Niho's Last Conjecture

Tor Helleseth*, Daniel J. Katz†, and Chunlei Li‡

*‡ Department of Informatics, University of Bergen, Norway

† Department of Mathematics, California State University, Northridge

*‡Supported by the Research Council of Norway
Grants No. 247742/O70 and No. 311646/O70

†Supported by National Science Foundation
Awards DMS-1500856 and CCF-1815487

‡Supported by National Natural Science Foundation of China
Grant No. 61771021

Fifth International Workshop on
Boolean Functions and their Applications (BFA 2020)
Loen, Norway
15 September 2020

In Memoriam

Hans Dobbertin

Petri Rosendahl

Power Permutations

Throughout the talk: $F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Power Permutations

Throughout the talk: $F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Power function on a finite field F: a function $f\colon F \to F$ with $f(x) = x^d$ for some positive integer d

Power Permutations

Throughout the talk: $F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Power function on a finite field F: a function $f\colon F \to F$ with $f(x) = x^d$ for some positive integer d

Power permutation of F: a power function $f(x) = x^d$ on F is a permutation of F if and only if $\gcd(d, |F^*|) = 1$

Power Permutations

Throughout the talk: $F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Power function on a finite field F: a function $f\colon F \to F$ with $f(x) = x^d$ for some positive integer d

Power permutation of F: a power function $f(x) = x^d$ on F is a permutation of F if and only if $\gcd(d, |F^*|) = 1$

If $\gcd(d, |F^*|) = 1$, we say that d is an invertible exponent over F: if $e = 1/d \pmod{|F^*|}$, then $x \mapsto x^e$ is the inverse function of $x \mapsto x^d$

Power Permutations

Throughout the talk: $F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Power function on a finite field F: a function $f\colon F \to F$ with $f(x) = x^d$ for some positive integer d

Power permutation of F: a power function $f(x) = x^d$ on F is a permutation of F if and only if $\gcd(d, |F^*|) = 1$

If $\gcd(d, |F^*|) = 1$, we say that d is an invertible exponent over F: if $e = 1/d \pmod{|F^*|}$, then $x \mapsto x^e$ is the inverse function of $x \mapsto x^d$

Cryptographic significance: arithmetically easy to implement power permutations within cryptosystems

Power Permutations

Throughout the talk: $F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Power function on a finite field F: a function $f\colon F \to F$ with $f(x) = x^d$ for some positive integer d

Power permutation of F: a power function $f(x) = x^d$ on F is a permutation of F if and only if $\gcd(d, |F^*|) = 1$

If $\gcd(d, |F^*|) = 1$, we say that d is an invertible exponent over F: if $e = 1/d \pmod{|F^*|}$, then $x \mapsto x^e$ is the inverse function of $x \mapsto x^d$

Cryptographic significance: arithmetically easy to implement power permutations within cryptosystems

Want power permutations that are resistant to linear cryptanalysis

Linear Functionals

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Linear Functionals

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Let $\mathrm{Tr}\colon F \to \mathbb{F}_p$ be the absolute trace:

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{n-1}}$$

Linear Functionals

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Let $\mathrm{Tr}\colon F \to \mathbb{F}_p$ be the absolute trace:

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{n-1}}$$

Then for any $c \in F$, we have an $\mathbb{F}_p$-linear functional:

$$\begin{aligned} F &\to \mathbb{F}_p \\ x &\mapsto \mathrm{Tr}(cx) \end{aligned}$$

Linear Functionals

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Let $\mathrm{Tr}\colon F \to \mathbb{F}_p$ be the absolute trace:

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{n-1}}$$

Then for any $c \in F$, we have an $\mathbb{F}_p$-linear functional:

$$\begin{aligned} F &\to \mathbb{F}_p \\ x &\mapsto \mathrm{Tr}(cx) \end{aligned}$$

Every $\mathbb{F}_p$-linear functional of F is uniquely represented in this way

Linear Functionals

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Let $\mathrm{Tr}\colon F \to \mathbb{F}_p$ be the absolute trace:

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{n-1}}$$

Then for any $c \in F$, we have an $\mathbb{F}_p$-linear functional:

$$\begin{aligned} F &\to \mathbb{F}_p \\ x &\mapsto \mathrm{Tr}(cx) \end{aligned}$$

