On Some Permutation Binomials of the Form $x^{\frac{2^n-1}{k}+1} + ax$ over $\mathbb{F}_{2^n}$: Existence and Count

Sumanta Sarkar, Srimanta Bhattacharya, Ayça Çeşmelioğlu

Outline of the talk

1. Introduction
   - Permutation polynomials over finite fields

2. Permutation Binomials
   - Binomials of the form $x^{\frac{2^n-1}{3}+1} + ax \in \mathbb{F}_{2^n}[x]$
   - Binomials of the form $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$

Outline of the talk

Outline of the talk

Permutation polynomials

Permutation polynomials over finite fields

Permutation polynomials

Permutation polynomials over finite fields

- $\mathbb{F}_q$ = The finite field of order q.

Permutation polynomials

Permutation polynomials over finite fields

- $\mathbb{F}_q$ = The finite field of order q.
- $F(x) \in \mathbb{F}_q[x]$ a *permutation polynomial* of $\mathbb{F}_q$ if $F : a \mapsto F(a), a \in \mathbb{F}_q$, is a permutation of $\mathbb{F}_q$.

Permutation Polynomials

Which polynomials are permutation polynomials ?

Permutation Polynomials

Which polynomials are permutation polynomials ?

- Monomials : x^d is a pp $\Leftrightarrow (d, q-1) = 1$.

Permutation Polynomials

Which polynomials are permutation polynomials ?

- Monomials : x^d is a pp $\Leftrightarrow (d, q-1) = 1$.

- Binomials: $x^m + ax^n, a \in \mathbb{F}_q$ is a pp $\Leftrightarrow$??

- Non-monomials: **Hermite-Dickson** criteria-
  Let $\mathbb{F}_q$ be of characteristic p. Then $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions are satisfied:
  1. $f(x)$ has exactly one root in $\mathbb{F}_q$.
  2. For each integer t with $1 \leq t \leq q-2$, and $p \nmid t$, the reduction of $f(x)^t \mod (x^q - x)$ has degree at most $q-2$.

  Difficult to apply for a general polynomial.

Outline of the talk

1 Introduction
- Permutation polynomials over finite fields

2 Permutation Binomials
- Binomials of the form $x^{\frac{2^n-1}{3}+1} + ax \in \mathbb{F}_{2^n}[x]$
- Binomials of the form $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$

Permutation binomials of the form $x^{\frac{q-1}{m}+1} + ax \in \mathbb{F}_q[x]$

Motivation:

Permutation binomials of the form $x^{\frac{q-1}{m}+1} + ax \in \mathbb{F}_q[x]$

Motivation:

- Simplest non-trivial case for a binomial.

Permutation binomials of the form $x^{\frac{q-1}{m}+1} + ax \in \mathbb{F}_q[x]$

Motivation:

- Simplest non-trivial case for a binomial.
- Widely studied in different contexts.

Outline of the talk

Our contribution I

Our contribution I

Theorem

For every even integer $n = 2^i t$, t odd and $n \notin \{2, 4\}$, a permutation binomial of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$ always exists.

Our contribution I

Theorem

For every even integer $n = 2^i t$, t odd and $n \notin \{2, 4\}$, a permutation binomial of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$ always exists.

Corollary

The number of permutation binomials of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^{2^i t}}[x]$, where $a \in \mathbb{F}_{2^t}$ and t odd is $\frac{2^{t+1}-1}{3}$.

Existing Results I

- **(Carlitz (1962)):**, for sufficiently large q, there exists $a \in \mathbb{F}_q$, such that $x^{\frac{q-1}{3}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
  - **(Carlitz and Wells (1966)):** Given m, for sufficiently large q, there exists $a \in \mathbb{F}_q$ such that $x^{\frac{q-1}{m}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
- Asymptotic estimate of number of such a s for given q was done by Laigle-Chapuy(2007), and Masuda and Zieve (2009).
- The above relies (directly or indirectly) on heavy tools from function fields.
  - **Our method is very elementary and results are exact.**

Existing Results I

- **(Carlitz (1962)):**, for sufficiently large q, there exists $a \in \mathbb{F}_q$, such that $x^{\frac{q-1}{3}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
  - **(Carlitz and Wells (1966)):** Given m, for sufficiently large q, there exists $a \in \mathbb{F}_q$ such that $x^{\frac{q-1}{m}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
- Asymptotic estimate of number of such a s for given q was done by Laigle-Chapuy(2007), and Masuda and Zieve (2009).
- The above relies (directly or indirectly) on heavy tools from function fields.
  - **Our method is very elementary and results are exact.**

Existing Results I

- **(Carlitz (1962)):**, for sufficiently large q, there exists $a \in \mathbb{F}_q$, such that $x^{\frac{q-1}{3}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
  - **(Carlitz and Wells (1966)):** Given m, for sufficiently large q, there exists $a \in \mathbb{F}_q$ such that $x^{\frac{q-1}{m}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
- Asymptotic estimate of number of such a s for given q was done by Laigle-Chapuy(2007), and Masuda and Zieve (2009).
- The above relies (directly or indirectly) on heavy tools from function fields.
  - **Our method is very elementary and results are exact.**

Existing Results I

- **(Carlitz (1962)):**, for sufficiently large q, there exists $a \in \mathbb{F}_q$, such that $x^{\frac{q-1}{3}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
  - **(Carlitz and Wells (1966)):** Given m, for sufficiently large q, there exists $a \in \mathbb{F}_q$ such that $x^{\frac{q-1}{m}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
- Asymptotic estimate of number of such a s for given q was done by Laigle-Chapuy(2007), and Masuda and Zieve (2009).
- The above relies (directly or indirectly) on heavy tools from function fields.
  - **Our method is very elementary and results are exact.**

Existing Results I

- **(Carlitz (1962)):**, for sufficiently large q, there exists $a \in \mathbb{F}_q$, such that $x^{\frac{q-1}{3}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
  - **(Carlitz and Wells (1966)):** Given m, for sufficiently large q, there exists $a \in \mathbb{F}_q$ such that $x^{\frac{q-1}{m}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
- Asymptotic estimate of number of such a s for given q was done by Laigle-Chapuy(2007), and Masuda and Zieve (2009).
- The above relies (directly or indirectly) on heavy tools from function fields.
  - **Our method is very elementary and results are exact.**

Existing Results I

- **(Carlitz (1962)):**, for sufficiently large q, there exists $a \in \mathbb{F}_q$, such that $x^{\frac{q-1}{3}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
  - **(Carlitz and Wells (1966)):** Given m, for sufficiently large q, there exists $a \in \mathbb{F}_q$ such that $x^{\frac{q-1}{m}+1} + ax$ is a permutation polynomial of $\mathbb{F}_q$.
- Asymptotic estimate of number of such a s for given q was done by Laigle-Chapuy(2007), and Masuda and Zieve (2009).
- The above relies (directly or indirectly) on heavy tools from function fields.
  - **Our method is very elementary and results are exact.**

Outline of the talk

Our contribution II

Theorem

Let $n \geq 3$ and $a \in \mathbb{F}_{2^{2n}}^*$. Then for odd n, $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a^{2^n-1} \in \{\omega, \omega^2\}$. For n even there is no such permutation polynomial of this form.

