IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 17, Issue 1 Ser. II (Jan. – Feb. 2021), PP 22-30
www.iosrjournals.org

New Classes of Strong Complete Permutation Polynomial

*SHAIP SURDULLI

Abstract. *We are introducing a new strong complete permutation polynomial with AGW criterion. These polynomials, as well as other similar polynomials, are being applied in cryptography, theory of codes, combinatorial design, and especially for Knut Vik design and solution of the n queens problem. For the construction of such polynomials, we have used the existing complete permutation polynomial and we have added additional conditions so that we have received strong complete permutation polynomial.*

Date of Submission: 18-01-2021 Date of Acceptance: 03-02-2021

I. Introduction

Let p be a prime number, let m be a positive integer and $q = p^m$. Suppose $\mathbb{F}_q$ is finite field of order q. Polynomial $f(x)$ in $\mathbb{F}_q[x]$ is called| permutation polynomial (PP) in $\mathbb{F}_q$ if it is induced with mapping $\mapsto \theta(c)$ from $\mathbb{F}_q$ in $\mathbb{F}_q$, which is permutation from $\mathbb{F}_q$, that is bijective function. Permutation polynomial $f(x)$ is called complete polynomial (CP) from $\mathbb{F}_q$ if $f(x) + x$ is a permutation polynomial. Permutation polynomial $f(x)$ is called orthomorphism from $\mathbb{F}_q$ if $f(x) - x$ is permutation polynomial. Suppose $q = p^n$, where $n \geq 1$ and p is odd prime number. Suppose $\mathbb{F}_q$ is finite field of order q. Permutation polynomial $f(x)$ is called **Strong Complete Polynomial** (SCP) over over $\mathbb{F}_q$ if $f(x) + x$ and $f(x) - x$ are permutation polynomials from $\mathbb{F}_q$. These polynomials are induced by strong complete mapping at additive group $(\mathbb{F}_q, +)$.

The number of strong complete polynomials from $\mathbb{F}_q$ is smaller than the number of permutation polynomials, complete permutation polynomials and the number of orthomorphism because strong complete polynomial does not exist when q is an even number and divisive with 3 and because of several conditions due to which some polynomial is strong complete polynomial.

More details regarding permutation polynomials, complete permutation polynomials and strong permutation polynomials over finite field are available in [1], [3], [6], [7], [8] [16], [21], [22], [23], [24], [26], [27], [29] [30],[31], [32].

n queen problem is the placement of n queens on chessboard of dimensions $n \times n$, or at torus so that queens cannot be attacked, or that maximum one queen is placed in every row, column and diagonal. This problem is generalization of the 8 queens problem that was set by M.Bezzel in 1848, but the problem continues to be solved even today.

Standard (simple) n queens problems is the placement of n queen on chessboard, in format $n \times n$, so that neither pair of queens is mutually attacked, that is, they do not belong to the same row, column and diagonal. (Picture 1).

Key words and phrases. Finite field, permutation polynomial, complete permutation polynomial, strong complete permutation polynomial, AGW criterion, problem of n queens.

**Shaip Surdulli, Doctor of Philosophy in Mathematical Sciences. Faculty of Science and Mathematics, University of Pristina, Republic of Kosovo. Email: shaipsurdulli@yahoo.com.*

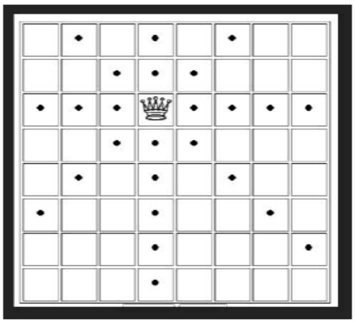

Figure 1. Standard n queen problem

Modular n queen problem is placement of n queen on modular board of dimension $n \times n$, that is, modular table or torus (specifically, the surface in three-dimensional space that is obtained by joining two opposite edges of the square of dimensions $n \times n$), so that two queens at torus $n \times n$ do not belong to the same row, column and diagonal.

More information concerning the n queen problem is available in [5], [12], [14], etc.

STRONG COMPLETE

With strong complete polynomials in the finite field $\mathbb{F}_q$ can be solved modular n queen problem, where $n = q = p^m$, m is a natural number, p is a prime odd number and $NZD(n, 6) = 1$, where NZD is the greatest common divisor. Likewise, with strong complete polynomials, Knut Vik design can be created (see [10], [11]).
This paper introduces some new strong complete permutation polynomials.

