

On generalized strong complete mappings and mutually orthogonal Latin squares*

Amela Muratović-Ribić[†] 

University of Sarajevo, Faculty of Science,
Zmaja od Bosne 33-35, Sarajevo, Bosnia and Herzegovina

Received 20 July 2020, accepted 1 April 2021, published online 2 November 2021

Abstract

We present an application of generalized strong complete mappings to construction of a family of mutually orthogonal Latin squares. We also determine a cycle structure of such mapping which form a complete family of MOLS. Many constructions of generalized strong complete mappings over an extension of finite field are provided.

Keywords: Strong complete mapping, group, finite field, mutually orthogonal Latin squares (MOLS).

Math. Subj. Class. (2020): 11T06, 12Y05

1 Introduction

Let G be an additive group. A mapping $\theta : G \rightarrow G$ is called a complete mapping if both $\theta(x)$ and $\theta(x) + x$ are 1-to-1 and onto. If both $\theta(x)$ and $\theta(x) - x$ are 1-to-1 and onto, $\theta(x)$ is called an orthomorphism. A strong complete mapping is a complete mapping which is also an orthomorphism. These mappings are used for a construction of Knut Vic designs and they exist only for the groups of order n where $\gcd(n, 6) = 1$. An Abelian group admits strong complete mappings if and only if its Sylow 2-subgroup is trivial or noncyclic, and also, its Sylow 3-group is trivial or noncyclic (see [2]).

Let p be a prime, m be a positive integer and $q = p^m$. Let \mathbb{F}_q be a finite field of order q . We consider complete and strong complete mappings (and orthomorphisms) over $(\mathbb{F}_q(x), +)$. Polynomials induced by these mappings are called complete and strong complete polynomials, respectively. In [1], strong complete mappings over finite fields are called very complete mappings. Many results have been established on this topic. In the

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

[†]The author gratefully thanks the anonymous referee for the constructive comments and recommendations which definitely helped to improve the quality of the paper.

E-mail address: amela@pmf.unsa.ba (Amela Muratović-Ribić)

sequel, $f^0(x) = x, f^2(x) = f \circ f(x), f^k(x) = f \circ f^{k-1}(x)$ for $k > 0$. Generalized complete polynomials were introduced in [6] with applications to the check digit systems. There were considered polynomials over finite fields with a property that $f(x), f(x) \pm x$ and $f^2(x) \pm x$ are all permutation polynomials. Note that there exist monomials of the form $x^{\ell \frac{q-1}{m}}$ where $m \mid q - 1$ with this property (see [5]).

We turn our attention to mappings $\theta(x)$ such that $\theta^k(x)$ are strong complete mappings for all $k = 1, 2, \dots, t$. Here, t is a positive integer. Our point of interest is an application of these mappings to construction of mutually orthogonal Latin squares (MOLS). Many constructions of such mappings over finite fields will be presented.

2 Construction of MOLS

Theorem 2.1. *Let G be an additive finite Abelian group of order n , where n is odd. Assume that $\theta : G \rightarrow G$ is such that $\theta^k(x)$ are strong complete mappings for $k = 1, 2, \dots, t$ where t is a positive integer. For $1 \leq k \leq t$ and $i, j \in G$ define*

$$\begin{aligned} a_{i,j}^k &= i + \theta^k(j) \\ a_{i,j}^{-k} &= i - \theta^k(j) \\ a_{i,j}^{0^+} &= i + j; \quad a_{i,j}^{0^-} = i - j. \end{aligned}$$

A family of Latin squares $L_k = (a_{i,j}^k)$ where $k = -t, \dots, -1, 0^-, 0^+, 1 \dots t$ is a family of pairwise mutually orthogonal Latin squares. Therefore, a family of $2(t + 1)$ MOLS is obtained.

Proof. We use the following convention $\theta^{0^\pm}(x) = x$. Assume $(a_{i,j}^k, a_{i,j}^s) = (a_{u,v}^k, a_{u,v}^s)$ for $k \neq s$ and consider the following cases:

- If $(0 < s < k)$ or $(s = 0^+$ and $0 < k)$ we have that

$$i + \theta^k(j) = u + \theta^k(v) \tag{2.1}$$

and

$$i + \theta^s(j) = u + \theta^s(v).$$

Subtracting these equalities we obtain

$$\theta^k(j) - \theta^s(j) = \theta^k(v) - \theta^s(v).$$

Thus

$$\theta^{k-s}(\theta^s(j)) - \theta^s(j) = \theta^{k-s}(\theta^s(v)) - \theta^s(v).$$

By assumption, $\theta^{k-s}(y) - y$ is a permutation. Hence, $\theta^s(j) = \theta^s(v)$ and $j = v$. Inserting this in (2.1) we obtain $i = u$.

