University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.17 No.1 Mar 2022

Some of permutation polynomials of the form $D_{n,k}(x,a) + (Tr_m^n(D_{n,k}(x,a)^k + \alpha_1)^{s_1} + (Tr_m^n(D_{n,k}(x,a)^k + \alpha_2)^{s_2}$ over $\mathbb{F}_2^{2m}$

Hasan H. Mushatet

Ministry of Education, Thi-Qar Education Directorate, Iraq.

hasanalhelaly@utq.edu.iq

https://doi.org/10.32792/utq/utj/vol17/1/2

ABSTRACT

By this paper, we intend structure of some class of permutation polynomials which having the form $D_{n,k}(x,a) + (Tr_m^n(D_{n,k}(x,a)^k + \alpha_1)^{s_1} + (Tr_m^n(D_{n,k}(x,a)^k + \alpha_2)^{s_2}$ over $\mathbb{F}_2^{2m}$ depend on (AGW criterion).

Keywords: Permutation polynomial, Dickson polynomial, Reversed Dickson polynomial, Trace function.

1. Introduction

Let q be a prime power, and $q = p^n$, p is a prime positive integer number, and let $\mathbb{F}_q$ be a finite field, then a polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) over $\mathbb{F}_q$ if It is bijective.

There are an important applications of permutation polynomial in a several areas as cryptography , coding theory , communication engineering , and combinatorial design theory. The first studies on permutation polynomial was by Hermite[3][7], after that , Dickson worked on this field[4][6]

Akbary, Ghioca and Wang structured a criterion (which known as the AGW criterion) to investigate by permutation polynomials. [1][7]

The target of this paper is to constructing some classes of permutation polynomials of the form

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.17 No.1 Mar 2022

$D_{n,k}(x,a) + (Tr_m^n(D_{n,k}(x,a)^k + \alpha_1)^{s_1} + (Tr_m^n(D_{n,k}(x,a)^k + \alpha_2)^{s_2}$

Over $\mathbb{F}_{2^{2m}}$,when m, n, s_1, s_2 , *and* k are positive integers, α_1 *and* α_2 are odd positive numbers in $\mathbb{F}_{2^{2m}}$ with $n = 2m$, and a fixed $a \in \mathbb{F}_{2^{2m}}$ .In this paper we will depend on AGW(criterion) with some propositions and lemmas to our proofs.

2. Preliminaries

The trace function from $\mathbb{F}_{p^n}$ into $\mathbb{F}_{p^m}$ denoted by :

$Tr_m^n(x) = x + x^{p^m} + x^{p^{2m}} + \cdots + x^{p^{\left(\frac{n}{m-1}\right)m}}$, where m , n are two positive integers and $m \mid n$, and p is a prime number.

Let π be a subset of $\mathbb{F}_{p^n}$ and define by:

$\pi = \{\gamma^{p^m} - \gamma \, : \, \gamma \in \mathbb{F}_{p^n}\}$ ……………….(1)

Then for each element $\alpha \in \pi$, satisfy:

$Tr_m^n(\alpha) = 0$ ………………………………...(2)

For a prime power , a function $\emptyset(x) = \sum_{i=0}^{s} a_i x^{q^i}$, when $a_0 , a_1 , \ldots , a_s$ in $\mathbb{F}_q$ then we called $\emptyset(x)$ a $\mathbb{F}_q -$ linear polynomial over $\mathbb{F}_{p^m}$.[1][8]

Lemma (2.1) [2]

Let m , n are positive integers , $m \mid n$, and let $\emptyset(x)$ be a $\mathbb{F}_q -$ linear polynomial over $\mathbb{F}_{p^m}$, $h(x) \in \mathbb{F}_{p^n}[x]$ be a polynomial such that $h(x^{p^m} - x) \in \mathbb{F}_{p^m} \backslash \{0\}$, and

$g(x) \in \mathbb{F}_{p^n}[x]$ be any polynomial , for all $x \in \mathbb{F}_{p^n}$.