2. Some new Classes of Strong Complete Permutation Polynomials

In [16], January 2019, some new classes of complete polynomials were given. We have added conditions that enable these classes of complete polynomials to be strong complete polynomials.

We will familiarize ourselves with one criterion for bijective (permutation) functions, which is called AGW criterion by first letters of last names of the following authors: Amir Akbary, Dragos Ghioca, Qiang Wang.

AGW criterion. ([1], Lemma 1.2) For three finite sets A, S, T such that $|S| = |T|$, suppose

$$f : A \to A, \quad g : S \to T, \quad \lambda : A \to S, \quad \theta : A \to T$$

mappings so that the following diagram commutes, which means $\theta \circ f = g \circ \lambda$.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\lambda"'] & A \arrow[d, "\theta"] \\
S \arrow[r, "g"'] & T
\end{tikzcd}$$

Figure 2. AGW criterion

If λ, θ are surjective, then the following claims are equivalent

(i) f is bijection (permutation) in A and
(ii) g is bijection from S to T and f is injective in $\lambda^{-1}(s), \forall s \in S$.

Let p be prime odd number and m be a positive integer. We will be observing new strong complete polynomials over $\mathbb{F}_{p^{2m}}$ form

$$ax^{p^m} + bx + h(x^{p^m} \pm x),$$

where $h(x) \in \mathbb{F}_{p^{2m}}[x]$.

For polynomial $h(x)$we take monomial, binomial or polynomial in form $c\sum_i (x+\delta)^i$.
Analogously with ([16], Theorem 2) we have

Theorem 2.1. *Let p prime odd number and for m positive integer, suppose that $a, b \in \mathbb{F}^*_{p^{2m}}$ so that*

$$a+b, a+b+1, a+b-1 \in \mathbb{F}^*_{p^m}$$

and $h(x) \in \mathbb{F}_{p^{2m}}[x]$. Then polynomial

$$f(x) = ax^{p^m} + bx + h(x^{p^m} - x)$$

is a strong complete polynomial in $\mathbb{F}_{p^{2m}}$ if and only if $g(x), g(x)+x, g(x)-x$ are bijective polynomials in $S = \{x^{p^m} - x | x \in \mathbb{F}_{p^{2m}}\}$, where

$$g(x) = h(x)^{p^m} - h(x) + (b - a^{p^m})x.$$

$A = F_{p^{2m}}, \quad T = S, \quad \theta = \lambda$ and define $\lambda : A \to S$, with $\lambda(x) = x^{p^m} - x, \forall x \in \mathbb{F}_{p^{2m}}$.
Thus, we have received a diagram::

For every $s \in S$, there exists $x \in \mathbb{F}_{p^{2m}}$ so that $\lambda(x) = x^{p^m} - x = s$. This means that λ is a surjection. Before we check whether the diagram in picture 3 (Diagram 1) commutes, because of $a+b \in \mathbb{F}^*_{p^m}$ we have

$$(a+b)^{p^m} = a+b, a^{p^m} + b^{p^m} = a+b$$

wherefrom

$$b^{p^m} - a = b - a^{p^m}, a^{p^m} - b = a - b^{p^m} = -(b^{p^m} - a) = -(b - a^{p^m}). \quad (2.1)$$

Now, by using equations (2.1), we have

$$\begin{tikzcd}
\mathbb{F}_{p^{2m}} \arrow[r, "f"] \arrow[d, "\lambda"'] & \mathbb{F}_{p^{2m}} \arrow[d, "\lambda"] \\
S \arrow[r, "g"'] & S
\end{tikzcd}$$

FIGURE 3. Diagram 1

$$
\begin{aligned}
&(\lambda \circ f)(x) = \lambda(f(x)) = (f(x))^{p^m} - f(x)\\
&= (ax^{p^m} + bx + h(x^{p^m} - x))^{p^m} - (ax^{p^m} + bx + h(x^{p^m} - x))\\
&= (b^{p^m} - a)x^{p^m} + (a^{p^m} - b)x + (h(x^{p^m} - x))^{p^m} - h(x^{p^m} - x)\\
&= (b - a^{p^m})x^{p^m} - (b - a^{p^m})x + (h(x^{p^m} - x))^{p^m} - h(x^{p^m} - x)\\
&= (b - a^{p^m})(x^{p^m} - x) + (h(x^{p^m} - x))^{p^m} - h(x^{p^m} - x)\\
&= g(x^{p^m} - x) = (g \circ \lambda)(x).
\end{aligned}
$$

We have seen that diagram in picture 3 commutes.