- If $(k < s < 0)$ or $(k < 0$ and $s = 0^-)$ then we have

$$i - \theta^{|k|}(j) = u - \theta^{|k|}(v) \tag{2.2}$$

and

$$i - \theta^{|s|}(j) = u - \theta^{|s|}(v).$$

Subtracting these equalities, we obtain

$$\theta^{|k|}(j) - \theta^{|s|}(j) = \theta^{|k|}(v) - \theta^{|s|}(v).$$

Thus

$$\theta^{|k|-|s|}(\theta^{|s|}(j)) - \theta^{|s|}(j) = \theta^{|k|-|s|}(\theta^{|s|}(v)) - \theta^{|s|}(v).$$

Reasoning as above, we get $j = v$ and $i = u$.

- If $(-s < 0 < k)$, ($s = 0^-$ and $k > 0$) or ($s < 0$ and $k = 0^+$) then we have that

$$i + \theta^k(j) = u + \theta^k(v) \tag{2.3}$$

and

$$i - \theta^{|s|}(j) = u - \theta^{|s|}(v)$$

which implies

$$\theta^k(j) + \theta^{|s|}(j) = \theta^k(v) + \theta^{|s|}(v).$$

Assume first $k > |s|$. Then $\theta^{k-|s|}(\theta^{|s|}(j)) + \theta^{|s|}(j) = \theta^{k-|s|}(\theta^{|s|}(v)) + \theta^{|s|}(v)$. As $\theta^{k-|s|}(y) + y$ is a permutation, it follows that $\theta^{|s|}(j) = \theta^{|s|}(v)$. Thus $j = v$. Using this in (2.3), we obtain $i = u$. If $k \leq |s|$ then $\theta^{|s|-k}(\theta^k(j)) + \theta^k(j) = \theta^{|s|-k}(\theta^k(v)) + \theta^k(v)$ similarly implies $j = v$ and $i = u$.

- If $k = 0^+$ and $s = 0^-$ then $i + j = u + v$ and $i - j = u - v$ which implies $2i = 2u$. Then $2ki = 2ku$ for all integers k . By assumption, the order of the group G is an odd integer. Then $n + 1$ is even and thus $(n + 1)i = (n + 1)u$. However, $ni = nu$ by Lagrange's theorem. Hence, $i = u$ and further $j = v$.

□

Lemma 2.2. *Let G be a group of order n . Assume that $\theta : G \rightarrow G$ is such that all $\theta^k(x)$ are strong complete mappings for $k = 1, 2, \dots, t$. Then the permutation θ has exactly one fixed element and lengths of all other cycles are greater than t .*

Proof. Assume that ℓ is the length of a cycle $(a_1, a_2, \dots, a_\ell)$ of the permutation θ , where $1 < \ell \leq t$. Then $\theta^\ell(a_1) = a_1$ and $\theta^\ell(a_2) = a_2$. Therefore $\theta^\ell(a_1) - a_1 = \theta^\ell(a_2) - a_2 = 0$. It follows that $\theta^\ell(x) - x$ is not a permutation which is a contradiction. Therefore, there is no cycle of the length $1 < \ell \leq t$. Since $\theta(x) - x$ is a permutation, there is exactly one solution of the equation $\theta(x) - x = 0$ and thus exactly one fixed element of θ . □

Theorem 2.3. *If θ generates a complete set of MOLS over a finite Abelian group of order n as in the Theorem 2.1, then θ has either one fixed element and one cycle of the length $n - 1$ or one fixed element and two cycles of the length $\frac{n-1}{2}$.*

Proof. In this case all $\theta^k(x)$ are strong complete mappings for $k = 1, 2, \dots, \frac{n-1}{2} - 1$. By the Lemma 2.2, there is one fixed element in the permutation θ and the lengths of nontrivial cycles are greater than $\frac{n-1}{2} - 1$. It follows that there can either one such cycle with the length $n - 1$ or two cycles of the length $\frac{n-1}{2}$. □

Remark 2.4. Let \mathbb{Z}_p be a field of order p , where $p > 2$ is a prime. Let d be a generator of \mathbb{Z}_p^* . Then $\theta^k(s) = d^k s$ is a strong complete mapping for $k = 1, 2, \dots, \frac{p-3}{2}$. The mapping $\theta(s)$ has a fixed element $s = 0$ and one full cycle $(1, d, d^2, \dots, d^{p-2})$ of the length $p - 1$. On the other hand, $\theta^2(s) = d^2 s$ has a property that $\theta^{2k}(s) = d^{2k} s$ is also a strong complete mapping for all $k = 1, 2, \dots, \frac{p-3}{2}$ since $\frac{p-1}{2}$ is odd. This mapping has a fixed element $s = 0$ and two cycles of the length $\frac{p-1}{2}$.