Every $\mathbb{F}_p$-linear functional of F is uniquely represented in this way

If $c_1, \ldots, c_n$ form an $\mathbb{F}_p$-basis of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$, then we have the $\mathbb{F}_p$-linear isomorphism:

$$\begin{aligned} F &\to \mathbb{F}_p^n \\ x &\mapsto (\mathrm{Tr}(c_1 x), \ldots, \mathrm{Tr}(c_n x)), \end{aligned}$$

Linear Functionals

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field of characteristic p and order $q = p^n$

Let $\mathrm{Tr}\colon F \to \mathbb{F}_p$ be the absolute trace:

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{n-1}}$$

Then for any $c \in F$, we have an $\mathbb{F}_p$-linear functional:

$$\begin{aligned} F &\to \mathbb{F}_p \\ x &\mapsto \mathrm{Tr}(cx) \end{aligned}$$

Every $\mathbb{F}_p$-linear functional of F is uniquely represented in this way

If $c_1, \ldots, c_n$ form an $\mathbb{F}_p$-basis of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$, then we have the $\mathbb{F}_p$-linear isomorphism:

$$\begin{aligned} F &\to \mathbb{F}_p^n \\ x &\mapsto (\mathrm{Tr}(c_1 x), \ldots, \mathrm{Tr}(c_n x)), \end{aligned}$$

So we call our $\mathbb{F}_p$-linear functionals $x \mapsto \mathrm{Tr}(cx)$ (with $c \neq 0$) component linear functionals

Nonlinearity

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ has absolute trace $\mathrm{Tr}\colon F \to \mathbb{F}_p$

Nonlinearity

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ has absolute trace $\mathrm{Tr}\colon F \to \mathbb{F}_p$

If $f\colon F \to F$, then for each $b \in F^*$, we get a component function of f:

$$\begin{aligned} F &\to \mathbb{F}_p \\ x &\mapsto \mathrm{Tr}(bf(x)) \end{aligned}$$

Nonlinearity

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ has absolute trace $\mathrm{Tr}\colon F \to \mathbb{F}_p$

If $f\colon F \to F$, then for each $b \in F^*$, we get a component function of f:

$$\begin{aligned} F &\to \mathbb{F}_p \\ x &\mapsto \mathrm{Tr}(bf(x)) \end{aligned}$$

To resist linear cryptanalysis: want component functions $\mathrm{Tr}(bf(x))$ of f uncorrelated with the linear functionals $x \mapsto \mathrm{Tr}(cx)$ (for all $c \in F$)

Nonlinearity

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ has absolute trace $\mathrm{Tr}\colon F \to \mathbb{F}_p$

If $f\colon F \to F$, then for each $b \in F^*$, we get a component function of f:

$$\begin{aligned} F &\to \mathbb{F}_p \\ x &\mapsto \mathrm{Tr}(bf(x)) \end{aligned}$$

To resist linear cryptanalysis: want component functions $\mathrm{Tr}(bf(x))$ of f uncorrelated with the linear functionals $x \mapsto \mathrm{Tr}(cx)$ (for all $c \in F$)

When $p = 2$, $\displaystyle\sum_{x \in F} (-1)^{\mathrm{Tr}(bf(x)) - \mathrm{Tr}(cx)}$

$= \#$ of agreements between $\mathrm{Tr}(bf(x))$ and $\mathrm{Tr}(cx)$

$- \#$ of disagreements between $\mathrm{Tr}(bf(x))$ and $\mathrm{Tr}(cx)$

Nonlinearity

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ has absolute trace $\mathrm{Tr}\colon F \to \mathbb{F}_p$

If $f\colon F \to F$, then for each $b \in F^*$, we get a component function of f:

$$\begin{aligned} F &\to \mathbb{F}_p \\ x &\mapsto \mathrm{Tr}(bf(x)) \end{aligned}$$

To resist linear cryptanalysis: want component functions $\mathrm{Tr}(bf(x))$ of f uncorrelated with the linear functionals $x \mapsto \mathrm{Tr}(cx)$ (for all $c \in F$)