If $f(x)$ is permutation in $\mathbb{F}_{p^{2m}}$ then $f(x)$ is injective in $\lambda^{-1}(S) \subset \mathbb{F}_{p^{2m}}$, which means it is injective in $\lambda^{-1}(s), \forall s \in S$. According to AGW criterion, $g(x)$) is permutation in S S. Similarly, due to $a + b + 1 \in F^*_{p^m}$ we have

$$(a + b + 1)^{p^m} = a + b + 1, a^{p^m} + (b + 1)^{p^m} = a + b + 1,$$

wherefrom

$$(b + 1)^{p^m} - a = b + 1 - a^{p^m}, a^{p^m} - (b + 1) = \tag{2.2}$$
$$= a - (b + 1)^{p^m} = -((b + 1)^{p^m} - a) = -((b + 1) - a^{p^m}).$$

By taking $f(x) + x = \bar{f}(x), g(x) + x = \bar{g}(x)$) and by using equations (2.2) we have

$$
\begin{aligned}
&(\lambda \circ \bar{f})(x) = \lambda(\bar{f}(x)) = (\bar{f}(x))^{p^m} - \bar{f}(x)\\
&= (ax^{p^m} + (b + 1)x + h(x^{p^m} - x))^{p^m} - (ax^{p^m} + (b + 1)x + h(x^{p^m} - x))\\
&= ((b + 1)^{p^m} - a)x^{p^m} + (a^{p^m} - (b + 1))x + (h(x^{p^m} - x))^{p^m} - h(x^{p^m} - x)\\
&= (b + 1 - a^{p^m})x^{p^m} - (b + 1 - a^{p^m})x + (h(x^{p^m} - x))^{p^m} - h(x^{p^m} - x)\\
&= (b + 1 - a^{p^m})(x^{p^m} - x) + (h(x^{p^m} - x))^{p^m} - h(x^{p^m} - x)\\
&= \bar{g}(x^{p^m} - x) = (\bar{g} \circ \lambda)(x).
\end{aligned}
$$

If $f(x) + x = \bar{f}(x)$ is permutation in $\mathbb{F}_{p^{2m}}$, then it is also injective in $\lambda^{-1}(s), \forall s \in S$. According to AGW criterion $g(x) + x = \bar{g}(x)$ is permutation in S. .

Analogously, it can be seen that if $f(x) - x$ is permutation in $F_{p^{2m}}$, then it is injective in $\lambda^{-1}(s), \forall s \in S$. By AGW criterion $g(x) - x$ is permutation in S.

Thus, if $f(x)$ is a strong complete polynomial in $\mathbb{F}_{p^{2m}}$, then $g(x), g(x) + x, g(x) - x$ are permutations in S and $f(x), f(x) + x, f(x) - x$ are injective in $\lambda^{-1}(s), \forall s \in S$.

Conversely, if we suppose that $g(x)$ is permutation in S. We can prove that $f(x)$ is injective in $\lambda^{-1}(S) \subset F_{p^{2m}}$, or we can write on $(x^{p^m} - x)^{-1}(s), \forall s \in S$. Let $x, y \in \lambda^{-1}(S)$ and $f(x) = f(y)$. Then $\lambda(x) = x^{p^m} - x, \lambda(y) = y^{p^m} - y \in S$. Due to permutation $g(x)$ in S, from $g(x^{p^m} - x) = g(y^{p^m} - y)$ it follows that $x^{p^m} - x = y^{p^m} - y$, wherefrom we have equation $x^{p^m} - y^{p^m} = x - y$. From $f(x) = f(y)$ we have $ax^{p^m} + bx + h(x^{p^m} - x) = ay^{p^m} + by + h(y^{p^m} - y)$, wherefrom we have $(a + b)(x - y) = 0$. Since by assumption it is $a + b \neq 0$, then it remains that $x - y = 0$, $x = y$. That means that $f(x)$ is injective on $(x^{p^m} - x)^{-1}(s), \forall s \in S$. Then, according to AGW criterion, $f(x)$ is permutation in $\mathbb{F}_{p^{2m}}$.