Proposition 2.5. Assume that $\Psi : G \rightarrow G$, is a permutation such that $\Psi(x \pm y) = \Psi(x) \pm \Psi(y)$ for all $x, y \in G$. If $\theta(x)$ generates a complete set of MOLS as in Theorem 2.1, then $\eta(x) = \Psi \circ \theta \circ \Psi^{-1}(x)$ also generates a complete set of MOLS.

Note: An example of the mapping is $\Psi(x) = kx$ where k is an integer, which prove its existence.

Proof. Since $\eta^k(x) = \Psi \circ \theta^k \circ \Psi^{-1}(x)$ is a permutation we need to show that $\eta^k(x) + x$ and $\eta^k(x) - x$ are permutations for all $k = 1, 2, \dots, \frac{|G|-1}{2}$. Using substitution $y = \psi^{-1}(x)$ we get

$$\eta^k(x) \pm x = \Psi[\theta^k(\Psi^{-1}(x))] \pm \Psi(\Psi^{-1}(x)) = \Psi[\theta^k(\Psi^{-1}(x)) \pm \Psi^{-1}(x)] = \Psi(\theta^k(y) \pm y).$$

This is a permutation since $\Psi(x)$ and $\theta^k(x) \pm x$ are permutations. Therefore, $\eta(x)$ generates a complete set of MOLS. □

Let \mathbb{F}_q be a field with a prime subfield \mathbb{Z}_p . Linearized polynomials over \mathbb{F}_q are of the form $L(x) = \sum_{k=0}^m a_k x^{p^k}$ and these polynomials have property that $L(ax) = aL(x)$ for all $a \in \mathbb{Z}_p$ and $L(x + y) = L(x) + L(y)$ for all $x, y \in \mathbb{F}_q$. Thus, if we consider \mathbb{F}_q as a vector space over \mathbb{Z}_p , then $L(x)$ is a linear operator on \mathbb{F}_q .

Corollary 2.6. Let \mathbb{F}_q be a finite field of order $q = p^n$ where p is a prime. Let d be a primitive element of \mathbb{F}_q and $L(x)$ be a linearized permutation polynomial of \mathbb{F}_q . Then the polynomial $f(x) = L(dL^{-1}(x))$ generates a complete set of MOLS as in Theorem 2.1.

Proof. It is easy to see that sx is strong complete polynomial for $s \in \mathbb{F}_q \setminus \{0, \pm 1\}$. Therefore, for $g(x) = dx$, $g^k(x) = d^kx$ are strong complete mappings for all $k \neq \frac{q-1}{2}, q-1$. Since, $L(x \pm y) = L(x) \pm L(y)$ we have that $f(x) = L \circ g \circ L^{-1}(x) = L(dL^{-1}(x))$ generates a complete set of MOLS as in Theorem 2.1. □

Remark 2.7. Consider a family of strong complete polynomials over finite field \mathbb{F}_q which generate a complete set of MOLS as in Theorem 2.1 and which have one fixed element and one cycle of the length $q - 1$. Let d be a generator of \mathbb{F}_q^* . Then $f(x) = dx$ is in this family and considering the cycle structure, all other polynomials are conjugate with $f(x)$. Therefore, all polynomials in this family are of the form $\Psi(d\Psi^{-1}(x))$ for some permutation polynomial $\Psi(x)$ over \mathbb{F}_q .

If $\frac{q-1}{2}$ is odd, then $g(x) = d^2x$ is a strong polynomial which generate a complete family of MOLS as in Theorem 2.1 and which have one fixed element and two cycles of the length $\frac{q-1}{2}$. Similarly, all other strong complete mappings with a same cycle structure induce a polynomial of the form $\Psi(d^2\Psi^{-1}(x))$ for some permutation polynomial $\Psi(x)$ over \mathbb{F}_q .