Corollary

Let n be odd, then $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a \in \omega\mathbb{F}_{2^n}^* \bigcup \omega^2\mathbb{F}_{2^n}^*$ where $\omega^2 + \omega + 1 = 0$ in $\mathbb{F}_{2^{2n}}$. Hence the number of such a is exactly $2(2^n - 1)$

Our contribution II

Theorem

Let $n \geq 3$ and $a \in \mathbb{F}_{2^{2n}}^*$. Then for odd n, $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a^{2^n-1} \in \{\omega, \omega^2\}$. For n even there is no such permutation polynomial of this form.

Corollary

Let n be odd, then $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a \in \omega\mathbb{F}_{2^n}^* \bigcup \omega^2\mathbb{F}_{2^n}^*$ where $\omega^2 + \omega + 1 = 0$ in $\mathbb{F}_{2^{2n}}$. Hence the number of such a is exactly $2(2^n - 1)$

Our contribution II

Theorem

Let $n \geq 3$ and $a \in \mathbb{F}_{2^{2n}}^*$. Then for odd n, $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a^{2^n-1} \in \{\omega, \omega^2\}$. For n even there is no such permutation polynomial of this form.

Corollary

Let n be odd, then $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a \in \omega\mathbb{F}_{2^n}^* \bigcup \omega^2\mathbb{F}_{2^n}^*$ where $\omega^2 + \omega + 1 = 0$ in $\mathbb{F}_{2^{2n}}$. Hence the number of such a is exactly $2(2^n - 1)$

Existing Results II

Existing Results II

- **Charpin and Kyureghyan (2008)**
  Let $0 \leq k \leq t-1$ and $\nu \neq 0$. Then the polynomial

$$x^{2^k+2} + \nu x \in \mathbb{F}_{2^t}[x]$$

  is a permutation polynomial of $\mathbb{F}_{2^t}$ if and only if t is even and
  - either $k = 1$ and ν is not a third power in $\mathbb{F}_{2^t}$, or
  - $t = 2r$ with r odd, $k = r$, and $\nu \in \omega\mathbb{F}_{2^r}$, where $\omega \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$

Existing Results II

- **Charpin and Kyureghyan (2008)**
  Let $0 \leq k \leq t-1$ and $\nu \neq 0$. Then the polynomial

$$x^{2^k+2} + \nu x \in \mathbb{F}_{2^t}[x]$$

  is a permutation polynomial of $\mathbb{F}_{2^t}$ if and only if t is even and
  - either $k = 1$ and ν is not a third power in $\mathbb{F}_{2^t}$, or
  - $t = 2r$ with r odd, $k = r$, and $\nu \in \omega\mathbb{F}_{2^r}$, where $\omega \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$
- Uses results from Walsh-spectra of boolean functions.

Existing Results II

- **Charpin and Kyureghyan (2008)**
  Let $0 \leq k \leq t-1$ and $\nu \neq 0$. Then the polynomial

$$x^{2^k+2} + \nu x \in \mathbb{F}_{2^t}[x]$$

  is a permutation polynomial of $\mathbb{F}_{2^t}$ if and only if t is even and
  - either $k = 1$ and ν is not a third power in $\mathbb{F}_{2^t}$, or
  - $t = 2r$ with r odd, $k = r$, and $\nu \in \omega\mathbb{F}_{2^r}$, where $\omega \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$
- Uses results from Walsh-spectra of boolean functions.
- **We prove the "if" part using very elementary and more direct method.**

Tools

Tools

- **(Wan and Lidl (1991))**
  Let m and r be two positive integers such that m divides $q-1$. Let α be a primitive element in $\mathbb{F}_q$ and assume P is a polynomial in $\mathbb{F}_q[x]$. Then $Q(x) = x^r P(x^{\frac{q-1}{m}})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions are satisfied.

Tools

- **(Wan and Lidl (1991))**
  Let m and r be two positive integers such that m divides $q-1$. Let α be a primitive element in $\mathbb{F}_q$ and assume P is a polynomial in $\mathbb{F}_q[x]$. Then $Q(x) = x^r P(x^{\frac{q-1}{m}})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions are satisfied.
  1. $\gcd(r, \frac{q-1}{m}) = 1$,

Tools

- **(Wan and Lidl (1991))**
  Let m and r be two positive integers such that m divides $q-1$. Let α be a primitive element in $\mathbb{F}_q$ and assume P is a polynomial in $\mathbb{F}_q[x]$. Then $Q(x) = x^r P(x^{\frac{q-1}{m}})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions are satisfied.
  1. $\gcd(r, \frac{q-1}{m}) = 1$,
  2. for all i, $0 \le i < m$, $P(\alpha^{i\frac{q-1}{m}}) \neq 0$,

Tools

- **(Wan and Lidl (1991))**
  Let m and r be two positive integers such that m divides $q-1$. Let α be a primitive element in $\mathbb{F}_q$ and assume P is a polynomial in $\mathbb{F}_q[x]$. Then $Q(x) = x^r P(x^{\frac{q-1}{m}})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions are satisfied.
  1. $\gcd(r, \frac{q-1}{m}) = 1$,
  2. for all i, $0 \le i < m$, $P(\alpha^{i\frac{q-1}{m}}) \neq 0$,
  3. for all j, $0 \le i < j < m$, $Q(\alpha^i)^{\frac{q-1}{m}} \neq Q(\alpha^j)^{\frac{q-1}{m}}$.

Tools

- **(Wan and Lidl (1991))**
  Let m and r be two positive integers such that m divides $q-1$. Let α be a primitive element in $\mathbb{F}_q$ and assume P is a polynomial in $\mathbb{F}_q[x]$. Then $Q(x) = x^r P(x^{\frac{q-1}{m}})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions are satisfied.
  1. $\gcd(r, \frac{q-1}{m}) = 1$,
  2. for all i, $0 \le i < m$, $P(\alpha^{i\frac{q-1}{m}}) \neq 0$,
  3. for all j, $0 \le i < j < m$, $Q(\alpha^i)^{\frac{q-1}{m}} \neq Q(\alpha^j)^{\frac{q-1}{m}}$.
- Elementary methods.

Norm and Trace: Definitions

Norm and Trace: Definitions

- **Norm:**

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma) = \gamma^{\frac{q^m-1}{q-1}}, \gamma \in F_{q^m}$$

.

Norm and Trace: Definitions

- **Norm:**

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma) = \gamma^{\frac{q^m-1}{q-1}}, \gamma \in F_{q^m}$$

.

- **Trace:**

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma) = \gamma + \gamma^q + \ldots + \gamma^{q^{m-1}}, \gamma \in F_{q^m}$$

.

Proof Highlights

Theorem

For every integer $n = 2^i t$, $t > 1$ odd, a permutation binomial of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$ always exists.

Note: $a \in \mathbb{F}_{2^2}^* \Rightarrow x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$ is not a permutation polynomial.

Proof Highlights (contd..)

(Wan and Lidl)

Proof Highlights (contd..)