Suppose that $g(x) - x$ is permutation in S. Let us prove that $f(x) - x = u(x)$ is injective on $(x^{p^m} - x)^{-1}(s), \forall s \in S$.

Suppose $u(x) = u(y)$, for $x = \lambda^{-1}(s_1)$, $y = \lambda^{-1}(s_2)$, where $s_1 = \lambda(x) = x^{p^m} - x$ and $s_2 = \lambda(y) = y^{p^m} - y$. Since $g(x) - x$ is permutation in S, then from $g(s_1) - s_1 = g(s_2) - s_2$ it follows that $s_1 = s_2$, which means $x^{p^m} - x = y^{p^m} - y$. From this equation, we have $x^{p^m} - y^{p^m} = x - y$. Since $u(x) = u(y)$ it follows that $(a + b - 1)(x - y) = 0$. Since assumption is that it is $a + b - 1 \neq 0$, then it remains that $x - y = 0$, wherefrom $x = y$.
According to AGW criterion, it follows that $f(x) - x$ is permutation in $\mathbb{F}_{p^{2m}}$.
If $g(x) + x$ is permutation in S, then similarly we prove that $f(x) + x$ is injective on $(x^{p^m} - x)^{-1}(s), \forall s \in S$, so that by AGW criterion, $f(x) + x$ is permutation in $\mathbb{F}_{p^{2m}}$. Thus, if $g(x), g(x) + x, g(x) - x$ are permutations in S, then $f(x)$ is strong complete polynomial in $F_{p^{2m}}$. Theorem 2.1 has been proven. □

For polynomial $f(x) = ax^{p^m} + bx + h(x^{p^m} + x)$) it stands

Theorem 2.2. *For p prime odd number and m positive integer, let $a, b \in \mathbb{F}^*_{p^{2m}}$ tako da*

$$a - b, a - b - 1, a - b + 1 \in \mathbb{F}^*_{p^m}\ h(x) \in \mathbb{F}_{p^{2m}}[x].$$

Then polynomial $f(x) = ax^{p^m} + bx + h(x^{p^m} + x)$ is strong complete polynomial in $\mathbb{F}_{p^{2m}}$ if and only if $t(x), t(x) + x, t(x) - x$ are bijective polynomials in $T = \{x^{p^m} + x / x \in F_{p^{2m}}\}$, where
$t(x) = h(x)^{p^m} + h(x) + (b + a^{p^m})x$.

Proof of Theorem 2.2 is similar to the proof of Theorem 2.1.

In the remaining text we will construct polynomials $h(x) \in \mathbb{F}_{p^{2m}}[x]$] that meet conditions stated in Theorems 2.1 and 2.2, with which we generate new classes of strong complete polynomial in $\mathbb{F}_{p^{2m}}$.

2.1. Construction of polynomial $h(x)$ according to Theorem 2.1.

Let the set be

$$\Omega = \{(a, b) \in \mathbb{F}^*_{p^{2m}} \times \mathbb{F}^*_{p^{2m}} | a + b \in \mathbb{F}^*_{p^m},$$

$$(a + b + 1)(a + b - 1)(b - a^{p^m})(b - a^{p^m} + 1)(b - a^{p^m} - 1) \neq 0\}.$$

We shall observe various forms of the function $h(x)$.

A) $h(x) = cx^k$, where $c \in \mathbb{F}_{p^{2m}}$ and k is positive number.

Let us expand ([16], **Proposition 3**) with strong complete polynomials.

Corollary 2.3. *Let p be prime odd number, m positive integer and $h(x) = cx^k$, where*
$c \in \mathbb{F}_{p^m}$, if k is even number and
$c \in S$, if k is odd number.
Then $f(x) = ax^{p^m} + bx + c(x^{p^m} - x)^k$ is strong complete polynomial in $\mathbb{F}_{p^{2m}}$ if and only if $(a, b) \in \Omega$.

Number $(a, b) \in \Omega$ so that $f(x)$ is strong complete polynomial in $\mathbb{F}_{p^{2m}}$ is $N = p^{3m} - 6p^{2m} + 7p^m + 8$.