When $p = 2$, $\sum_{x \in F} (-1)^{\mathrm{Tr}(bf(x)) - \mathrm{Tr}(cx)}$

$$\begin{aligned} &= \#\text{ of agreements between } \mathrm{Tr}(bf(x)) \text{ and } \mathrm{Tr}(cx) \\ &\quad - \#\text{ of disagreements between } \mathrm{Tr}(bf(x)) \text{ and } \mathrm{Tr}(cx) \end{aligned}$$

Notice: $x \mapsto (-1)^{\mathrm{Tr}(x)}$ is the canonical additive character of F into $\{\pm 1\} \subseteq \mathbb{C}^*$ (when F is characteristic 2)

Walsh Transform

If F has characteristic 2, want $\sum_{x \in F}(-1)^{\mathrm{Tr}(bf(x))-\mathrm{Tr}(cx)}$ to be close to 0

Walsh Transform

If F has characteristic 2, want $\sum_{x \in F} (-1)^{\mathrm{Tr}(bf(x)) - \mathrm{Tr}(cx)}$ to be close to 0

For F of arbitrary characteristic p, let $\zeta_p = \exp(2\pi i/p)$ and then define the canonical additive character of F to be

$$\psi_F : F \to \langle \zeta_p \rangle \subseteq \mathbb{C}^*$$
$$\psi_F(x) = \zeta_p^{\mathrm{Tr}(x)} = \zeta_p^{x + x^p + \cdots + x^{q/p}}$$

Walsh Transform

If F has characteristic 2, want $\sum_{x \in F}(-1)^{\mathrm{Tr}(bf(x)) - \mathrm{Tr}(cx)}$ to be close to 0

For F of arbitrary characteristic p, let $\zeta_p = \exp(2\pi i/p)$ and then define the canonical additive character of F to be

$$\psi_F : F \to \langle \zeta_p \rangle \subseteq \mathbb{C}^*$$
$$\psi_F(x) = \zeta_p^{\mathrm{Tr}(x)} = \zeta_p^{x + x^p + \cdots + x^{q/p}}$$

We define the Walsh Transform of f to be the function

$$W_f : F \times F \to \mathbb{C}$$
$$W_f(b, c) = \sum_{x \in F} \psi_F(bf(x) - cx) = \sum_{x \in F} \zeta_p^{\mathrm{Tr}(bf(x)) - \mathrm{Tr}(cx)}$$

Walsh Transform

If F has characteristic 2, want $\sum_{x\in F}(-1)^{\mathrm{Tr}(bf(x))-\mathrm{Tr}(cx)}$ to be close to 0

For F of arbitrary characteristic p, let $\zeta_p = \exp(2\pi i/p)$ and then define the canonical additive character of F to be

$$\psi_F : F \to \langle \zeta_p \rangle \subseteq \mathbb{C}^*$$
$$\psi_F(x) = \zeta_p^{\mathrm{Tr}(x)} = \zeta_p^{x+x^p+\cdots+x^{q/p}}$$

We define the Walsh Transform of f to be the function

$$W_f : F \times F \to \mathbb{C}$$
$$W_f(b,c) = \sum_{x\in F} \psi_F(bf(x) - cx) = \sum_{x\in F} \zeta_p^{\mathrm{Tr}(bf(x))-\mathrm{Tr}(cx)}$$

And we define the Walsh Spectrum of f to be $\{W_f(b,c) : b \in F^*, c \in F\}$ ($b = 0$ tells us nothing about f)

Walsh Transform

If F has characteristic 2, want $\sum_{x \in F} (-1)^{\mathrm{Tr}(bf(x)) - \mathrm{Tr}(cx)}$ to be close to 0

For F of arbitrary characteristic p, let $\zeta_p = \exp(2\pi i/p)$ and then define the canonical additive character of F to be

$$\psi_F : F \to \langle \zeta_p \rangle \subseteq \mathbb{C}^*$$
$$\psi_F(x) = \zeta_p^{\mathrm{Tr}(x)} = \zeta_p^{x + x^p + \cdots + x^{q/p}}$$

We define the Walsh Transform of f to be the function

$$W_f : F \times F \to \mathbb{C}$$
$$W_f(b, c) = \sum_{x \in F} \psi_F(bf(x) - cx) = \sum_{x \in F} \zeta_p^{\mathrm{Tr}(bf(x)) - \mathrm{Tr}(cx)}$$

And we define the Walsh Spectrum of f to be $\{W_f(b, c) : b \in F^*, c \in F\}$ ($b = 0$ tells us nothing about f)