Then $h\left(x^{p^m} - x\right)\emptyset(x) + g(x^{p^m} - x)$ is a permutation of $\mathbb{F}_{p^n}$ if and only if:

(i) $\emptyset(x)$ induces a permutation polynomial of $\mathbb{F}_{p^m}$;
(ii) $h(x)\emptyset(x) + g(x)^{p^m} - g(x)$ permutes π which defined in (1) .

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.17 No.1 Mar 2022

Lemma(2.2) [2]

Let $,n$, and t are positive integers with $m \mid n$, s_i be nonnegative integer, $1 \le i \le t$

And a fixed $\delta \in \mathbb{F}_{p^n}$ then $f(x) = \sum_{i=1}^{t}\left(x^{p^m} - x + \delta\right)^{s_i} + x$ is a permutation polynomial over $\mathbb{F}_{p^n}$ if and only if :

$\sum_{i=1}^{t}((x+\delta)^{p^m s_i} - (x+\delta)^{s_i}) + x$ permutes .

Lemma(2.3)[10]

Let $,n\,,s$, and k are positive integers with $n = 2m$, And a fixed $\delta \in \mathbb{F}_{p^n}$ then the polynomial $f(x) = x + (Tr_m^n(x)^k + \delta)^{sp^m}$ induces a permutation over $\mathbb{F}_{p^{2m}}$

if and only if $g(x) = (x^k + \alpha)^{sp^m}(x^k + \alpha)^s + x$ be a bijection on the set :

$$S = \{\, x \in \mathbb{F}_{p^{2m}} : x^{p^m} - x = 0\}$$

Proposition(2.1)[10]

Let $\alpha \in \mathbb{F}_{2^{2m}}$, and m is an odd then the polynomial

$$f(x) = x + (Tr_m^n(x)^{\frac{2^m+1}{3}} + \alpha)^{2^{m-1}+1}$$ permutes $\mathbb{F}_{p^{2m}}$.

Proposition(2.2)[6]

Assume that $\alpha \in \mathbb{F}_{2^{2m}}$, and let m is an odd then the polynomial

$$f(x) = x + (Tr_m^n(x)^{2^{\frac{m+1}{3}}-1} + \alpha)^{2^{\frac{m+1}{3}}+1}$$ permutes $\mathbb{F}_{p^{2m}}$.

Proposition(2.3)[10]

When $\alpha_1, \alpha_2 \in \mathbb{F}_{2^{2m}}$, and $s_1, s_2\,, k_1, k_2$ are positive integers then:

$f(x) = x + (Tr_m^n(x)^{k_1} + \alpha_1)^{s_1} + (Tr_m^n(x)^{k_2} + \alpha_2)^{s_2}$ is a permutation polynomial over $\mathbb{F}_{2^{2m}}$ if and only if :

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.17 No.1 Mar 2022

$h(x) = x + (Tr_m^n(x)^{k_1} + \alpha_1)^{s_1}$ permutes $\mathbb{F}_{2^{2m}}$.

Definition (2.1) [5]

Let $a \in \mathbb{F}_q$, for any positive integers n , k we can define an $n - th$ Dickson Polynomial of the $(k+1) - th$ kind over $\mathbb{F}_q$ as:

$$D_{n,k}(x,a) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-jk}{n-j} \binom{n-j}{j} (-a)^j \, x^{n-2j}$$

Definition (2.2) [5][9]

Let $a \in \mathbb{F}_q$, and $n , k \in \mathbb{Z}^+$ then the $n - th$ Reversed Dickson Polynomial from the $(k+1) - th$ kind over $\mathbb{F}_q$ can be define as:

$$D_{n,k}(x,a) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-jk}{n-j} \binom{n-j}{j} (-1)^j \, a^{n-2j} x^j$$

Lemma (2.4) [6]

$$D_{n,k}(x,a) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-jk}{n-j} \binom{n-j}{j} (-a)^j \, x^{n-2j}$$

when $a \in \mathbb{F}_{2^n}$ is a permutation polynomial over $\mathbb{F}_{2^n}$ if and only if

$\gcd(n, 2^{2n} - 1) = 1$.