Proof. As in Theorem 2.1., if $g(x) = (b - a^{p^m})x + h(x)^{p^m} - h(x), x \in S$. For each $s \in S$ it is $s^{p^m} = -s$. Really, let $s = x^{p^m} - x, x \in F_{p^{2m}}$. Then we have

$$s^{p^m} = (x^{p^m} - x)^{p^m} = x^{p^{2m}} - x^{p^m} = x - x^{p^m} = -s.$$

If k is even number and $c \in F_{p^m}$, then we have
$g(x) = (b - a^{p^m})x + c^{p^m}(x^k)^{p^m} - cx^k$
$= (b - a^{p^m})x + c(x^{p^m})^k - cx^k$
$= (b - a^{p^m})x + c(-x)^k - cx^k$
$= (b - a^{p^m})x + cx^k - cx^k$
$= (b - a^{p^m})x.$

If k is an odd number and $c \in S$, then we have

$g(x) = (b - a^{p^m})x + c^{p^m}(x^k)^{p^m} - cx^k$
$= (b - a^{p^m})x - c(x^{p^m})^k - cx^k$
$= (b - a^{p^m})x - c(-x)^k - cx^k$
$= (b - a^{p^m})x + cx^k - cx^k$
$= (b - a^{p^m})x.$

Thus, in both cases, for k and c, we receive $g(x) = (b - a^{p^m})x$, wherefrom we have $g(x) + x = (b - a^{p^m} + 1)x$ and $g(x) - x = (b - a^{p^m} - 1)x$. Thus, $g(x), g(x) + x, g(x) - x$, as linear polynomials are permutation polynomials in S, if $b - a^{p^m}, b - a^{p^m} + 1, b - a^{p^m} - 1 \neq 0$. Now, according to Theorem 2.1. we have that $f(x)$ is is a strong complete polynomial, if and only if $(a, b) \in \Omega$.

Let N be the number of $(a, b) \in \Omega$, for which pairs $f(x)$ is strong complete polynomial in $F_{p^{2m}}$. Taking that $C = \{(a, b) \in \mathbb{F}^*_{p^{2m}} \times \mathbb{F}^*_{p^{2m}} | a + b \in F_{p^m}\}$, we can observe subsets

$A_1 = \{(a, b) \in \mathbb{F}^*_{p^{2m}} \times \mathbb{F}^*_{p^{2m}} | a + b = 0\};$
$A_2 = \{(a, b) \in \mathbb{F}^*_{p^{2m}} \times \mathbb{F}^*_{p^{2m}} | a + b + 1 = 0\};$
$A_3 = \{(a, b) \in \mathbb{F}^*_{p^{2m}} \times \mathbb{F}^*_{p^{2m}} | a + b - 1 = 0\};$
$B_1 = \{(a, b) \in \mathbb{F}^*_{p^{2m}} \times \mathbb{F}^*_{p^{2m}} | b - a^{p^m} = 0\};$
$B_2 = \{(a, b) \in \mathbb{F}^*_{p^{2m}} \times \mathbb{F}^*_{p^{2m}} / b - a^{p^m} + 1 = 0\};$
$B_3 = \{(a, b) \in \mathbb{F}^*_{p^{2m}} \times \mathbb{F}^*_{p^{2m}} / b - a^{p^m} - 1 = 0\}.$

We have

$A_1 \cap A_2 = \emptyset, A_1 \cap A_3 = \emptyset, A_2 \cap A_3 = \emptyset, B_1 \cap B_2 = \emptyset, B_1 \cap B_3 = \emptyset, B_2 \cap B_3 = \emptyset.$

$$N=|C|-(|A_1|+|A_2|+|A_3|+|B_1|+|B_2|+|B_3|-|A_1\cap B_1|-|A_1\cap B_2|-|A_1\cap B_3|-|A_2\cap B_1|-|A_2\cap B_2|-|A_2\cap B_3|-|A_3\cap B_1|-|A_3\cap B_2|-|A_3\cap B_3|). \tag{2.3}$$