Want every element of this spectrum to have small magnitude

Walsh Spectrum of a Power Permutation

$\psi_F \colon F \to \mathbb{C}^*$ is the canonical additive character of F

Walsh Spectrum of a Power Permutation

$\psi_F \colon F \to \mathbb{C}^*$ is the canonical additive character of F

$f(x) = x^d$ is a power permutation of F (so $\gcd(d, |F^*|) = 1$)

Walsh Spectrum of a Power Permutation

$\psi_F \colon F \to \mathbb{C}^*$ is the canonical additive character of F

$f(x) = x^d$ is a power permutation of F (so $\gcd(d, |F^*|) = 1$)

For $b \in F^*, c \in F$, the Walsh transform is

$$W_f(b,c) = \sum_{x \in F} \psi_F(bx^d - cx),$$

which is a Weil sum of a binomial

Walsh Spectrum of a Power Permutation

$\psi_F \colon F \to \mathbb{C}^*$ is the canonical additive character of F

$f(x) = x^d$ is a power permutation of F (so $\gcd(d, |F^*|) = 1$)

For $b \in F^*, c \in F$, the Walsh transform is

$$W_f(b, c) = \sum_{x \in F} \psi_F(bx^d - cx),$$

which is a Weil sum of a binomial, which can be reparameterized with $y = b^{1/d} x$

$$W_f(b, c) = \sum_{y \in F} \psi_F(y^d - cb^{-1/d} y) = W_f(1, b^{-1/d} c)$$

Walsh Spectrum of a Power Permutation

$\psi_F \colon F \to \mathbb{C}^*$ is the canonical additive character of F

$f(x) = x^d$ is a power permutation of F (so $\gcd(d, |F^*|) = 1$)

For $b \in F^*, c \in F$, the Walsh transform is

$$W_f(b, c) = \sum_{x \in F} \psi_F(bx^d - cx),$$

which is a Weil sum of a binomial, which can be reparameterized with $y = b^{1/d}x$

$$W_f(b, c) = \sum_{y \in F} \psi_F(y^d - cb^{-1/d}y) = W_f(1, b^{-1/d}c)$$

So define

$$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax),$$

Walsh Spectrum of a Power Permutation

$\psi_F \colon F \to \mathbb{C}^*$ is the canonical additive character of F

$f(x) = x^d$ is a power permutation of F (so $\gcd(d, |F^*|) = 1$)

For $b \in F^*, c \in F$, the Walsh transform is

$$W_f(b,c) = \sum_{x \in F} \psi_F(bx^d - cx),$$

which is a Weil sum of a binomial, which can be reparameterized with $y = b^{1/d}x$

$$W_f(b,c) = \sum_{y \in F} \psi_F(y^d - cb^{-1/d}y) = W_f(1, b^{-1/d}c)$$

So define

$$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax),$$

and then the Walsh spectrum of $f(x) = x^d$ over F is

$$\{W_{F,d}(a) : a \in F\}$$

Weil Spectrum and Crosscorrelation

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$ is a Weil sum

$\{W_{F,d}(a) : a \in F\}$ is the Walsh spectrum of f

Weil Spectrum and Crosscorrelation

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$ is a Weil sum

$\{W_{F,d}(a) : a \in F\}$ is the Walsh spectrum of f

Notice that $W_{F,d}(0) = \sum_{x \in F} \psi_F(x^d) = \sum_{y \in F} \psi_F(y) = 0$

Weil Spectrum and Crosscorrelation

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$ is a Weil sum

$\{W_{F,d}(a) : a \in F\}$ is the Walsh spectrum of f

Notice that $W_{F,d}(0) = \sum_{x \in F} \psi_F(x^d) = \sum_{y \in F} \psi_F(y) = 0$

Weil spectrum for $f(x) = x^d$ over F is $\{W_{F,d}(a) : a \in F^*\}$.

Weil Spectrum and Crosscorrelation

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$ is a Weil sum

$\{W_{F,d}(a) : a \in F\}$ is the Walsh spectrum of f

Notice that $W_{F,d}(0) = \sum_{x \in F} \psi_F(x^d) = \sum_{y \in F} \psi_F(y) = 0$

Weil spectrum for $f(x) = x^d$ over F is $\{W_{F,d}(a) : a \in F^*\}$.