3 Construction of the strong complete mappings over extension fields

Let n be a positive integer and \mathbb{F}_{q^n} be an extension field of \mathbb{F}_q . Let $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be a basis of the vector space \mathbb{F}_{q^n} over \mathbb{F}_q . We shall use similar technique as in the proof of Theorem 2.1 in [3] to obtain the following recursive constructions of many strong complete polynomials over the extension field.

Theorem 3.1. *Let $f_i(x)$ be strong complete polynomials over \mathbb{F}_q for $i = 1, 2, \dots, n$. Let $\psi_i : \mathbb{F}_q^i \rightarrow \mathbb{F}_q$ be arbitrary functions for $i = 1, 2, \dots, n - 1$. Denote $X = x_1\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n$. Then the function*

$$F(X) = f_1(x_1)\alpha_1 + [f_2(x_2) + \psi_1(x_1)]\alpha_2 + \dots + [f_n(x) + \psi_{n-1}(x_1, x_2, \dots, x_{n-1})]\alpha_n$$

is a strong complete polynomial over \mathbb{F}_{q^n} .

Proof. In the proof of Theorem 1 in [3], it was shown that $F(X)$ is a complete polynomial. To show that it is a strong complete polynomial, let's check that $F(X) - X$ is $1 - to - 1$. Assume that $F(X) - X = F(Y) - Y$ for $X = x_1\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n$ and $Y = y_1\alpha_1 + y_2\alpha_2 + \dots + y_n\alpha_n$. Then the coefficients with the basis elements on the two sides of equation are identical.

Looking at the coefficient with α_1 we see that $f_1(x_1) - x_1 = f_1(y_1) - y_1$. As $f_1(x)$ is orthomorphism it follows that $x_1 = y_1$.

Now, equating the coefficients with α_2 we get $f_2(x_2) + \psi_1(x_1) - x_2 = f_2(y_2) + \psi_1(y_1) - y_2$. Taking into account $x_1 = y_1$, this implies $f_2(x_2) - x_2 = f_2(y_2) - y_2$. Hence, $x_2 = y_2$ since $f_2(x)$ is an orthomorphism. We proceed by induction. Assume that $x_1 = y_1, x_2 = y_2, \dots, x_{i-1} = y_{i-1}$ which imply $\psi_{i-1}(x_1, x_2, \dots, x_{i-1}) = \psi_{i-1}(y_1, y_2, \dots, y_{i-1})$. Comparing the coefficients with α_i , we obtain

$$f_i(x_i) + \psi_{i-1}(x_1, x_2, \dots, x_{i-1}) - x_i = f_i(y_i) + \psi_{i-1}(y_1, y_2, \dots, y_{i-1}) - y_i.$$

Thus $f_i(x_i) - x_i = f_i(y_i) - y_i$. So, $x_i = y_i$ since $f_i(x)$ is an orthomorphism. Therefore, $x_i = y_i$ for all $i = 1, 2, \dots, n$ and $X = Y$. Now, $F(X) - X$ being $1 - to - 1$ on the finite set \mathbb{F}_{q^n} it is a bijection, i.e. a permutation. \square

In the case of linearized polynomials, we extend the same technique to the compositions of mappings. The proofs of the next theorems are similar to the proof of the Theorem 3.1. So, we may omit a number of details.

Theorem 3.2. *Let $f_i(x)$, $i = 1, 2, \dots, n$, be linearized strong complete polynomials over \mathbb{F}_q such that $f_i^k(x)$ are also strong complete polynomials for $k = 1, 2, \dots, t$. Let $\psi_i : \mathbb{F}_q^i \rightarrow \mathbb{F}_q$ be arbitrary functions for $i = 1, 2, \dots, n - 1$. Denote $X = x_1\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n$. Then function*

$$F(X) = f_1(x_1)\alpha_1 + [f_2(x_2) + \psi_1(x_1)]\alpha_2 + \dots + [f_n(x) + \psi_{n-1}(x_1, x_2, \dots, x_{n-1})]\alpha_n$$

is a strong complete polynomial over \mathbb{F}_{q^n} such that $F^{(k)}(X)$ are also strong complete mappings for all $k = 2, 3, \dots, t$.

Proof. By Theorem 3.1, $F(X)$ is a strong complete polynomial. Since $F(X)$ is permutation, it follows that $F^{(k)}(X)$ are permutations for all $k = 2, \dots, t$. Assume now that $F^{(2)}(X) + X = F^{(2)}(Y) + Y$ (or $F^{(2)}(X) - X = F^{(2)}(Y) - Y$).