We notice it is

$|A_1|=p^{2m}-1, |A_2|=p^{2m}-2, |A_3|=p^{2m}-2, |B_1|=p^{2m}-1, |B_2|=p^{2m}-2, |B_3|=p^{2m}-2, |C|=(p^{2m}-2)(p^m-1)+p^{2m}-1=p^{3m}-2p^m+1, |A_1\cap B_1|=p^m-1, |A_1\cap B_2|=p^m, |A_1\cap B_3|=p^m, |A_2\cap B_1|=p^m, |A_2\cap B_2|=p^m-1, |A_2\cap B_3|=p^m,$

$$|A_3\cap B_1|=p^m, A_3\cap B_2|=p^m, |A_3\cap B_2|=p^m-1. \tag{2.4}$$

After replacement values from (2.4) in (2.3), we receive

$N=p^{3m}-6p^{2m}+7p^m+8.$ □

Example 2.4. For $p=3, m=2, a=2+2\beta^2, b=1+2\beta+\beta^2\in\mathbb{F}_{3^4}$, where $\beta^4+\beta^3+2=0$, we have $(a,b)\in\Omega$. We take $h(x)=cx^k, k=3, c=\beta+2\beta^2+\beta^3\in S=\{x^9-x, x\in\mathbb{F}_{3^4}\}$. For such conditions, it can be checked that polynomial

$$\begin{aligned}f(x)&=(2+2\beta^2)x^9+(1+2\beta+\beta^2)x+(\beta+2\beta^2+\beta^3)(x^9-x)^3\\&=(2+2\beta^2)x^9+(1+2\beta+\beta^2)x+(\beta+2\beta^2+\beta^3)(x^{27}-x^3)\end{aligned}$$

is strong complete polynomial in $\mathbb{F}_{3^4}$, where x^4+x^3+2 is irreducible polynomial that generates finite field $\mathbb{F}_{3^4}$.
With program Wolfram Mathematica 11.0 we have checked that $f(x)$ is really a permutation polynomial in $\mathbb{F}_{81}$. Also, $f(x)+x, f(x)-x$ are permutation polynomials in $\mathbb{F}_{81}$, so that $f(x)$ is strong complete polynomial in $\mathbb{F}_{81}$.
With polynomial

$$f(x)=(2+2\beta^2)x^9+(1+2\beta+\beta^2)x+(\beta+2\beta^2+\beta^3)(x^{27}-x^3)$$

in $\mathbb{F}_{81}$ we can solve the problem of 81 queens..

B) Now, let us observe the polynomial of the form

$$h(x)=\sum_{i=1}^{t}c_i x^{k_i}$$

where $t\geq 1, c_i\in\mathbb{F}_{p^{2m}}, k_i>0, 1\leq i\leq t$.

According to ([16], Proposition 4), we have

Corollary 2.5. *Let them be $t\geq 1$, $1\leq i\leq t$, where*
$c_i\in F_{p^m}$, if k_i are even numbers and
$c_i\in S$, if k_i are odd numbers,
polynomial

$$f(x)=ax^{p^m}+bx+\sum_{i=1}^{t}c_i(x^{p^m}-x)^{k_i}$$

is strong complete polynomial in $\mathbb{F}_{p^{2m}}$ *if and only if* $(a,b) \in \Omega$.

Proof. Let $g(x) = (b - a^{p^m})x + h(x)^{p^m} - h(x), x \in S$. If k_i are even numbers, and $c_i \in \mathbb{F}_{p^m}$, then we have

$$h(x)^{p^m} - h(x) = (\sum_{i=1}^{t} c_i x^{k_i})^{p^m} - \sum_{i=1}^{t} c_i x^{k_i}$$

$$= \sum_{i=1}^{t} c_i(-x)^{k_i} - \sum_{i=1}^{t} c_i x^{k_i} = 0.$$

Likewise, if k_i are odd numbers and respectively with index i,$c_i \in S$, then we have

$$h(x)^{p^m} - h(x) = (\sum_{i=1}^{t} c_i x^{k_i})^{p^m} - \sum_{i=1}^{t} c_i x^{k_i}$$

$$= \sum_{i=1}^{t} (-c_i)(-x)^{k_i} - \sum_{i=1}^{t} c_i x^{k_i} = 0.$$

Therefore, in both cases for k_i, respectively for c_i, we have $g(x) = (b - a^{p^m})x$. For $(a,b) \in \Omega$ polynomials $g(x), g(x) + x, g(x) - x$ permute S, so that due to Theorem 6.1. polynomial $f(x)$ is strong complete polynomial in $\mathbb{F}_{p^{2m}}$. The reverse is also true. If $f(x)$ is strong complete polynomial in $\mathbb{F}_{p^{2m}}$, then $(a,b) \in \Omega$. □

C) Now we will expand ([16], Proposition 5) for $h(x)$ in a more complicated form.