The Weil spectrum gives the crosscorrelation spectrum for a pair of p-ary maximum length linear feedback shift register sequences (m-sequences) of period $q - 1 = |F^*|$

Weil Spectrum and Crosscorrelation

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$
$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$ is a Weil sum
$\{W_{F,d}(a) : a \in F\}$ is the Walsh spectrum of f

Notice that $W_{F,d}(0) = \sum_{x \in F} \psi_F(x^d) = \sum_{y \in F} \psi_F(y) = 0$

Weil spectrum for $f(x) = x^d$ over F is $\{W_{F,d}(a) : a \in F^*\}$.

The Weil spectrum gives the crosscorrelation spectrum for a pair of p-ary maximum length linear feedback shift register sequences (m-sequences) of period $q - 1 = |F^*|$

One m-sequence comes from the other by decimating by d

Weil Spectrum and Crosscorrelation

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$ is a Weil sum

$\{W_{F,d}(a) : a \in F\}$ is the Walsh spectrum of f

Notice that $W_{F,d}(0) = \sum_{x \in F} \psi_F(x^d) = \sum_{y \in F} \psi_F(y) = 0$

Weil spectrum for $f(x) = x^d$ over F is $\{W_{F,d}(a) : a \in F^*\}$.

The Weil spectrum gives the crosscorrelation spectrum for a pair of p-ary maximum length linear feedback shift register sequences (m-sequences) of period $q - 1 = |F^*|$

One m-sequence comes from the other by decimating by d

The values of the periodic crosscorrelations between these sequences for the $q - 1$ relative shifts equal $-1 + W_{F,d}(a)$ for the $q - 1$ different $a \in F^*$.

Equivalence and Degeneracy

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$

Equivalence and Degeneracy

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$

The power permutation $g(x) = x^{d'}$ produces the same Weil spectrum as $f(x) = x^d$ when

Equivalence and Degeneracy

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$

The power permutation $g(x) = x^{d'}$ produces the same Weil spectrum as $f(x) = x^d$ when

- $d' \equiv d \pmod{|F^*|}$, because $x^{d'} = x^d$ for every $x \in F$

Equivalence and Degeneracy

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$

The power permutation $g(x) = x^{d'}$ produces the same Weil spectrum as $f(x) = x^d$ when

- $d' \equiv d \pmod{|F^*|}$, because $x^{d'} = x^d$ for every $x \in F$
- $d' = pd$, because $\mathrm{Tr}(x^{pd}) = \mathrm{Tr}(x^d)$, so $\psi_F(x^{pd}) = \psi_F(x^d)$

Equivalence and Degeneracy

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$
$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$

The power permutation $g(x) = x^{d'}$ produces the same Weil spectrum as $f(x) = x^d$ when

- $d' \equiv d \pmod{|F^*|}$, because $x^{d'} = x^d$ for every $x \in F$
- $d' = pd$, because $\mathrm{Tr}(x^{pd}) = \mathrm{Tr}(x^d)$, so $\psi_F(x^{pd}) = \psi_F(x^d)$
- d' is the inverse of d modulo $|F^*|$

Equivalence and Degeneracy

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$

The power permutation $g(x) = x^{d'}$ produces the same Weil spectrum as $f(x) = x^d$ when

- $d' \equiv d \pmod{|F^*|}$, because $x^{d'} = x^d$ for every $x \in F$
- $d' = pd$, because $\mathrm{Tr}(x^{pd}) = \mathrm{Tr}(x^d)$, so $\psi_F(x^{pd}) = \psi_F(x^d)$
- d' is the inverse of d modulo $|F^*|$

Thus we declare an exponent d' to be equivalent to d over F if $d' \equiv p^k d \pmod{|F^*|}$ or $d' \equiv p^k/d \pmod{|F^*|}$ for some $k \in \mathbb{Z}$

Equivalence and Degeneracy

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$

The power permutation $g(x) = x^{d'}$ produces the same Weil spectrum as $f(x) = x^d$ when

- $d' \equiv d \pmod{|F^*|}$, because $x^{d'} = x^d$ for every $x \in F$
- $d' = pd$, because $\mathrm{Tr}(x^{pd}) = \mathrm{Tr}(x^d)$, so $\psi_F(x^{pd}) = \psi_F(x^d)$
- d' is the inverse of d modulo $|F^*|$