(Wan and Lidl)

$\Updownarrow$

Lemma (**Niederreiter and Winterhof (2005), Evans (1992)**)

Let $n = 2k$, $k > 2$ be any integer. Then $W(x) = x(x^{\frac{2^n-1}{3}} + a), a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$ is a permutation polynomial over $\mathbb{F}_{2^n}$ if and only if the elements $(1+a)^{\frac{2^n-1}{3}}, \omega(\omega+a)^{\frac{2^n-1}{3}}, \omega^2(\omega^2+a)^{\frac{2^n-1}{3}}$ are all distinct.

Proof Highlights (contd..)

Lemma 1:

Lemma

Let $t \geq 3$ be an odd integer. Then for each $\delta \in \{0, 1\}$ there exists an element $a \in \mathbb{F}_{2^t}$ such that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a + \omega) = \omega^{2^\delta}$.

Proof Highlights (contd..)

Lemma 1:

Lemma

Let $t \geq 3$ be an odd integer. Then for each $\delta \in \{0, 1\}$ there exists an element $a \in \mathbb{F}_{2^t}$ such that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a + \omega) = \omega^{2^\delta}$.

$\Updownarrow$

Proof Highlights (contd..)

Lemma 1:

Lemma

Let $t \geq 3$ be an odd integer. Then for each $\delta \in \{0, 1\}$ there exists an element $a \in \mathbb{F}_{2^t}$ such that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a + \omega) = \omega^{2^\delta}$.

$$\Updownarrow$$

On the coset $\mathbb{F}_{2^t} + \omega$ of the finite field $\mathbb{F}_{2^{2t}}$, the norm $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ takes the values ω, ω^2.

Proof Highlights (contd..)

t odd and $\alpha \in \mathbb{F}_{2^t}^* \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha) = 1$.

Proof Highlights (contd..)

t odd and $\alpha \in \mathbb{F}_{2^t}^* \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha) = 1$.
$\beta \in \mathbb{F}_{2^t}, \alpha \in \mathbb{F}_{2^t}^* \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\beta + \alpha\omega) = N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha^{-1}\beta + \omega)$.

Proof Highlights (contd..)

$$\left\{ \begin{array}{l} t \text{ odd and } \alpha \in \mathbb{F}_{2^t}^* \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha) = 1. \\ \beta \in \mathbb{F}_{2^t}, \alpha \in \mathbb{F}_{2^t}^* \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\beta + \alpha\omega) = N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha^{-1}\beta + \omega). \end{array} \right\}$$

$$\Downarrow$$

$N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ takes same values on the cosets $\mathbb{F}_{2^t} + \alpha\omega, \alpha \in \mathbb{F}_{2^t}^*$.

Proof Highlights (contd..)

$$\left\{ \begin{array}{l} t \text{ odd and } \alpha \in \mathbb{F}_{2^t}^* \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha) = 1. \\ \beta \in \mathbb{F}_{2^t}, \alpha \in \mathbb{F}_{2^t}^* \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\beta + \alpha\omega) = N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha^{-1}\beta + \omega). \end{array} \right\}$$

$$\Downarrow$$

$N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ takes same values on the cosets $\mathbb{F}_{2^t} + \alpha\omega, \alpha \in \mathbb{F}_{2^t}^*$.
$N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ is onto $\mathbb{F}_{2^2}$.

Proof Highlights (contd..)

$$\left\{ \begin{array}{l} t \text{ odd and } \alpha \in \mathbb{F}_{2^t}^* \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha) = 1. \\ \beta \in \mathbb{F}_{2^t}, \alpha \in \mathbb{F}_{2^t}^* \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\beta + \alpha\omega) = N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha^{-1}\beta + \omega). \end{array} \right\}$$

$$\Downarrow$$

$N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ takes same values on the cosets $\mathbb{F}_{2^t} + \alpha\omega, \alpha \in \mathbb{F}_{2^t}^*$.
$N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ is onto $\mathbb{F}_{2^2}$.
$N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ Takes the values $0, 1$ on $\mathbb{F}_{2^t}$.

Proof Highlights (contd..)

$$\left\{ \begin{array}{l} t \text{ odd and } \alpha \in \mathbb{F}_{2^t}^* \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha) = 1. \\ \beta \in \mathbb{F}_{2^t}, \alpha \in \mathbb{F}_{2^t}^* \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\beta + \alpha\omega) = N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha^{-1}\beta + \omega). \end{array} \right\}$$

$$\Downarrow$$

$$\left\{ \begin{array}{ll} N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}} & \text{takes same values on the cosets } \mathbb{F}_{2^t} + \alpha\omega, \alpha \in \mathbb{F}_{2^t}^*. \\ N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}} & \text{is onto } \mathbb{F}_{2^2}. \\ N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}} & \text{Takes the values } 0, 1 \text{ on } \mathbb{F}_{2^t}. \end{array} \right\}$$

$$\Downarrow$$

On each of the cosets $\mathbb{F}_{2^t} + \alpha\omega, \alpha \in \mathbb{F}_{2^t}^*$, $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ takes the values ω, ω^2. $\square$

Proof Highlights (contd..)

$q = 2^t,\ m = 2^i, n = 2^{2^i t} = q^m.$

Proof Highlights (contd..)

$q = 2^t,\ m = 2^i, n = 2^{2^i t} = q^m.$

To show that there exists $a \in \mathbb{F}_q$ such that the elements $(1+a)^{\frac{q^m-1}{3}}, \omega(\omega+a)^{\frac{q^m-1}{3}}, \omega^2(\omega^2+a)^{\frac{q^m-1}{3}} \in \mathbb{F}_{2^2}^*$ are all distinct.

Proof Highlights (contd..)

- Lemma 1 $\Rightarrow \exists a \in \mathbb{F}_q$ such that $(a+\omega)^{\frac{q^2-1}{3}} = \omega^{2^\delta}$, $\delta \in \{0,1\}$.

Proof Highlights (contd..)

- Lemma 1 $\Rightarrow \exists a \in \mathbb{F}_q$ such that $(a+\omega)^{\frac{q^2-1}{3}} = \omega^{2^\delta}$, $\delta \in \{0,1\}$.
- $(2^t-1)(2^t+1)/3$ elements $\beta + \alpha\omega \in \mathbb{F}_{2^{2t}}, \alpha \in \mathbb{F}_{2^t}^*, \beta \in \mathbb{F}_{2^t}$ such that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\beta + \alpha\omega) = \omega$.

Proof Highlights (contd..)

- Lemma 1 $\Rightarrow \exists a \in \mathbb{F}_q$ such that $(a+\omega)^{\frac{q^2-1}{3}} = \omega^{2^\delta}$, $\delta \in \{0,1\}$.
- $(2^t-1)(2^t+1)/3$ elements $\beta + \alpha\omega \in \mathbb{F}_{2^{2t}}, \alpha \in \mathbb{F}_{2^t}^*, \beta \in \mathbb{F}_{2^t}$ such that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\beta + \alpha\omega) = \omega$.
- $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(1+\omega) = \omega \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha + \alpha\omega) = \omega, \alpha \in \mathbb{F}_{2^t}^*$.

Proof Highlights (contd..)