Corollary 2.6. *Polynomial* $f(x) = ax^{p^m} + bx + h(x^{p^m} - x)$ *is strong complete polynomial in* $\mathbb{F}_{p^{2m}}$ *if and only if* $(a,b) \in \Omega$, *where* $h(x)$ *has some of the following forms*

(i) $h(x) = u(x)^{sp^m} + u(x)$, *where* $u(x) \in \mathbb{F}_{p^{2m}}[x]$;

(ii) $h(x) = c(x+\delta)^{i(p^m+1)}$, *for* i *positive integer,* $\delta \in F_{p^{2m}}, c \in F_{p^m}$;

(iii) $h(x) = c(x+\delta)^s$, *for* s *even number and* $c \in F_{p^m}$ *and* $\delta \in S$ *or* s *odd number and* $c, \delta \in S$.

Proof. For example, if we consider the case (ii), $g(x) = (b - a^{p^m})x + h(x)^{p^m} - h(x)$, $x \in S$, then we have
$h(x)^{p^m} - h(x) = (c(x+\delta)^{i(p^m+1)})^{p^m} - c(x+\delta)^{i(p^m+1)} = c^{p^m}(x+\delta)^{i(p^{2m}+p^m)}) - c(x+\delta)^{i(p^m+1)} = c(x+\delta)^{ip^{2m}}(x+\delta)^{ip^m} - c(x+\delta)^{i(p^m+1)} = c(x^{p^{2m}} + \delta^{p^{2m}})^i(x+\delta)^{ip^m} - c(x+\delta)^{i(p^m+1)} = c(x+\delta)^i(x+\delta)^{ip^m} - c(x+\delta)^{i(p^m+1)} = c(x+\delta)^{i(p^m+1)} - c(x+\delta)^{i(p^m+1)} = 0.$
Likewise in cases $(i), (iii)$ it is $h(x)^{p^m} - h(x) = 0$, so that it remains $g(x) = (b - a^{p^m})x$. Then, according to Theorem 2.1. $f(x)$ is a strong complete polynomial if and only if $(a,b) \in \Omega$. □

In a similar manner, we can add more polynomials $h(x) \in \mathbb{F}_{p^{2m}}$, so that polynomial $f(x) = ax^{p^m} + bx + h(x^{p^m} - x)$ is a strong complete polynomial in $\mathbb{F}_{p^{2m}}$ according to Theorem 2.1. Likewise, if we take $h(x)$ as under A), B), C) polynomial $f(x) = ax^{p^m} + bx + h(x^{p^m} + x)$ is a strong complete polynomial in $\mathbb{F}_{p^{2m}}$ according to Theorem 2.2.

References

[1] A. Akbary, D. Ghioca, Q. Wang, On constructing permutations of finite fields, *Finite Fields and Their Applications* **17** (2011), no. 1, 51–67.

[2] A.O.L. Atkin, L. Hay and R.G. Larson, Enumeration and construction of pandiagonal Latin squares of prime order, *Comput. Math. Appl.* **9** (1983), no. 2, 267–292.

[3] L.A. Bassalygo, V.A. Zinoviev, Permutation and complete permutation polynomials, *Finite Fields Appl.* **33** (2015), 198–211.

[4] J. Bell, Cyclotomic orthomorphisms of finite fields, *Discrete Appl. Math.* **161** (2013), no. 1-2, 294–300.

[5] A.A. Bruen, R. Dixon, The n-queen problem, *Discrete Math.* **12** (1975), no. 4, 393-395.

[6] W. S. Chou, Permutation polynomials on finite fields and combinatorial applications, Ph.D. Thesis, Pennsylvania State University, 1990.

[7] A.B. Evans, On strong complete mappings. *Congr. Numer.* **70** (1990), 241–248.

[8] A.B. Evans, The existence of strong complete mappings, *Electron. J. Combin.* **19** (2012), no. 1, paper no. 34, pp. 10.

[9] M. Hall, L.J. Paige, Complete mappings of finite groups, *Pacific J. Math.*, **5** (1955), no. 4, 541–549.

[10] A. Hedayat, A complete solution to the existence and nonexistence of Knut Vik designs and orthogonal Knut Vik designs, *J. Combinatorial Theory Ser. A* **22** (1977), no. 3, 331–337.

[11] A. Hedayat, W.T. Federer, On the nonexistence of Knut Vik designs for all even orders, *Ann. Statist.* **3** (1975), no. 2, 445–447.