\Psi_n(x) = x^{\frac{q-1}{n}}$ for $n|q-1$ (see [8]). We will use the following two results.

Lemma 2.1 (Lemma 1., [8]). *If $n \geq 2$ is an integer such that $q \equiv 1 \pmod{n}$, then $x^{\frac{q-n+1}{n}} + bx \in \mathbb{F}_q$ is a permutation polynomial of \mathbb{F}_q if and only if the following conditions hold:*

- (i) $(-b)^n \neq 1$
- (ii) $\Psi_n((b + \omega^i)(b + \omega^j)^{-1}) \neq \omega^{j-i}$ for all $0 \leq i < j < n$, where ω is a fixed primitive n -th root of unity in \mathbb{F}_q .

Theorem 2.2 (Theorem 4, [8]). *If $n \geq 2$ is an integer such that $q \equiv 1 \pmod{n}$, then $ax^{\frac{q-n+1}{n}} + bx \in \mathbb{F}_q$ is a complete mapping of \mathbb{F}_q if and only if the following conditions hold:*

- (i) $b^n \neq (-a)^n, (b+1)^n \neq (-a)^n$
- (ii) $\Psi_n((b+a\omega^i)(b+a\omega^j)^{-1}) \neq \omega^{j-i}$ and $\Psi_n((b+1+a\omega^i)(b+1+a\omega^j)^{-1}) \neq \omega^{j-i}$ for all $0 \leq i < j < n$, where ω is a fixed primitive n -th root of unity in \mathbb{F}_q .

Note that $f(x)$ is a strong complete mapping if and only if both $f(x)$ and $f(x) - x$ are complete mappings. Using $b = 0$ and $b = -1$ in Theorem 4, [8] we directly obtain the following result.

Theorem 2.3. *If $n \geq 2$ is an integer such that $q \equiv 1 \pmod{n}$, then $ax^{\frac{q-1}{n}+1}, a \neq 0$ is a strong complete mapping polynomial of \mathbb{F}_q if and only if the following conditions hold:*

- (i) $a^n \neq 1$ if n is even, and $a^n \neq \pm 1$ if n is odd.
- (ii) $\gcd(\frac{q-1}{n} - 1, n) = 1$ and $\Psi_n((\pm 1 + a\omega^i)(\pm 1 + a\omega^j)^{-1}) \neq \omega^{j-i}$ for all $0 \leq i < j < n$, where ω is a fixed primitive n -th root of unity in \mathbb{F}_q .

Proof. Using $b = -1$ and $b = 0$ in (i) of the Theorem 4, [8] we obtain $(-1)^n \neq (-a)^n, a \neq 0$ and $1^n \neq (-a)^n$. If n is even it follows $a^n \neq 1$. If n is odd then we have $a^n \neq \pm 1$.

Using $b = 0$ in (ii) of the Theorem 4, [8] we obtain $\Psi_n(\omega^{j-i}) \neq \omega^{j-i}$ where $0 \leq i < j < n$ what is equivalent with $\omega^{i\frac{q-1}{n}} \neq \omega^i$ for all $1 \leq i < n$. As ω is a primitive n -th root of unity this is possible only if $i\frac{q-1}{n} \not\equiv i \pmod{n}$ or equivalently $i(\frac{q-1}{n} - 1) \not\equiv 0 \pmod{n}$ for $1 \leq i < n$. If $d = \gcd(\frac{q-1}{n} - 1, n)$ then for $i = \frac{n}{d}$ we have that $i(\frac{q-1}{n} - 1) \equiv 0 \pmod{n}$ and this with $1 \leq i$ implies $i = \frac{n}{d} = n$, i.e. $d = 1$.

Also, substitution of $b = 0$ and $b = -1$ implies $\Psi_n((\pm 1 + a\omega^i)(\pm 1 + a\omega^j)^{-1}) \neq \omega^{j-i}$ for all $0 \leq i < j < n$. □

Note that if both b and $b - 1$ fulfill the Theorem 4, [8] we can obtain conditions for strong complete binomials of the given form.