Example(2.1) : Let $n = even\ number$ then that yield

$\gcd(n, 2^{2n} - 1) = 1.$

For example $n = 4$ then $\gcd(4, 2^{2\times 4} - 1) = \gcd(4, 255) = 1$

That implies $D_{4,k}(x,a)$ is permutation polynomial over $\mathbb{F}_{2^n}$ when $a , x \in \mathbb{F}_{2^n}, and\ k \in \mathbb{Z}^+$.

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.17 No.1 Mar 2022

Lemma(2.5)[6]

Let m be an odd positive integer number then

$\gcd\left(2^{\frac{m+1}{2}}+1, 2^m-1\right)=1.$

3. PPs of the form $\boldsymbol{D_{n,k}(x,a)+(Tr_m^n(D_{n,k}(x,a)^k+a)^s}$

Proposition (3.1)

Let $,n\,,s\,,$ and $k\in\mathbb{Z}^+$, and a fixed $a\in\mathbb{F}_{p^n}$ where $n=2m$, and m is odd then the polynomial:

$$D_{n,k}(x,a)=\sum_{j=0}^{\left\lfloor\frac{n}{2}\right\rfloor}\frac{n-jk}{n-j}\binom{n-j}{j}(-a)^j\,x^{n-2j}$$

Is a permutation polynomial if and only if $\gcd\left(2^{\frac{m+1}{2}}, 2^m-1\right)=1.$

Proof: Suppose that $D_{n,k}(x,a)$ be a permutation polynomial then:

$\gcd(n, 2^{2n}-1)=1$ (Lemma 2.4)

That implies to $\gcd\left(2^{\frac{m+1}{2}}, 2^m-1\right)=1$

Now assume that $\gcd\left(2^{\frac{m+1}{2}}, 2^m-1\right)=1$ then by (Lemma 2.4) we obtain $D_n(x,a)$ is a permutation polynomial.

Then $D_{n,k}(x,a)$ is a permutation polynomial □

Example(3.1) : Let $n=2m$, and m is odd positive integer number then that yield $\gcd\left(2^{\frac{m+1}{2}}+1, 2^m-1\right)=1$.

For example $m=3$ then $\gcd\left(2^{\frac{3+1}{2}}+1, 2^3-1\right)=\gcd(5,7)=1.$

That is equivalence to $\gcd(n, 2^{2n}-1)$ when $n=4$,which implies

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.17 No.1 Mar 2022

$\gcd(4, 2^{2\times 4} - 1) = \gcd(4, 255) = 1$

Thus $D_{6,k}(x,a)$ is permutation polynomial over $\mathbb{F}_{2^{2m}}$ when $a, x \in \mathbb{F}_{2^{2m}}, and\ k \in \mathbb{Z}^+$. $m = 5$ then $\gcd\left(2^{\frac{5+1}{2}} + 1, 2^5 - 1\right) = \gcd(8,31) = 1$.

Example(3.2) : In the following Table 3.2 we take some values for $m, n, k\ and\ a$, when a is odd to find the form of Dickson Polynomial $D_{n,k}(x,a)$:

Table 3.2

m	$n = 2m$	k	a	$\mathbb{F}_{2^{2m}}$	$D_{n,k}(x,a)$
3	6	1	1	$\mathbb{F}_{2^6}$	$x^6 + 59x^4 + 6x^2 + 63$
5	10	2	3	$\mathbb{F}_{2^{10}}$	$x^{10} + 1000x^8 + 189x^6 + 484x^4 + 405x^2$
7	14	3	5	$\mathbb{F}_{2^{14}}$	$x^{14} + 16329x^{12} + 1100x^{10} + 7009x^8 + 9866x^6 + 10982x^4 + 10626x^2 + 12589$
9	18	4	7	$\mathbb{F}_{2^{18}}$	$x^{18} + 262046x^{16} + 3675x^{14} + 199718x^{12} + 81299x^{10} + 182058x^8 + 172114x^6 + 123252x^4 + 149121x^2 + 229006$