- Lemma 1 $\Rightarrow \exists a \in \mathbb{F}_q$ such that $(a+\omega)^{\frac{q^2-1}{3}} = \omega^{2^\delta}$, $\delta \in \{0,1\}$.
- $(2^t-1)(2^t+1)/3$ elements $\beta + \alpha\omega \in \mathbb{F}_{2^{2t}}, \alpha \in \mathbb{F}_{2^t}^*, \beta \in \mathbb{F}_{2^t}$ such that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\beta + \alpha\omega) = \omega$.
- $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(1+\omega) = \omega \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha + \alpha\omega) = \omega, \alpha \in \mathbb{F}_{2^t}^*$.
- # of such $\alpha \in \mathbb{F}_{2^t}^* = (2^t-1) \Rightarrow \exists \alpha \in \mathbb{F}_{2^t}^*, \beta \in \mathbb{F}_{2^t}$, $\alpha \neq \beta, N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\beta + \alpha\omega) = \omega$.

Proof Highlights (contd..)

- Lemma 1 $\Rightarrow \exists a \in \mathbb{F}_q$ such that $(a+\omega)^{\frac{q^2-1}{3}} = \omega^{2^\delta}$, $\delta \in \{0,1\}$.
- $(2^t-1)(2^t+1)/3$ elements $\beta + \alpha\omega \in \mathbb{F}_{2^{2t}}, \alpha \in \mathbb{F}_{2^t}^*, \beta \in \mathbb{F}_{2^t}$ such that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\beta + \alpha\omega) = \omega$.
- $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(1+\omega) = \omega \Rightarrow N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\alpha + \alpha\omega) = \omega, \alpha \in \mathbb{F}_{2^t}^*$.
- # of such $\alpha \in \mathbb{F}_{2^t}^* = (2^t-1) \Rightarrow \exists \alpha \in \mathbb{F}_{2^t}^*, \beta \in \mathbb{F}_{2^t}$, $\alpha \neq \beta, N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\beta + \alpha\omega) = \omega$.
- Similarly, $\exists \gamma \in \mathbb{F}_{2^t}^*, \tau \in \mathbb{F}_{2^t}$, $\gamma \neq \tau, N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(\gamma + \tau\omega) = \omega^2$.

Proof Highlights (contd..)

For $\delta \in \{0,1\}$ $\exists a \neq 1$ in $\mathbb{F}_{2^t}$ such that $(a+\omega)^{\frac{q^2-1}{3}} = \omega^{2^\delta}$

For such a we have the following.

- $(a+\omega^2)^{\frac{q^2-1}{3}} = \omega^{2^{\delta+t}}$.
- $(1+a)^{\frac{q^m-1}{3}} = 1$, since $(1+a) \in \mathbb{F}_q$ and $a \neq 1$
- $\omega(a+\omega)^{\frac{q^m-1}{3}} = \omega^{2^{\delta+i-1}+1}$
- $\omega^2(a+\omega^2)^{\frac{q^m-1}{3}} = (\omega^{2^{\delta+i-1}+1})^2$

Proof Highlights (contd..)

$\omega^{2^{i+\delta-1}+1} \neq 1$ if and only if $i + \delta$ is odd.

Proof Highlights (contd..)

$\omega^{2^{i+\delta-1}+1} \neq 1$ if and only if $i + \delta$ is odd. choose a such that:

$$\delta := \begin{cases} 0 & \text{if } i \text{ is odd} \\ 1 & \text{if } i \text{ is even.} \end{cases}$$

Proof Highlights (contd..)

$\omega^{2^{i+\delta-1}+1} \neq 1$ if and only if $i + \delta$ is odd. choose a such that:

$$\delta := \begin{cases} 0 & \text{if } i \text{ is odd} \\ 1 & \text{if } i \text{ is even.} \end{cases}$$

$\omega^{2^{i+\delta-1}+1} \neq 1 \Rightarrow \omega^{2^{i+\delta-1}+1} = \omega$ or ω^2.

Proof Highlights (contd..)

Theorem

For every integer $n = 2^i$, where $i > 2$, a permutation binomial of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$ always exists.

Proof Highlights (contd..)

Theorem

For every integer $n = 2^i$, where $i > 2$, a permutation binomial of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$ always exists.

It is enough to show that for $n = 2^i$, $i > 2$ there always exists $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$ such that

$$\{(1+a)^{\frac{2^n-1}{3}}, \omega(\omega+a)^{\frac{2^n-1}{3}}, \omega^2(\omega^2+a)^{\frac{2^n-1}{3}}\}$$

are all distinct.

Proof Highlights (contd..)

Theorem

For every integer $n = 2^i$, where $i > 2$, a permutation binomial of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$ always exists.

It is enough to show that for $n = 2^i$, $i > 2$ there always exists $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$ such that

$$\{(1+a)^{\frac{2^n-1}{3}}, \omega(\omega+a)^{\frac{2^n-1}{3}}, \omega^2(\omega^2+a)^{\frac{2^n-1}{3}}\}$$

are all distinct.

Case 1: $i = 3$, i.e., $n = 8$. $a \in \mathbb{F}_{2^8} \setminus \mathbb{F}_{2^2}$ such that $N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(1+a) = 1, N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(\omega+a) = 1$ and $N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(\omega^2+a) = 1$.(By direct computation)

Proof Highlights (contd..)

Theorem

For every integer $n = 2^i$, where $i > 2$, a permutation binomial of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^n}[x]$ always exists.

It is enough to show that for $n = 2^i$, $i > 2$ there always exists $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$ such that

$$\{(1+a)^{\frac{2^n-1}{3}}, \omega(\omega+a)^{\frac{2^n-1}{3}}, \omega^2(\omega^2+a)^{\frac{2^n-1}{3}}\}$$

are all distinct.

Case 1: $i = 3$, i.e., $n = 8$. $a \in \mathbb{F}_{2^8} \setminus \mathbb{F}_{2^2}$ such that $N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(1+a) = 1, N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(\omega+a) = 1$ and $N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(\omega^2+a) = 1$.(By direct computation)

Case 2: $i \geq 4$.

For $\beta \in \mathbb{F}_{2^8}$, $N_{\mathbb{F}_{2^{2^i}}/\mathbb{F}_{2^2}}(\beta) = (N_{\mathbb{F}_{2^8}/\mathbb{F}_{2^2}}(\beta))^{2^{i-3}}$

Proof Highlights (contd..)

For a obtained in Case 1,

$$N_{\mathbb{F}_{2^{2i}}/\mathbb{F}_{2^2}}(1+a) = 1, N_{\mathbb{F}_{2^{2i}}/\mathbb{F}_{2^2}}(\omega+a) = 1, N_{\mathbb{F}_{2^{2i}}/\mathbb{F}_{2^2}}(\omega^2+a) = 1.$$

Proof Highlights (contd..)

Corollary

The number of permutation binomials of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^{2^i t}}[x]$, *where* $a \in \mathbb{F}_{2^t}$ *and* t *odd is*

$$(2^{t+1} - 1)/3.$$

Proof Highlights (contd..)