Even some researchers considered the monomials of the form $f(x) = ax^{\frac{q-1}{n}+1}$ where $q = p^m$ and n is an integer such that $n \mid q - 1$, there are examples of the strong complete monomials (and therefore the complete monomials) of the form

$$ax^{\ell\frac{q-1}{n}+1}$$

where $0 < \ell < n$ which was not mentioned in any literature before.

Example 2.1. *For $p = q = 73, n = 4, \ell = 3$ and $a = 4$ polynomial*

$$f(x) = ax^{\ell\frac{q-1}{n}+1} = 4x^{3\frac{73-1}{4}+1} = 4x^{55} = 4x^{3\frac{q-1}{4}+1},$$

is a strong complete polynomial.

For $p = q = 89, n = 4, \ell = 3$ and $a = 8$ polynomial $g(x) = ax^{\ell\frac{q-1}{n}+1} = 8x^{3\frac{q-1}{4}+1} = 8x^{67}$ is a strong complete polynomial.

Modifying the proof of Lemma 1 in [8] we can easily obtain the following results.

Theorem 2.4. *Let $q = p^m$, where p is a prime and m is a positive integer. Let \mathbb{F}_q be a finite field of order q . Assume that $n \mid q - 1$. The polynomial $f(x) = ax^{\ell \frac{q-1}{n} + 1} \in \mathbb{F}_q$ where $0 < \ell < n$, $\gcd(\ell, n) = 1$ and $\gcd(\ell \frac{q-1}{n} + 1, q - 1) = 1$ is a complete polynomial if*

- (i) $(-a^{-1})^n \neq 1$
- (ii) $\Psi_n((a\omega^{\ell i} + 1)(a\omega^{\ell j} + 1)^{-1}) \neq \omega^{j-i}$ for all $0 \leq i < j < n$ where ω is primitive n -th root of unity in \mathbb{F}_q .

Theorem 2.5. *Let $q = p^m$, where p is a prime and m is a positive integer. Let \mathbb{F}_q be a finite field of order q . Assume that $n \mid q - 1$. The polynomial $f(x) = ax^{\ell \frac{q-1}{n} + 1} \in \mathbb{F}_q$ where $0 < \ell < n$, $\gcd(\ell, n) = 1$ and $\gcd(\ell \frac{q-1}{n} + 1, q - 1) = 1$ is a strong complete polynomial if*

- (i) $(\pm a^{-1})^n \neq 1$
- (ii) $\Psi_n((a\omega^{\ell i} \pm 1)(a\omega^{\ell j} \pm 1)^{-1}) \neq \omega^{j-i}$ for all $0 \leq i < j < n$ where ω is primitive n -th root of unity in \mathbb{F}_q .

We will show that some of these monomials have property that $f(x)$, $f(x) \pm x$ and $f^{(2)} \pm x$ are all permutations, i.e. $f^{(2)}(x)$ is also the strong complete mapping.

Indeed, $f(x) = ax^{\frac{q-1}{2} + 1}$ is a strong complete mapping if $\Psi_2(1 - a^2) = 1$ and $4 \mid q - 1$. But then

$$f^{(2)}(x) = a(ax^{\frac{q-1}{2} + 1})^{\frac{q-1}{2} + 1} = a^{\frac{q-1}{2} + 2} x^{\frac{q-1}{4}(q-1) + (q-1) + 1} = a^{\frac{q-1}{2} + 2} x$$

which is a strong complete mapping if $a^{\frac{q-1}{2} + 2} \neq \pm 1$. Since, $a^{\frac{q-1}{2}} = \pm 1$ it follows $a^2 \neq \pm 1$. But, as $\Psi_2(1 - a^2) = 1$ we have that $a^2 \neq 1$. Thus, if $a^2 \neq -1$ then every strong complete polynomial of the form $f(x) = ax^{\frac{q-1}{2} + 1}$ has property that $f^{(2)}(x)$ is strong complete polynomial what was required for check digit systems in [5].