Example(3.3) : In the following Table 2.2 we take some values for $m, n, k\ and\ a$, when a is $even$ to find the form of Dickson Polynomial $D_{n,k}(x,a)$:

Table 3.3

m	$n = 2m$	k	a	$\mathbb{F}_{2^{2m}}$	$D_{n,k}(x,a)$
3	6	1	2	$\mathbb{F}_{2^6}$	$x^6 + 54x^4 + 24x^2 + 56$

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.17 No.1 Mar 2022

5	10	2	4	$\mathbb{F}_{2^{10}}$	$x^2(x^8+992x^6+336x^4+768x^2+256)$
7	14	3	6	$\mathbb{F}_{2^{14}}$	$x^{14}+16318x^{12}+1584x^{10}+184x^8+5280x^6+10560x^4+2176x^2+1408$
9	18	4	8	$\mathbb{F}_{2^{18}}$	$x^{18}+262032x^{16}+4800x^{14}+168960x^{12}+61440x^{10}+196608x^8$

Proposition (3.2)

Let $,n\,,s$, and $k \in \mathbb{Z}^+$, and a fixed $a \in \mathbb{F}_{p^n}$, a *is even* where $n = 2m$, and m is odd then the polynomial:

$$D_{n,k}(x,a) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-jk}{n-j}\binom{n-j}{j}(-1)^j\, a^{n-2j} x^j$$

Is a permutation polynomial if and only if $\gcd\left(2^{\frac{m+1}{2}}, 2^m-1\right) = 1$.

Proof: Suppose that $D_{n,k}(x,a)$ be a permutation polynomial then:

$\gcd(n, 2^{2n}-1) = 1$ (Lemma2.4)

That implies to $\gcd\left(2^{\frac{m+1}{2}}, 2^m-1\right) = 1$

Now since $\gcd\left(2^{\frac{m+1}{2}}, 2^m-1\right) = 1$ then by (Lemma 2.4) we obtain $D_n(x,a)$ is a permutation polynomial

Then $D_{n,k}(x,a)$ is a permutation polynomial □

Example(3.4) : In the following Table 3.4 we take some values for $m, n\,, k$ *and* a , when a is *odd* to find the form of reversed Dickson Polynomial $D_{n,k}(x,a)$:

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.17 No.1 Mar 2022

Table 3.4

m	$n=2m$	k	a	$\mathbb{F}_{2^{2m}}$	$D_{n,k}(x,a)$
3	6	1	2	$\mathbb{F}_{2^6}$	$63x^3+24x^2+48x$
5	10	2	4	$\mathbb{F}_{2^{10}}$	$80x^4$
7	14	3	6	$\mathbb{F}_{2^{14}}$	$x^7+15880x^6+1760x^5+9856x^4+5376x^3+12288x^2+4096x$
9	18	4	8	$\mathbb{F}_{2^{18}}$	$2x^7(129056x+90112x^2)$

4. PPs of the form $\boldsymbol{D_{n,k}(x,a)+(Tr_m^n(D_{n,k}(x,a)^{k_1}+\alpha_1)^{s_1}+(Tr_m^n(D_{n,k}(x,a)^{k_2}+\alpha_2)^{s_2}}$

Proposition (4.1)

For a positive integers $m\,,n\,,s\,,and\ k$ with $n=2m$ and a fixed $a\in\mathbb{F}_{p^n}$, and $an\ odd\ \alpha\in\mathbb{F}_{p^n}$ then :

$f(x)=D_{n,k}(x,a)+(Tr_m^n(D_{n,k}(x,a)^k+\alpha)^s$

induces a permutation polynomial on $\mathbb{F}_{2^{2m}}$ if and only if

$g(x)=[(D_{n,k}(x,a))^k+\alpha]^{s.p^m}+[(D_{n,k}(x,a))^k+\alpha]^s+(D_{n,k}(x,a)$ is one-to-one and onto over the set $\pi=\{l\in\mathbb{F}_{p^{2m}}: l^{p^m}-l=0\}$.