Corollary

The number of permutation binomials of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^{2^i t}}[x]$, *where* $a \in \mathbb{F}_{2^t}$ *and* t *odd is*

$$(2^{t+1} - 1)/3.$$

Count the number of $a \in \mathbb{F}_{2^t}$ such that

$$\{N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(1+a), \omega N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega+a), \omega^2 N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega^2+a)\}$$

are all distinct.

Proof Highlights (contd..)

Corollary

The number of permutation binomials of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^{2^i t}}[x]$, *where* $a \in \mathbb{F}_{2^t}$ *and* t *odd is*

$$(2^{t+1} - 1)/3.$$

Count the number of $a \in \mathbb{F}_{2^t}$ such that

$$\{N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(1+a), \omega N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega+a), \omega^2 N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega^2+a)\}$$

are all distinct.

Possible only in the following two ways.

1. $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+1) = 1$, $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = 1$ and $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega^2) = 1$,

Proof Highlights (contd..)

Corollary

The number of permutation binomials of the form $x(x^{\frac{2^n-1}{3}} + a) \in \mathbb{F}_{2^{2^i t}}[x]$, *where* $a \in \mathbb{F}_{2^t}$ *and* t *odd is*

$$(2^{t+1} - 1)/3.$$

Count the number of $a \in \mathbb{F}_{2^t}$ such that

$$\{N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(1+a), \omega N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega+a), \omega^2 N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(\omega^2+a)\}$$

are all distinct.

Possible only in the following two ways.

1. $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+1) = 1, N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = 1$ and $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega^2) = 1$,
2. $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+1) = 1, N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = \omega$ and $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega^2) = \omega^2$.

Proof Highlights (contd..)

Observation: $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega^2) = N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}((a+\omega)^{2^t})$ for odd t.

Proof Highlights (contd..)

Observation: $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega^2) = N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}((a+\omega)^{2^t})$ for odd t.

$$\Downarrow$$

Proof Highlights (contd..)

Observation: $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega^2) = N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}((a+\omega)^{2^t})$ for odd t.

$$\Downarrow$$

$$N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega^2) = (N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega))^{2^t}$$

.

$$\Downarrow$$

Case 1: Enough to count the number of $a \in \mathbb{F}_{2^t}$ such that $N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+\omega) = 1$.

Proof Highlights (contd..)

For any $a \in \mathbb{F}_{2^t}^*$, $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a) = 1$

Proof Highlights (contd..)

For any $a \in \mathbb{F}_{2^t}^*$, $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a) = 1$

$$\Downarrow$$

Proof Highlights (contd..)

For any $a \in \mathbb{F}_{2^t}^*$, $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a) = 1$

$$\Downarrow$$

$$N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a) = N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(N_{\mathbb{F}_{2^{2^i t}}/\mathbb{F}_{2^{2t}}}(a))$$

Proof Highlights (contd..)

$$\text{For any } a \in \mathbb{F}_{2^t}^*, N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a) = 1$$

$$\Downarrow$$

$$N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a) = N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(N_{\mathbb{F}_{2^{2^i t}}/\mathbb{F}_{2^{2t}}}(a))$$

$$= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a^{2^{i-1}})$$

Proof Highlights (contd..)

For any $a \in \mathbb{F}_{2^t}^*$, $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a) = 1$

$$\Downarrow$$

$$\begin{aligned} N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a) &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(N_{\mathbb{F}_{2^{2^i t}}/\mathbb{F}_{2^{2t}}}(a)) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a^{2^{i-1}}) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a)^{2^{i-1}} \end{aligned}$$

Proof Highlights (contd..)

For any $a \in \mathbb{F}_{2^t}^*$, $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a) = 1$

$$\Downarrow$$

$$\begin{aligned} N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a) &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(N_{\mathbb{F}_{2^{2^i t}}/\mathbb{F}_{2^{2t}}}(a)) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a^{2^{i-1}}) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a)^{2^{i-1}} \\ &= 1. \end{aligned}$$

Proof Highlights (contd..)

For any $a \in \mathbb{F}_{2^t}^*$, $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a) = 1$

$$\Downarrow$$

$$\begin{aligned} N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a) &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(N_{\mathbb{F}_{2^{2^i t}}/\mathbb{F}_{2^{2t}}}(a)) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a^{2^{i-1}}) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a)^{2^{i-1}} \\ &= 1. \end{aligned}$$

$$\Downarrow$$

Proof Highlights (contd..)

$$\text{For any } a \in \mathbb{F}_{2^t}^*, N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a) = 1$$

$$\Downarrow$$

$$\begin{aligned} N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a) &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(N_{\mathbb{F}_{2^{2^i t}}/\mathbb{F}_{2^{2t}}}(a)) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a^{2^{i-1}}) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a)^{2^{i-1}} \\ &= 1. \end{aligned}$$

$$\Downarrow$$

$$\left|\{a \in \mathbb{F}_{2^t} : N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+1) = 1\}\right| = 2^t - 1$$

.

Proof Highlights (contd..)

$$\text{For any } a \in \mathbb{F}_{2^t}^*, N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a) = 1$$

$$\Downarrow$$

$$\begin{aligned} N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a) &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(N_{\mathbb{F}_{2^{2^i t}}/\mathbb{F}_{2^{2t}}}(a)) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a^{2^{i-1}}) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a)^{2^{i-1}} \\ &= 1. \end{aligned}$$

$$\Downarrow$$

$$\left|\{a \in \mathbb{F}_{2^t} : N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+1) = 1\}\right| = 2^t - 1$$

$$\Downarrow$$

.

Proof Highlights (contd..)

$$\text{For any } a \in \mathbb{F}_{2^t}^*, N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a) = 1$$

$$\Downarrow$$

$$\begin{aligned} N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a) &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(N_{\mathbb{F}_{2^{2^i t}}/\mathbb{F}_{2^{2t}}}(a)) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a^{2^{i-1}}) \\ &= N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a)^{2^{i-1}} \\ &= 1. \end{aligned}$$

$$\Downarrow$$

$$\left|\{a \in \mathbb{F}_{2^t} : N_{\mathbb{F}_{2^n}/\mathbb{F}_{2^2}}(a+1) = 1\}\right| = 2^t - 1$$

$$\Downarrow$$

.

$$\left|\{b \in \mathbb{F}_{2^{2t}} \setminus \mathbb{F}_{2^t} : N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(b) = 1\}\right| = (2^{2t}-1)/3 - (2^t - 1) = (2^t - 1)(2^t - 2)/3.$$

Proof Highlights (contd..)

- Can be shown that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ maps equal number of elements in every coset $\mathbb{F}_{2^t} + \alpha\omega$, $\alpha \in \mathbb{F}_{2^t}^*$ to a fixed element of $\mathbb{F}_{2^2}^*$

Proof Highlights (contd..)

- Can be shown that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ maps equal number of elements in every coset $\mathbb{F}_{2^t} + \alpha\omega$, $\alpha \in \mathbb{F}_{2^t}^*$ to a fixed element of $\mathbb{F}_{2^2}^*$
- Number of such cosets is $2^t - 1$

Proof Highlights (contd..)