Example 2.2. *For $p = 13$, the polynomial $f(x) = 2x^7$ is a strong complete polynomial with $f^{(2)}(x) = 9x$ also being a strong complete polynomial.*

Similarly, if $n^2 \mid q - 1$ then for a strong complete polynomial of the form $f(x) = ax^{\ell \frac{q-1}{n} + 1}$ we have that $f^{(2)}(x) = a^{\ell \frac{q-1}{n} + 2} x^{2\ell \frac{q-1}{n} + 1}$ which is a polynomial of the same form and can be a strong complete polynomial.

Example 2.3. *For $p = q = 73$, $n = 3$, $a = 16$ and $\ell = 1$ polynomial*

$$f(x) = ax^{\ell \frac{q-1}{n} + 1} = 16x^{25}$$

and $f^{(2)}(x) = 37x^{49}$ are both a strong complete polynomials.

From the Theorem 2.6. we directly obtain the following result.

Theorem 2.6. *Let $q = p^m$ where p is a prime and m is a positive integer. Let \mathbb{F}_q be a finite field of order q . Assume that $n \mid q - 1$. The polynomials $f(x) = ax^{\ell \frac{q-1}{n} + 1} \in$*

$\mathbb{F}_q[x]$, where $0 < \ell < n$ and $\gcd(\ell \frac{q-1}{n} + 1, q-1) = 1$, is a strong complete and $f^{(2)}(x) = f \circ f(x)$ is also a strong complete if

- (i) $(\pm a)^n \neq 1, (\pm a)^{2n} \neq 1$.
- (ii) $\Psi_n((a\omega^{\ell i} \pm 1)(a\omega^{\ell j} \pm 1)^{-1}) \neq \omega^{j-i}$ and $\Psi_n((a^{\ell \frac{q-1}{n} + 2} \omega^{2\ell i} \pm 1)(a^{\ell \frac{q-1}{n} + 2} \omega^{2\ell j} \pm 1)^{-1}) \neq \omega^{j-i}$ for all $0 \leq i < j < n$ where ω is primitive n -th root of unity in \mathbb{F}_q .

Note that $n^2 \mid q-1$ implies $f^{(3)}(x) = a^{3\ell \frac{q-1}{n} + 3} x^{3\ell \frac{q-1}{n} + 1}$ and this polynomial can satisfy conditions of the Theorem 2.6. and it can also be the strong complete polynomial as well as $f^{(4)}(x), f^{(5)}(x), \dots$

Open problem: Extend the above results for $f^{(t)}$ for $t > 2$ and \mathcal{K} -complete mappings.

3. COMPLETE MAPPING OVER MULTIPLICATIVE GROUP OF THE FINITE FIELD

Let ψ be a generator of the multiplicative group (\mathbb{F}_q^*, \cdot) of the finite field \mathbb{F}_q .

Let $\phi: \mathbb{Z}_{q-1} \rightarrow \mathbb{Z}_{q-1}$ be a complete mapping where \mathbb{Z}_{q-1} is the additive group. Then the mapping $f: \mathbb{F}_q \rightarrow \mathbb{F}_q$ defined by

$$f(\psi^z) = \psi^{\phi(z)}, \quad f(0) = 0$$

is a permutation of the \mathbb{F}_q such that for $x = \psi^z$,

$$xf(x) = \psi^{z+\phi(z)}$$

and $0f(0) = 0$. Therefore, $xf(x)$ is also a permutation over \mathbb{F}_q .

Therefore, we can define $f: \mathbb{F}_q \rightarrow \mathbb{F}_q$ as a **multiplicative complete mapping** if both $f(x)$ and $xf(x)$ are permutations of \mathbb{F}_q . The polynomial induced by the multiplicative complete mapping will be called a multiplicative complete polynomial.

Assume that $f(x)$ and $xf(x)$ are both permutations over \mathbb{F}_q . If $f(a) = 0$ then $af(a) = 0 = 0f(0)$. According to the fact that $xf(x)$ is the injection it follows $a = 0$. Therefore, if $f(x)$ is the multiplicative complete mapping then $f(0) = 0$.

Example 3.1. Let $q = 2^3 = 8$ and thus $q-1 = 7$. Then for $f_i(x) = cx^i$, $i = 1, 2, \dots, 5$, $c \in \mathbb{F}_8^*$ all mappings $f_i(x)$ are multiplicative complete mappings because both $f_i(x) = cx^i$ and $xf_i(x) = cx^{i+1}$ are permutation polynomials since $\gcd(i, 7) = \gcd(i+1, 7) = 1$ for all $i = 1, 2, \dots, 5$.