Equating the coefficients with α_1 on the both sides, we get $f_1^{(2)}(x_1) + x_1 = f_1^{(2)}(y_1) + y_1$ (or $f_1^{(2)}(x_1) - x_1 = f_1^{(2)}(y_1) - y_1$). This implies $x_1 = y_1$ because $f_1^{(2)}(x)$ is a strong complete polynomial. With α_2 we have

$$f_2[f_2(x_2) + \psi_1(x_1)] + \psi_1(f_1(x_1)) \pm x_2 = f_2[f_2(y_2) + \psi_1(y_1)] + \psi_1(f_1(y_1)) \pm y_2.$$

Since f_2 is linearized, we obtain

$$f_2(f_2(x_2)) + f_2(\psi_1(x_1)) + \psi_1(f_1(x_1)) \pm x_2 = f_2(f_2(y_2)) + f_2(\psi_1(y_1)) + \psi_1(f_1(y_1)) \pm y_2.$$

Taking into account that $x_1 = y_1$, we get $f_2(f_2(x_2)) \pm x_2 = f_2(f_2(y_2)) \pm y_2$. This yields $x_2 = y_2$ since $f_2^{(2)}(x_2)$ is a strong complete polynomial. Proceeding by induction, we can prove that $x_3 = y_3, \dots, x_n = y_n$ and thus $X = Y$. Therefore, $F^{(2)}(X)$ is strong complete. We can also prove by induction that $F^{(k)}(X)$ are strong complete for all $k = 2, 3, \dots, t$. \square

Proposition 3.3. *Assume that $f(x)$ is a permutation and that $f(dx) + f(x), f(dx) - f(x)$ are also permutations where $d \in \mathbb{F}_q, d \neq 0, d \neq \pm 1$. Then the polynomial $g_d(x) = f(df^{-1}(x))$ is strong complete.*

Proof. Assume that $f(x), f(dx) + f(x)$ and $f(dx) - f(x)$ are permutations. Let $x = f^{-1}(y)$. Then $f(df^{-1}(y)), f(df^{-1}(y)) + y$ and $f(df^{-1}(y)) - y$ are permutations. Therefore, $g_d(x) = f(df^{-1}(x))$ is a strong complete polynomial. \square

Note that $g_d^{(2)}(x) = g_d(f(df^{-1}(x))) = f(df^{-1}(f(df^{-1}(x)))) = f(d^2 f^{-1}(x)) = g_{d^2}(x)$ and, by induction $g_d^{(k)}(x) = g_{d^k}(x)$.

A permutation polynomial $f(x)$ such that $f(dx) - f(x)$ is also a permutation for all $d \in \mathbb{F}_q, d \neq 1$, is called a Costas polynomial. The only Costas polynomial over a field of the prime order p is x^s where $\gcd(s, p - 1) = 1$. The only known Costas polynomial over \mathbb{F}_q is $L(x^s)$ where $\gcd(s, q - 1) = 1$ and L is a linearized permutation polynomial (see [4]). The polynomial $L(x^s)$ satisfies the conditions of Proposition 2.5. Indeed, $L(dx^s) \pm L(x^s) = L((d \pm 1)x^s)$ is permutation polynomial whenever $d \pm 1 \neq 0$ and $d \neq 0$. Thus, $g_d(x) = L(d^s L^{-1}(x))$ is strong complete polynomial for all $d^s \notin \{0, 1, -1\}$. Then, $g_d^{(k)}(x) = g_{d^k}(x)$ is the strong complete polynomial whenever $d^{ks} \notin \{0, 1, -1\}$. If $d^{sk_1} + d^{sk_2} + \dots + d^{sk_t} \notin \{0, 1, -1\}$ for a set of positive integers $\mathcal{K} = \{k_1, k_2, \dots, k_t\}$ then

$$\sum_{i=1}^t g_d^{k_i}(x) \pm x = \sum_{i=1}^t L(d^{sk_i} L^{-1}(x)) \pm x = L\left(\left(\sum_{i=1}^t d^{sk_i}\right) L^{-1}(x)\right) \pm x$$

is also a permutation. It follows that $g_d(x)$ is the \mathcal{K} -strong complete mapping (see [6]). This class of \mathcal{K} -strong complete polynomials is linearized. Now, we will present one more construction of the nonlinearized generalized strong complete polynomials over extension fields.