- Can be shown that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ maps equal number of elements in every coset $\mathbb{F}_{2^t} + \alpha\omega$, $\alpha \in \mathbb{F}_{2^t}^*$ to a fixed element of $\mathbb{F}_{2^2}^*$
- Number of such cosets is $2^t - 1$
- Considering the coset $\mathbb{F}_{2^t} + \omega$, we have

$$\left|a \in \mathbb{F}_{2^t} : N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a + \omega) = 1\right| = (2^t - 2)/3.$$

Proof Highlights (contd..)

- Can be shown that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ maps equal number of elements in every coset $\mathbb{F}_{2^t} + \alpha\omega$, $\alpha \in \mathbb{F}_{2^t}^*$ to a fixed element of $\mathbb{F}_{2^2}^*$
- Number of such cosets is $2^t - 1$
- Considering the coset $\mathbb{F}_{2^t} + \omega$, we have

$$|a \in \mathbb{F}_{2^t} : N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a + \omega) = 1| = (2^t - 2)/3.$$

-

$$|a \in \mathbb{F}_{2^t} : N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a + \omega) = \omega| = (2^{2t} - 1)/3 \cdot \frac{1}{2^t - 1} = (2^t + 1)/3.$$

Proof Highlights (contd..)

- Can be shown that $N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}$ maps equal number of elements in every coset $\mathbb{F}_{2^t} + \alpha\omega$, $\alpha \in \mathbb{F}_{2^t}^*$ to a fixed element of $\mathbb{F}_{2^2}^*$
- Number of such cosets is $2^t - 1$
- Considering the coset $\mathbb{F}_{2^t} + \omega$, we have

$$|a \in \mathbb{F}_{2^t} : N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a + \omega) = 1| = (2^t - 2)/3.$$

-

$$|a \in \mathbb{F}_{2^t} : N_{\mathbb{F}_{2^{2t}}/\mathbb{F}_{2^2}}(a + \omega) = \omega| = (2^{2t} - 1)/3 \cdot \frac{1}{2^t - 1} = (2^t + 1)/3.$$

- The total number of permutations with $a \in \mathbb{F}_{2^t}$ is $(2^t - 2)/3 + (2^t + 1)/3 = (2^{t+1} - 1)/3$.

Proof Highlights (contd..)

Theorem

Let $n \geq 3$ and $a \in \mathbb{F}_{2^{2n}}^*$. Then for odd n, $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a^{2^n-1} \in \{\omega, \omega^2\}$. For n even there is no such permutation polynomial of this form.

Proof Highlights (contd..)

Theorem

Let $n \geq 3$ and $a \in \mathbb{F}_{2^{2n}}^*$. Then for odd n, $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a^{2^n-1} \in \{\omega, \omega^2\}$. For n even there is no such permutation polynomial of this form.

Observation: $f(x) = x^{2^n+2} + ax$ is a pp $\Rightarrow a \in \mathbb{F}_{2^{2n}}^* \setminus \mathbb{F}_{2^n}^*$.

Proof Highlights (contd..)

Theorem

Let $n \geq 3$ and $a \in \mathbb{F}_{2^{2n}}^*$. Then for odd n, $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a^{2^n-1} \in \{\omega, \omega^2\}$. For n even there is no such permutation polynomial of this form.

Observation: $f(x) = x^{2^n+2} + ax$ is a pp $\Rightarrow a \in \mathbb{F}_{2^{2n}}^* \setminus \mathbb{F}_{2^n}^*$.

$$x^{2^n+2} + ax = x\left(x^{\frac{2^{2n}-1}{2^n-1}} + a\right)$$

Proof Highlights (contd..)

Theorem

Let $n \geq 3$ and $a \in \mathbb{F}_{2^{2n}}^*$. Then for odd n, $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a^{2^n-1} \in \{\omega, \omega^2\}$. For n even there is no such permutation polynomial of this form.

Observation: $f(x) = x^{2^n+2} + ax$ is a pp $\Rightarrow a \in \mathbb{F}_{2^{2n}}^* \setminus \mathbb{F}_{2^n}^*$.

$$x^{2^n+2} + ax = x\left(x^{\frac{2^{2n}-1}{2^n-1}} + a\right)$$

Wan-Lidl Theorem

Proof Highlights (contd..)

Theorem

Let $n \geq 3$ and $a \in \mathbb{F}_{2^{2n}}^*$. Then for odd n, $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a^{2^n-1} \in \{\omega, \omega^2\}$. For n even there is no such permutation polynomial of this form.

Observation: $f(x) = x^{2^n+2} + ax$ is a pp $\Rightarrow a \in \mathbb{F}_{2^{2n}}^* \setminus \mathbb{F}_{2^n}^*$.

$$x^{2^n+2} + ax = x\left(x^{\frac{2^{2n}-1}{2^n-1}} + a\right)$$

Wan-Lidl Theorem

1. *Condition 1:* Trivially satisfied.

Proof Highlights (contd..)

Theorem

Let $n \geq 3$ and $a \in \mathbb{F}_{2^{2n}}^*$. Then for odd n, $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a^{2^n-1} \in \{\omega, \omega^2\}$. For n even there is no such permutation polynomial of this form.

Observation: $f(x) = x^{2^n+2} + ax$ is a pp $\Rightarrow a \in \mathbb{F}_{2^{2n}}^* \setminus \mathbb{F}_{2^n}^*$.

$$x^{2^n+2} + ax = x\left(x^{\frac{2^{2n}-1}{2^n-1}} + a\right)$$

Wan-Lidl Theorem

1. *Condition 1:* Trivially satisfied.
2. *Condition 2:* α a primitive element of $\mathbb{F}_{2^{2n}} \Rightarrow 0 \leq i < 2^n - 1$, $\alpha^{(2^n+1)i} \in \mathbb{F}_{2^n}^*$. Satisfied by the above observation.

Proof Highlights (contd..)

$x^{2^n+2} + ax$ is a permutation polynomial.

Proof Highlights (contd..)

$x^{2^n+2} + ax$ is a permutation polynomial.

$$\Updownarrow$$

Condition 3 of Wan-Lidl Theorem is satisfied.

Proof Highlights (contd..)

$x^{2^n+2} + ax$ is a permutation polynomial.

$$\Updownarrow$$

Condition 3 of Wan-Lidl Theorem is satisfied.

$$\Updownarrow$$

$f(\alpha^i)^{2^n+1}$ is $1-1$, α primitive element of $\mathbb{F}_{2^{2n}}$, $0 \leq i < 2^n - 1$.

Proof Highlights (contd..)

$x^{2^n+2} + ax$ is a permutation polynomial.

$$\Updownarrow$$

Condition 3 of Wan-Lidl Theorem is satisfied.

$$\Updownarrow$$

$f(\alpha^i)^{2^n+1}$ is $1-1$, α primitive element of $\mathbb{F}_{2^{2n}}$, $0 \leq i < 2^n - 1$.

$$\Updownarrow$$

$g(v) = v(v+a)^{2^n+1}$ induces a $1-1$ mapping for $v \in \mathbb{F}_{2^n}^*$

Proof Highlights (contd..)