Theorem 3.1. Assume that $f(x)$ is a multiplicative complete polynomial over \mathbb{F}_q . Then the following polynomials are also multiplicative complete:

- (a) $bf(ax)$ where $a, b \in \mathbb{F}_q^*$.
- (b) $f^{(-1)}(x)$.

Proof.

- (a) Clearly, $bf(ax)$ is a permutation polynomial. As $xf(x)$ is a permutation polynomial we have that $ba^{-1}(ax)f(ax)$ is a permutation polynomial and it follows that $xbf(ax)$ is also a permutation polynomial. Thus, $bf(ax)$ is a multiplicative complete polynomial.
- (b) We have that $f^{(-1)}(x)$ is a permutation polynomial. Since $yf(y)$ is a permutation polynomial, using a substitution $y = f^{(-1)}(x)$ we obtain that $f^{(-1)}(x)x$ is a permutation polynomial. \square

In [8] it was shown that complete polynomials over finite fields are of the degree $\leq q - 3$. For the multiplicative complete polynomials over finite fields we have the same degree bound.

Theorem 3.2. *Let $f(x)$ be a multiplicative complete polynomial over \mathbb{F}_q . Then its reduced degree is $\leq q - 3$.*

Proof. It is known that the permutation polynomials over finite fields are of the degree $< q - 1$. But then $\deg(xf(x)) = 1 + \deg(f(x)) < q - 1$ and thus $\deg(f(x)) < q - 2$. \square

This bound cannot be improved since in \mathbb{F}_8 , $f(x) = x^5$ is multiplicative complete polynomial.

It is well known that there are permutation polynomials over finite fields of the form $x^r\Psi(x)$ where $\gcd(r, q - 1) = 1$ (see [7], pages 221-223). If both $\gcd(r, q - 1) = 1$ and $\gcd(r + 1, q - 1) = 1$ then we obtain multiplicative complete mappings of this form. If q is odd then $2|q - 1$ and 2 divides one of the numbers r or $r + 1$ and condition $\gcd(r, q - 1) = 1$ and $\gcd(r + 1, q - 1) = 1$ can not be satisfied. Therefore, we can consider permutation polynomials of this form only for the fields of characteristic $p = 2$.

Analogously, we can define the multiplicative strong complete mapping over finite field and its induced polynomial. We say that a polynomial $f(x)$ is a **multiplicative strong complete** polynomial if all $f(x)$, $xf(x)$ and $x^{q-2}f(x)$ ($= x^{-1}f(x)$) are permutation polynomials over \mathbb{F}_q .

If $\theta : \mathbb{Z}_{q-1} \rightarrow \mathbb{Z}_{q-1}$ is a strong complete mapping and ψ a generator of the multiplicative group \mathbb{F}_q^* then a mapping $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ defined by

$$f(\psi^z) = \psi^{\theta(z)} \quad \text{and} \quad f(0) = 0$$

is multiplicatively strong complete.

Every strong complete mapping $f(x)$ is also a complete mapping. Thus, we have that $f(0) = 0$ and $\deg f(x) \leq q - 3$. It is evident that this bound cannot be reduced since $f(x) = x^5$ is a multiplicative strong complete over \mathbb{F}_8 . Also, $\deg(f(x)) \geq 2$. From the theory of Knut Vic designs (see [2]) it follows that if there is a strong complete mapping on \mathbb{F}_q^* then $\gcd(6, q - 1) = 1$ and thus multiplicative strong complete mappings can be defined over the fields of characteristic $p = 2$ where $3 \nmid q - 1$.

A permutation polynomial of the form $x^r\Psi(x)$ where $\gcd(r, q-1) = 1$ is a multiplicative strong complete if it holds $\gcd(r-1, q-1) = \gcd(r+1, q-1) = 1$.

Theorem 3.3. *Assume that $f(x)$ is a multiplicative strong complete polynomial over \mathbb{F}_q . Then the following polynomials have the same property:*

- (a) $bf(ax)$ where $a, b \in \mathbb{F}_q^*$.
- (b) $f^{(-1)}(x)$

Proof.