Proof: since $\pi=\{l\in\mathbb{F}_{p^{2m}}: l^{p^m}-l=0\}$ then we can write :

$\pi=\{l^{p^m}+l: l\in\mathbb{F}_{p^{2m}}\}$.

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.17 No.1 Mar 2022

Suppose that $\Psi(x) = \overline{\Psi}(x) = l^{p^m} + l = Tr_m^n(D_{n,k}(x,a))$ then we can note it verified the following diagram:

$$\begin{array}{ccc} \mathbb{F}_{p^{2m}} & \xrightarrow{f} & \mathbb{F}_{p^{2m}} \\ \Psi \downarrow & & \downarrow \overline{\Psi} \\ \pi & \xrightarrow{g} & \pi \end{array} \qquad \text{commutes.}$$

For any $\delta \in \pi$ we have $\Psi^{-1}(\delta) = \{x \in \mathbb{F}_{p^{2m}}: x^{p^m} + x = \delta\}$, so that

$f(x) = D_{n,k}(x,a) + (Tr_m^n(D_{n,k}(x,a)^k + \alpha)^s$ is one-to-one over $\Psi^{-1}(\delta)$.

By (AGW criterion) f is a permutation on $\mathbb{F}_{p^{2m}}$ if and only if $g(x)$ is

a permutation over π . □

Lemma (4.1)

Let m, n, s_1, s_2 , $k_1, and\ k_2$, are positive integers, α_1 and α_2 are odd positive numbers in $\mathbb{F}_{2^{2m}}$ with $n = 2m$, and a fixed $a \in \mathbb{F}_{2^{2m}}$ then:

$f(x) = D_{n,k}(x,a) + (Tr_m^n(D_{n,k}(x,a)^{k_1} + \alpha_1)^{s_1} + (Tr_m^n(D_{n,k}(x,a)^{k_2} + \alpha_2)^{s_2}$ is permutes $\mathbb{F}_{2^{2m}}$

if and only if it induces a bijection :

$g(x) = D_{n,k}(x,a) + (Tr_m^n(D_{n,k}(x,a)^k + \alpha_1)^{s_1}$ over $\mathbb{F}_{2^{2m}}$.

Proof : Let $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ then (By proposition 2.3) we obtain :

$g(x) = D_{n,k}(x,a) + (Tr_m^n(D_{n,k}(x,a)^k + \alpha_1)^{s_1}$ permutes $\mathbb{F}_{2^{2m}}$.

Now let $g(x)$ permutes $\mathbb{F}_{2^{2m}}$ then (By Lemma 3.2) g is a bijection on the set $\pi = \{l \in \mathbb{F}_{2^{2m}}: l^{p^m} - l = 0\}$

Then by (AGW Criterion) we obtain f is permutes $\mathbb{F}_{2^{2m}}$. □

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.17 No.1 Mar 2022

Example(4.1) : In the following Table 4.1 we take some values for $m, n\ , k, k_1, and\ a$ to find $Tr_m^n(D_{n,k}(x,a))^{k_1}$,where $D_{n,k}(x,a)$ be Dickson polynomial :

Table 4.1

m	n	k	a	k_1	$Tr_m^n(D_{n,k}(x,a))^{k_1}$
3	6	1	1	1	$52x^2 + 18x^4 + 6x^6 + 35x^8 + 34x^{10} + 4x^{12})$
5	10	2	2	2	$x^{24}(256x^4 + 352x^8 + 256x^{10} + 336x^{12} + 896x^{14} + 3x^{16} + 256)$
7	14	3	4	4	$4096x^{60} + 14336x^{62} + 1792x^{64} + 15104x^{66} + 4208x^{68} + 6904x^{70} + 1418x^{72} + 9188x^{74} + 5214x^{76} + 5488x^{78} + 2278x^{80} + 15988x^{82} + 4x^{84}$