Theorem 3.4. *Let $f_i(x)$ be permutation polynomials over \mathbb{F}_q such that $f_i(d^k x) \pm f_i(x)$ are permutation polynomials for $d \in \mathbb{F}_q^*, k = 1, 2, \dots, t < q - 1$ and $i = 1, 2, \dots, n$. Let $\psi_i : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q$ be arbitrary functions for $i = 1, 2, \dots, n - 1$. Denote $X = x_1\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n$. Then the mapping*

$$F(X) = f_1(x_1)\alpha_1 + [f_2(x_2) + \psi_1(x_1)]\alpha_2 + \dots + [f_n(x) + \psi_{n-1}(x_1, x_2, \dots, x_{n-1})]\alpha_n$$

is a permutation polynomial such that $F(d^k X) \pm F(X)$ are permutation polynomials for all $k = 1, 2, \dots, t$.

Note: For functions $f_i(x)$ we can take $L(x^s)$ as discussed above.

Proof. As $d^k \in \mathbb{F}_q^*$ we have that $d^k X = d^k x_1 \alpha_1 + d^k x_2 \alpha_2 + \dots + d^k x_n \alpha_n$. Assume $F(d^k X) \pm F(X) = F(d^k Y) \pm F(Y)$. Then, equating the coefficients with the basis elements, we get $f_1(d^k x_1) \pm f_1(x_1) = f_1(d^k y_1) \pm f_1(y_1)$. Thus $x_1 = y_1$. Further, $f_2(d^k x_2) + \psi_1(d^k x_1) \pm (f_2(x_2) + \psi_1(x_1)) = f_2(d^k y_2) + \psi_1(d^k y_1) \pm (f_2(y_2) + \psi_1(y_1))$. Since $x_1 = y_1$, we have $f_2(d^k x_2) \pm f_2(x_2) = f_2(d^k y_2) \pm f_2(y_2)$. It follows that $x_2 = y_2$. By induction, $x_3 = y_3, \dots, x_n = y_n$. Hence, $X = Y$. Therefore, $F(d^k X) \pm F(X)$ are permutations for all $k = 1, 2, \dots, t$. \square

Corollary 3.5. For a function $F(X)$ defined in Theorem 3.4, the function $G_d(X) = F(dF^{-1}(X))$ is strong complete mapping with a property that $G_d^{(k)}(X)$ are strong complete mappings for all $d = 1, 2, \dots, t$.

Proof. The result follows from Proposition 3.3 and $G_d^{(k)}(X) = G_{d^k}(X)$. \square

Note: If we put $x_1 = x_2 = \dots = x_{n-1} = 0$ and $x_n = 1$, then in all constructions presented in Section 3 we will form a cycle whose elements are of the form $(0, 0, \dots, 0, s)$. The length of this cycle is less or equals to q . Using Lemma 2.2, we obtain $t < q$. Therefore, by means of Theorem 2.1 we can not obtain more than $2q$ of MOLS over \mathbb{F}_{q^n} using constructions in the Section 3.

ORCID iDs

Amela Muratović-Ribić  <https://orcid.org/0000-0001-7903-4884>

References

- [1] W.-S. Chou, *Permutation polynomials on finite fields and their combinatorial applications*, Ph.D. thesis, Penn State Universit, 1990, <https://www.proquest.com/openview/24d2ca00f8f48ffe88a97a7c431a2096/1?pq-origsite=gscholar&cbl=18750&diss=y>.
- [2] A. B. Evans, The existence of strong complete mappings of finite groups: a survey, *Discrete Math.* **313** (2013), 1191–1196, doi:10.1016/j.disc.2011.11.040.
- [3] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in cryptography, *Finite Fields Appl.* **25** (2014), 306–315, doi:10.1016/j.ffa.2013.10.008.
- [4] A. Muratović-Ribić, A. Pott, D. Thomson and Q. Wang, On the characterization of a semi-multiplicative analogue of planar functions over finite fields, in: *Topics in finite fields*, Amer. Math. Soc., Providence, RI, volume 632 of *Contemp. Math.*, pp. 317–325, 2015, doi:10.1090/conm/632/12635.
- [5] A. Muratović-Ribić and S. Surdulli, On strong complete monomials and its multiplicative analogue over finite fields, *Sarajevo J. Math.* **16(29)** (2020), 137–144, doi:10.5644/sjm.
- [6] A. Winterhof, Generalizations of complete mappings of finite fields and some applications, *J. Symbolic Comput.* **64** (2014), 42–52, doi:10.1016/j.jsc.2013.12.006.