Thus we declare an exponent d' to be equivalent to d over F if $d' \equiv p^k d \pmod{|F^*|}$ or $d' \equiv p^k/d \pmod{|F^*|}$ for some $k \in \mathbb{Z}$

If d is equivalent to 1 (i.e., a power of p modulo $q-1$), then

$$W_{F,d}(a) = W_{F,1}(a) = \sum_{x \in F} \psi_F(x^1 - ax) = \begin{cases} |F| & \text{if } a = 1 \\ 0 & \text{otherwise} \end{cases}$$

Equivalence and Degeneracy

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$

The power permutation $g(x) = x^{d'}$ produces the same Weil spectrum as $f(x) = x^d$ when

- $d' \equiv d \pmod{|F^*|}$, because $x^{d'} = x^d$ for every $x \in F$
- $d' = pd$, because $\mathrm{Tr}(x^{pd}) = \mathrm{Tr}(x^d)$, so $\psi_F(x^{pd}) = \psi_F(x^d)$
- d' is the inverse of d modulo $|F^*|$

Thus we declare an exponent d' to be equivalent to d over F if $d' \equiv p^k d \pmod{|F^*|}$ or $d' \equiv p^k/d \pmod{|F^*|}$ for some $k \in \mathbb{Z}$

If d is equivalent to 1 (i.e., a power of p modulo $q-1$), then

$$W_{F,d}(a) = W_{F,1}(a) = \sum_{x \in F} \psi_F(x^1 - ax) = \begin{cases} |F| & \text{if } a = 1 \\ 0 & \text{otherwise} \end{cases}$$

So the Walsh spectrum is $\{0, |F|\}$ and we say that d and $f(x) = x^d$ are degenerate over F

Degeneracy and Number of Values

$$f(x) = x^d \text{ is a power permutation of } F = \mathbb{F}_q = \mathbb{F}_{p^n}$$

$$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$$

$$\text{If } d \text{ is degenerate, then } W_{F,d}(a) = \begin{cases} |F| & \text{if } a = 1 \\ 0 & \text{otherwise} \end{cases}$$

Degeneracy and Number of Values

$$f(x) = x^d \text{ is a power permutation of } F = \mathbb{F}_q = \mathbb{F}_{p^n}$$

$$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$$

$$\text{If } d \text{ is degenerate, then } W_{F,d}(a) = \begin{cases} |F| & \text{if } a = 1 \\ 0 & \text{otherwise} \end{cases}$$

So the Weil spectrum $\{W_{F,d}(a) : a \in F^*\}$ has two values if d is degenerate and $|F| > 2$ (and only one value if $|F| = 2$)

Degeneracy and Number of Values

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$

If d is degenerate, then $W_{F,d}(a) = \begin{cases} |F| & \text{if } a = 1 \\ 0 & \text{otherwise} \end{cases}$

So the Weil spectrum $\{W_{F,d}(a) : a \in F^*\}$ has two values if d is degenerate and $|F| > 2$ (and only one value if $|F| = 2$)

Helleseth (1976): Weil spectrum of power permutation has at least three distinct values when d is nondegenerate

Degeneracy and Number of Values

$f(x) = x^d$ is a power permutation of $F = \mathbb{F}_q = \mathbb{F}_{p^n}$

$$W_{F,d}(a) = \sum_{x \in F} \psi_F(x^d - ax)$$

If d is degenerate, then $W_{F,d}(a) = \begin{cases} |F| & \text{if } a = 1 \\ 0 & \text{otherwise} \end{cases}$

So the Weil spectrum $\{W_{F,d}(a) : a \in F^*\}$ has two values if d is degenerate and $|F| > 2$ (and only one value if $|F| = 2$)

Helleseth (1976): Weil spectrum of power permutation has at least three distinct values when d is nondegenerate

Research has often focused on F and d that produce Weil spectra with few distinct values (e.g., 3, 4, or 5) and with values of small magnitude (not much larger than $\sqrt{|F|}$)

Niho Exponents

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a field of characteristic p and order $q = p^n$

Niho Exponents

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a field of characteristic p and order $q = p^n$