$x^{2^n+2} + ax$ is a permutation polynomial.

$$\Updownarrow$$

Condition 3 of Wan-Lidl Theorem is satisfied.

$$\Updownarrow$$

$f(\alpha^i)^{2^n+1}$ is $1-1$, α primitive element of $\mathbb{F}_{2^{2n}}$, $0 \leq i < 2^n - 1$.

$$\Updownarrow$$

$g(v) = v(v+a)^{2^n+1}$ induces a $1-1$ mapping for $v \in \mathbb{F}_{2^n}^*$

$$\Updownarrow$$

$g(v) = v^3 + (a^{2^n} + a)v^2 + a^{2^n+1}v$ induces $1-1$ mapping for $v \in \mathbb{F}_{2^n}^*$.

Proof Highlights (contd..)

$x^{2^n+2} + ax$ is a permutation polynomial.

$$\Updownarrow$$

Condition 3 of Wan-Lidl Theorem is satisfied.

$$\Updownarrow$$

$f(\alpha^i)^{2^n+1}$ is $1-1$, α primitive element of $\mathbb{F}_{2^{2n}}$, $0 \leq i < 2^n - 1$.

$$\Updownarrow$$

$g(v) = v(v+a)^{2^n+1}$ induces a $1-1$ mapping for $v \in \mathbb{F}_{2^n}^*$

$$\Updownarrow$$

$g(v) = v^3 + (a^{2^n} + a)v^2 + a^{2^n+1}v$ induces $1-1$ mapping for $v \in \mathbb{F}_{2^n}^*$.

Proof Highlights (contd..)

Observation: $g(v) \in \mathbb{F}_{2^n}[v]$ as $(a^{2^n} + a)^{2^n} = a^{2^n} + a$ and $(a^{2^n+1})^{2^n-1} = 1$ are both in $\mathbb{F}_{2^n}$.

Proof Highlights (contd..)

Observation: $g(v) \in \mathbb{F}_{2^n}[v]$ as $(a^{2^n} + a)^{2^n} = a^{2^n} + a$ and $(a^{2^n+1})^{2^n-1} = 1$ are both in $\mathbb{F}_{2^n}$.

Substitution: $v = u + a^{2^n} + a$ in $g(v)$.

Proof Highlights (contd..)

Observation: $g(v) \in \mathbb{F}_{2^n}[v]$ as $(a^{2^n} + a)^{2^n} = a^{2^n} + a$ and $(a^{2^n+1})^{2^n-1} = 1$ are both in $\mathbb{F}_{2^n}$.

Substitution: $v = u + a^{2^n} + a$ in $g(v)$.

$g(v) = v^3 + (a^{2^n} + a)v^2 + a^{2^n+1}v$ induces $1-1$ mapping for $v \in \mathbb{F}_{2^n}^*$.

Proof Highlights (contd..)

Observation: $g(v) \in \mathbb{F}_{2^n}[v]$ as $(a^{2^n} + a)^{2^n} = a^{2^n} + a$ and $(a^{2^n+1})^{2^n-1} = 1$ are both in $\mathbb{F}_{2^n}$.

Substitution: $v = u + a^{2^n} + a$ in $g(v)$.

$g(v) = v^3 + (a^{2^n} + a)v^2 + a^{2^n+1}v$ induces $1-1$ mapping for $v \in \mathbb{F}_{2^n}^*$.

$$\Updownarrow$$

Proof Highlights (contd..)

Observation: $g(v) \in \mathbb{F}_{2^n}[v]$ as $(a^{2^n} + a)^{2^n} = a^{2^n} + a$ and $(a^{2^n+1})^{2^n-1} = 1$ are both in $\mathbb{F}_{2^n}$.

Substitution: $v = u + a^{2^n} + a$ in $g(v)$.

$g(v) = v^3 + (a^{2^n} + a)v^2 + a^{2^n+1}v$ induces $1-1$ mapping for $v \in \mathbb{F}_{2^n}^*$.

$$\Updownarrow$$

$h(u) = u^3 + (a^{2^{n+1}} + a^2 + a^{2^n+1})u$ is $1-1$ for $u \in \mathbb{F}_{2^n} \setminus \{a^{2^n} + a\}$

Proof Highlights (contd..)

Observation: $g(v) \in \mathbb{F}_{2^n}[v]$ as $(a^{2^n} + a)^{2^n} = a^{2^n} + a$ and $(a^{2^n+1})^{2^n-1} = 1$ are both in $\mathbb{F}_{2^n}$.

Substitution: $v = u + a^{2^n} + a$ in $g(v)$.

$g(v) = v^3 + (a^{2^n} + a)v^2 + a^{2^n+1}v$ induces $1-1$ mapping for $v \in \mathbb{F}_{2^n}^*$.

$$\Updownarrow$$

$h(u) = u^3 + (a^{2^{n+1}} + a^2 + a^{2^n+1})u$ is $1-1$ for $u \in \mathbb{F}_{2^n} \setminus \{a^{2^n} + a\}$

Proof Highlights (contd..)

n odd:

Proof Highlights (contd..)

n odd:

Claim: $h(u)$ is $1-1$ if and only if $a^{2^{n+1}} + a^2 + a^{2^n+1} = 0$.

Proof Highlights (contd..)

n odd:

Claim: $h(u)$ is $1-1$ if and only if $a^{2^{n+1}} + a^2 + a^{2^n+1} = 0$.

if: $a^{2^{n+1}} + a^2 + a^{2^n+1} = 0 \Rightarrow h(u) = u^3$ is $1-1$. ($\gcd(3, 2^n - 1) = 1$ for odd n).

Proof Highlights (contd..)

n odd:

Claim: $h(u)$ is $1-1$ if and only if $a^{2^{n+1}} + a^2 + a^{2^n+1} = 0$.

if: $a^{2^{n+1}} + a^2 + a^{2^n+1} = 0 \Rightarrow h(u) = u^3$ is $1-1$. ($\gcd(3, 2^n - 1) = 1$ for odd n).

Only if: $a^{2^{n+1}} + a^2 + a^{2^n+1} \neq 0$

Proof Highlights (contd..)

n odd:

Claim: $h(u)$ is $1-1$ if and only if $a^{2^{n+1}} + a^2 + a^{2^n+1} = 0$.

if: $a^{2^{n+1}} + a^2 + a^{2^n+1} = 0 \Rightarrow h(u) = u^3$ is $1-1$. ($\gcd(3, 2^n - 1) = 1$ for odd n).

Only if: $a^{2^{n+1}} + a^2 + a^{2^n+1} \neq 0 \Rightarrow h(u) = 0$ for $u = 0$ and $u = a^{2^n} + a + a^{2^{2n-1}+2^{n-1}}$,

Proof Highlights (contd..)

n odd:

Claim: $h(u)$ is $1-1$ if and only if $a^{2^{n+1}} + a^2 + a^{2^n+1} = 0$.

if: $a^{2^{n+1}} + a^2 + a^{2^n+1} = 0 \Rightarrow h(u) = u^3$ is $1-1$. ($\gcd(3, 2^n - 1) = 1$ for odd n).

Only if: $a^{2^{n+1}} + a^2 + a^{2^n+1} \neq 0 \Rightarrow h(u) = 0$ for $u = 0$ and
$u = a^{2^n} + a + a^{2^{2n-1}+2^{n-1}}$, $\Rightarrow g(v_1) = g(v_2)$ for $v_1 = a^{2^n} + a \in \mathbb{F}_{2^n}^*$ and
$v_2 = a^{2^{2n-1}+2^{n-1}} = \left(a^{2^n+1}\right)^{2^{n-1}} \in \mathbb{F}_{2^n}^*$.