- (a) We showed that $bf(ax)$ and $xbf(ax)$ are permutation polynomials. Since $ba(ax)^{-1}f(ax)$ is a permutation polynomial it follows that $x^{-1}bf(ax)$ is also the permutation polynomial. Thus, $bf(ax)$ is a multiplicative strong complete polynomial.
- (b) We showed that $f^{(-1)}(x)$ and $xf^{(-1)}(x)$ are permutation polynomials. As $y^{-1}f(y)$ is a permutation polynomial, while using the substitution $y = f^{(-1)}(x)$, we obtain that $(f^{(-1)}(x))^{-1}x$ is a permutation polynomial. But then $[(f^{(-1)}(x))^{-1}x]^{-1} = x^{-1}f^{(-1)}(x)$ is also a permutation polynomial. \square

The theory of complete and strong complete mappings over the cyclic group of order $q-1$ where $q = p^n$ (where $p = 2$ and $3 \nmid q-1$ for the strong complete mappings) can be improved by finding some new classes of multiplicative complete and multiplicative strong complete polynomials over finite fields and this topic deserves further research.

Open problem: Find new classes of multiplicative complete and multiplicative strong complete polynomials over finite fields.

Results in this article were partially presented on the Carleton Finite Fields Workshop, May 21-24, 2019.

REFERENCES

- [1] Wun-Seng Chou, *PhD Thesis*, Penn State University, 1990.
- [2] Anthony B. Evans, *The existence of strong complete mappings of finite groups: A survey*, Discrete mathematics, Volume 313, Issue 11, 6 June 2013, Pages 1191-1196.
- [3] Amela Muratović-Ribić, Enes Pašalić, *A note on complete polynomials over finite fields and their applications in cryptography*, Finite Fields and Their Applications, Volume 25, 1/1/2014, Pages 306-316.
- [4] Amela Muratović-Ribić, Alexander Pott, David Thomson, Qiang Wang, *On the characterization of a semi-multiplicative analogue of planar functions over finite fields*, Topics in Finite Fields, Volume 632, 2015/1/29, Page 317.
- [5] Arne Winterhof, *Generalizations of complete mappings of finite fields and some applications*, Journal of Symbolic Computation, Volume 64, August 2014, Pages 42-52.
- [6] Leonid A. Bassalygo, Victor A. Zinoviev, *Permutation and complete permutation polynomials*, Finite Fields and their Applications, Volume 33, 2015, Pages 198-211.
- [7] Gary L. Mullen, Daniel Panario, *Handbook on the Finite Fields and Their Applications*, Taylor & Francis Group, LLC, 2013.

- [8] Harald Niederreiter and Karl H. Robinson, *Complete mappings of finite fields*, Austral Math. Soc. , (Series A) Volume 33, 1982, Pages 197-212.
- [9] Rasha Schaheen, Arne Witerhof, *Permutations of finite fields for check digit systems*, Designs, Codes and Cryptography , Volume 57, 2010, Pages 361-371.
- [10] Wu Gao Fei, Li Nian, Helleseth Tor, Zhang Yu Qiang, *Some classes of complete permutation polynomials over \mathbb{F}_q* , Science China, Mathematics, Volume 58, No. 10, October 2015, Pages 2081-2014.
- [11] Gaofei Wu, Nian Li, Tor Helleseth, Yuqing Zhang, *Some classes of monomial complete permutation polynomials over finite fields of characteristic two*, Finite Fields Appl., Volume 28, 2014, Pages 148-165.

(Received: July 12, 2019)

(Revised: November 13, 2019)

Amela Muratović-Ribić
Department of Mathematics
Faculty of Natural Sciences and Mathematics
University of Sarajevo
Zmaja od Bosne 35, 71000 Sarajevo, BA
e-mail: amuratovicribic@gmail.com
e-mail: amela@pmf.unsa.ba
and
Shaip Surdulli
Selo Donje Karačevo
62000 Kosovska Kamenica
Kosovo
e-mail: shaipsurdulli@yahoo.com