If F is of even degree over $\mathbb{F}_p$ (i.e., $n = 2m$ for some positive integer m), then we define the half field of F, written H_F, to be the unique subfield of index 2 in F

Niho Exponents

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a field of characteristic p and order $q = p^n$

If F is of even degree over $\mathbb{F}_p$ (i.e., $n = 2m$ for some positive integer m), then we define the half field of F, written H_F, to be the unique subfield of index 2 in F

So $H_F = \mathbb{F}_{p^{n/2}} = \mathbb{F}_{p^m}$ and $|H_F| = \sqrt{|F|}$

Niho Exponents

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a field of characteristic p and order $q = p^n$

If F is of even degree over $\mathbb{F}_p$ (i.e., $n = 2m$ for some positive integer m), then we define the half field of F, written H_F, to be the unique subfield of index 2 in F

So $H_F = \mathbb{F}_{p^{n/2}} = \mathbb{F}_{p^m}$ and $|H_F| = \sqrt{|F|}$

A Niho exponent over F is a positive integer d that is nondegenerate over F but is degenerate over H_F, so

Niho Exponents

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a field of characteristic p and order $q = p^n$

If F is of even degree over $\mathbb{F}_p$ (i.e., $n = 2m$ for some positive integer m), then we define the half field of F, written H_F, to be the unique subfield of index 2 in F

So $H_F = \mathbb{F}_{p^{n/2}} = \mathbb{F}_{p^m}$ and $|H_F| = \sqrt{|F|}$

A Niho exponent over F is a positive integer d that is nondegenerate over F but is degenerate over H_F, so

- d is not a power of p modulo $|F^*| = p^n - 1$, but

Niho Exponents

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a field of characteristic p and order $q = p^n$

If F is of even degree over $\mathbb{F}_p$ (i.e., $n = 2m$ for some positive integer m), then we define the half field of F, written H_F, to be the unique subfield of index 2 in F

So $H_F = \mathbb{F}_{p^{n/2}} = \mathbb{F}_{p^m}$ and $|H_F| = \sqrt{|F|}$

A Niho exponent over F is a positive integer d that is nondegenerate over F but is degenerate over H_F, so

- d is not a power of p modulo $|F^*| = p^n - 1$, but
- d is a power of p modulo $|H_F^*| = p^{n/2} - 1 = p^m - 1$

Niho Exponents

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a field of characteristic p and order $q = p^n$

If F is of even degree over $\mathbb{F}_p$ (i.e., $n = 2m$ for some positive integer m), then we define the half field of F, written H_F, to be the unique subfield of index 2 in F

So $H_F = \mathbb{F}_{p^{n/2}} = \mathbb{F}_{p^m}$ and $|H_F| = \sqrt{|F|}$

A Niho exponent over F is a positive integer d that is nondegenerate over F but is degenerate over H_F, so

- d is not a power of p modulo $|F^*| = p^n - 1$, but
- d is a power of p modulo $|H_F^*| = p^{n/2} - 1 = p^m - 1$

Up to equivalence, we may assume that a Niho exponent d has $d \equiv 1 \pmod{|H_F^*|}$, so there is some integer $s \geq 2$ such that

$$d = 1 + s|H_F^*| = 1 + s(p^m - 1)$$

Niho Exponents

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a field of characteristic p and order $q = p^n$

If F is of even degree over $\mathbb{F}_p$ (i.e., $n = 2m$ for some positive integer m), then we define the half field of F, written H_F, to be the unique subfield of index 2 in F

So $H_F = \mathbb{F}_{p^{n/2}} = \mathbb{F}_{p^m}$ and $|H_F| = \sqrt{|F|}$

A Niho exponent over F is a positive integer d that is nondegenerate over F but is degenerate over H_F, so

- d is not a power of p modulo $|F^*| = p^n - 1$, but
- d is a power of p modulo $|H_F^*| = p^{n/2} - 1 = p^m - 1$

Up to equivalence, we may assume that a Niho exponent d has $d \equiv 1 \pmod{|H_F^*|}$, so there is some integer $s \geq 2$ such that

$$d = 1 + s|H_F^*| = 1 + s(p^m - 1)$$

Then d is invertible over F if and only if $\gcd(2s - 1, p^m + 1) = 1$

Niho Exponents

$F = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a field of characteristic p and order $q = p^n$