Proof Highlights (contd..)

n odd:

Claim: $h(u)$ is $1-1$ if and only if $a^{2^{n+1}} + a^2 + a^{2^n+1} = 0$.

if: $a^{2^{n+1}} + a^2 + a^{2^n+1} = 0 \Rightarrow h(u) = u^3$ is $1-1$. ($\gcd(3, 2^n - 1) = 1$ for odd n).

Only if: $a^{2^{n+1}} + a^2 + a^{2^n+1} \neq 0 \Rightarrow h(u) = 0$ for $u = 0$ and
$u = a^{2^n} + a + a^{2^{2n-1}+2^{n-1}}$, $\Rightarrow g(v_1) = g(v_2)$ for $v_1 = a^{2^n} + a \in \mathbb{F}_{2^n}^*$ and
$v_2 = a^{2^{2n-1}+2^{n-1}} = \left(a^{2^n+1}\right)^{2^{n-1}} \in \mathbb{F}_{2^n}^*$.

Proof Highlights (contd..)

$a^{2^{n+1}} + a^2 + a^{2^n+1} = a^2((a^{2^n-1})^2 + a^{2^n-1} + 1)$.

Proof Highlights (contd..)

$a^{2^{n+1}} + a^2 + a^{2^n+1} = a^2((a^{2^n-1})^2 + a^{2^n-1} + 1)$.

$$\Downarrow$$

$a^{2^{n+1}} + a^2 + a^{2^n+1} = 0$ iff a^{2^n-1} is a root of the equation $y^2 + y + 1 = 0$ in $\mathbb{F}_{2^{2n}}$, i.e., $a^{2^n-1} \in \{\omega, \omega^2\}$.

Proof Highlights (contd..)

$a^{2^{n+1}} + a^2 + a^{2^n+1} = a^2((a^{2^n-1})^2 + a^{2^n-1} + 1)$.

$\Downarrow$

$a^{2^{n+1}} + a^2 + a^{2^n+1} = 0$ iff a^{2^n-1} is a root of the equation $y^2 + y + 1 = 0$ in $\mathbb{F}_{2^{2n}}$, i.e., $a^{2^n-1} \in \{\omega, \omega^2\}$.

***n* even:**

Proof Highlights (contd..)

$a^{2^{n+1}} + a^2 + a^{2^n+1} = a^2((a^{2^n-1})^2 + a^{2^n-1} + 1)$.

$$\Downarrow$$

$a^{2^{n+1}} + a^2 + a^{2^n+1} = 0$ iff a^{2^n-1} is a root of the equation $y^2 + y + 1 = 0$ in $\mathbb{F}_{2^{2n}}$, i.e., $a^{2^n-1} \in \{\omega, \omega^2\}$.

n even:

$a^{2^{n+1}} + a^2 + a^{2^n+1} \neq 0 \Rightarrow h(u)$ is not $1-1$ for $u \in \mathbb{F}_{2^n} \setminus \{a^{2^n} + a\}$.(argument same as above)

Proof Highlights (contd..)

$a^{2^{n+1}} + a^2 + a^{2^n+1} = a^2((a^{2^n-1})^2 + a^{2^n-1} + 1)$.

$\Downarrow$

$a^{2^{n+1}} + a^2 + a^{2^n+1} = 0$ iff a^{2^n-1} is a root of the equation $y^2 + y + 1 = 0$ in $\mathbb{F}_{2^{2n}}$, i.e., $a^{2^n-1} \in \{\omega, \omega^2\}$.

n even:

$a^{2^{n+1}} + a^2 + a^{2^n+1} \neq 0 \Rightarrow h(u)$ is not $1-1$ for $u \in \mathbb{F}_{2^n} \setminus \{a^{2^n} + a\}$.(argument same as above)

$a^{2^{n+1}} + a^2 + a^{2^n+1} = 0 \Rightarrow h(u) = u^3$ is not $1-1$.(for even n, $3 \mid 2^n - 1$)

Proof Highlights (contd..)

Corollary

Let n be odd, then $x^{2^n+2} + ax \in \mathbb{F}_{2^{2n}}[x]$ is a permutation polynomial if and only if $a \in \omega\mathbb{F}_{2^n}^* \bigcup \omega^2\mathbb{F}_{2^n}^*$ where $\omega^2 + \omega + 1 = 0$ in $\mathbb{F}_{2^{2n}}$. Hence the number of such a is exactly $2(2^n - 1)$

References I


L. Carlitz,
Some theorems on permutation polynomials,
Bull. Amer. Math. Soc. vol 68, Number 2 (1962), 120-122.


L. Carlitz and C. Wells,
The number of solutions of a special system of equations in a finite field,
Acta Arithmetica, vol 12, pp. 77–84, 1966.


P. Charpin and G. M. Kyureghyan,
Cubic monomial bent functions: a subclass of $\mathcal{M}^*$,
Siam J. Disc. Math., vol 22 (2), pp. 650–665, 2008.

References II


P. Charpin and S. Sarkar.
Polynomials with linear structure and Maiorana-McFarland construction,
In IEEE Trans. on Inf. Theory, Vol 57 (6), 3796–3804, 2011.


S. Dubuc.
Characterization of linear structures,
Des. Codes Cryptography vol. 22, pp. 33–45, 2001.


A. B. Evans.
Orthomorphism graphs of groups,
Lecture Notes in Mathematics, vol. 1535, Springer, Berlin, 1992.

References III


J. H. Evertse.
Linear structures in block ciphers, In Proc. of EUROCRYPT 87, Lecture Notes in Computer Science, Springer-Verlag, 304, pp. 249–266, 1988.


T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences. Discrete Math. 16 (3) (1976) 209–232.


Y. Laigle-Chapuy,
Permutation polynomials and applications to coding theory,
Finite Fields and Their Applications, vol 13, pp. 58–70, 2007.

References IV


R. Lidl and H. Niederreiter,
Finite Fields, Encyclopedia of Mathematics and its Applications.
vol. 20, second edition, Cambridge University Press, 1997.


A. M. Masuda and M. E. Zieve,
Permutation binomials over finite fields. Trans. of the American Mathematical Society. Volume 361 (8), pp 4169–4180, 2009.


H. Niederreiter and K. H. Robinson,
Complete mappings of finite fields.
J. Australian Math. Soc. Ser. A 33 (1982), 197-212.


H. Niederreiter and A. Winterhof,
Cyclotomic $\mathscr{R}$-orthomorphisms of finite fields.
Discrete Math, vol 295 (2005) 161–171.

References V

D. Q. Wan and R. Lidl.

Permutation polynomials of the form $x^r f(x^{\frac{q-1}{m}})$ and their group structure.

Monatsh. Math., Vol 112 (2), pp. 149–163, 1991.

G. Turnwald,

Permutation polynomials of binomial type.

Contributions to General Algebra, vol. 6, Teubner, Stuttgart, 1988, pp. 281-286.

Thank You!