Example(4.2) : In the following Table 4.2 we take some values for $m, n\ , k, k_1, s, and\ a$ to find $(Tr_m^n D_{n,k}(x,a)^{k_1} + \alpha)^s$,where $D_{n,k}(x,a)$ be Dickson polynomial, and $\alpha\ an\ odd\ in\ \mathbb{F}_{2^{2m}}$:

Table 4.2

m	n	k	a	k_1	α	s	$(Tr_m^n D_{n,k}(x,a)^{k_1} + \alpha)^s$
3	6	1	1	1	1	1	$52x^2 + 54x^4 + 10x^6 + 58x^8 + 4x^{10} + 10x^{12} + 5$
5	10	2	2	2	3	2	$896x^{72} + 832x^{76} + 84x^{80} + 640x^{152} + 448x^{156} + 512x^{158} + 98x^{160} + 27$

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.17 No.1 Mar 2022

7	14	3	4	4	5	3	$12288x^{440} + 4096x^{442} + 3584x^{444} + 6400x^{446} + 7350x^{448} + 8192x^{888} + 8192x^{890} + 7168x^{892} + 4608x^{894} + 3966x^{896} + 12288x^{1336} + 4036x^{1338} + 13824x^{1340} + 9472x^{1342} + 11250x^{1344} + 375$

References

[1] Akbary, D. Ghioca, and Q. Wang, "On constructing permutations of finite fields," *Finite Fields their Appl.*, vol. 17, no. 1, pp. 51–67, 2011, doi: 10.1016/j.ffa.2010.10.002.

[2] L. Li, S. Wang, C. Li, and X. Zeng, "Finite Fields and Their Applications," *Finite Fields Their Appl.*, vol. 51, pp. 31–61, 2018, doi: 10.1016/j.ffa.2018.01.003.

[3] Mullen, Gary L., and Daniel Panario. *Handbook of finite fields*. Vol. 17. Boca Raton: CRC Press, 2013.

[4] N. Fernando, X. D. Hou, and S. D. Lappano, "A new approach to permutation polynomials over finite fields, II," *Finite Fields their Appl.*, vol. 22, pp. 122–158, 2013, doi: 10.1016/j.ffa.2013.01.001.

[5] Q. Wang and J. L. Yucas, "Dickson polynomials over finite fields," *Finite Fields their Appl.*, vol. 18, no. 4, pp. 814–831, 2012, doi: 10.1016/j.ffa.2012.02.001.

[6] Rota, Gian-Carlo, ed. *Encyclopedia of Mathematics and its Applications*. Addison-Wesley, 1976.

[7] X. D. Hou, "Permutation polynomials over finite fields - A survey of recent advances," *Finite Fields their Appl.*, vol. 32, pp. 82–119, 2015, doi: 10.1016/j.ffa.2014.10.001.

[8] X. Zeng, X. Zhu, N. Li, and X. Liu, "Finite Fields and Their Applications Permutation polynomials over F 2 n of the form," *Finite Fields Their Appl.*, vol. 47, pp. 256–268, 2017, doi: 10.1016/j.ffa.2017.06.012.

[9] Y. Zheng, F. Wang, L. Wang, and W. Wei, "Finite Fields and Their Applications On inverses of some permutation polynomials over finite fields of characteristic three ☆," *Finite Fields Their Appl.*, vol. 66, p. 101670, 2020, doi: 10.1016/j.ffa.2020.101670.

[10] Z. Li, M. Wang, J. Wu, and X. Zhu, "Finite Fields and Their Applications Some new forms of permutation polynomials based on the AGW criterion," *Finite Fields Their Appl.*, vol. 61, p. 101584, 2020, doi: 10.1016/j.ffa.2019.101584.