If F is of even degree over $\mathbb{F}_p$ (i.e., $n = 2m$ for some positive integer m), then we define the half field of F, written H_F, to be the unique subfield of index 2 in F

So $H_F = \mathbb{F}_{p^{n/2}} = \mathbb{F}_{p^m}$ and $|H_F| = \sqrt{|F|}$

A Niho exponent over F is a positive integer d that is nondegenerate over F but is degenerate over H_F, so

- d is not a power of p modulo $|F^*| = p^n - 1$, but
- d is a power of p modulo $|H_F^*| = p^{n/2} - 1 = p^m - 1$

Up to equivalence, we may assume that a Niho exponent d has $d \equiv 1 \pmod{|H_F^*|}$, so there is some integer $s \geq 2$ such that

$$d = 1 + s|H_F^*| = 1 + s(p^m - 1)$$

Then d is invertible over F if and only if $\gcd(2s - 1, p^m + 1) = 1$

Niho exponents can give Weil spectra with few distinct values

Weil Spectra for Some Niho Exponents ($s = 2$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$
and $d = 1 + s(p^m - 1)$ is a Niho exponent

Weil Spectra for Some Niho Exponents ($s = 2$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$ and $d = 1 + s(p^m - 1)$ is a Niho exponent

---

- $s = 2$ produces $d = 1 + 2(p^m - 1)$

Weil Spectra for Some Niho Exponents ($s = 2$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$ and $d = 1 + s(p^m - 1)$ is a Niho exponent

---

- $s = 2$ produces $d = 1 + 2(p^m - 1)$

  This is invertible over F if and only if $p^m \not\equiv 2 \pmod 3$

Weil Spectra for Some Niho Exponents ($s = 2$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$
and $d = 1 + s(p^m - 1)$ is a Niho exponent

- $s = 2$ produces $d = 1 + 2(p^m - 1)$

  This is invertible over F if and only if $p^m \not\equiv 2 \pmod{3}$

  So when $p = 2$, invertible over F if and only if m is even

Weil Spectra for Some Niho Exponents ($s = 2$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$ and $d = 1 + s(p^m - 1)$ is a Niho exponent

---

- $s = 2$ produces $d = 1 + 2(p^m - 1)$

  This is invertible over F if and only if $p^m \not\equiv 2 \pmod 3$

  So when $p = 2$, invertible over F if and only if m is even

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 2(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} = \{-2^m, 0, 2^m, 2 \cdot 2^m\}.$$

Weil Spectra for Some Niho Exponents ($s = 2$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$
and $d = 1 + s(p^m - 1)$ is a Niho exponent

- $s = 2$ produces $d = 1 + 2(p^m - 1)$

  This is invertible over F if and only if $p^m \not\equiv 2 \pmod 3$

  So when $p = 2$, invertible over F if and only if m is even

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 2(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} = \{-2^m, 0, 2^m, 2 \cdot 2^m\}.$$

So the Weil spectrum is 4-valued

Weil Spectra for Some Niho Exponents ($s = 3$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$
and $d = 1 + s(p^m - 1)$ is a Niho exponent

Weil Spectra for Some Niho Exponents ($s = 3$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$
and $d = 1 + s(p^m - 1)$ is a Niho exponent

- $s = 3$ produces $d = 1 + 3(p^m - 1)$, which is invertible over F if and only if $p^m \not\equiv 4 \pmod{5}$
  (so for $p = 2$, if and only if $m \not\equiv 2 \pmod{4}$)

Weil Spectra for Some Niho Exponents ($s = 3$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$ and $d = 1 + s(p^m - 1)$ is a Niho exponent

---

- $s = 3$ produces $d = 1 + 3(p^m - 1)$, which is invertible over F if and only if $p^m \not\equiv 4 \pmod 5$
  (so for $p = 2$, if and only if $m \not\equiv 2 \pmod 4$)

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$, $m \not\equiv 2 \pmod 4$, *and* $d = 1 + 3(2^m - 1)$, *then*

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 3 \cdot 2^m, 4 \cdot 2^m\}.$$

Weil Spectra for Some Niho Exponents ($s = 3$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$ and $d = 1 + s(p^m - 1)$ is a Niho exponent

---

- $s = 3$ produces $d = 1 + 3(p^m - 1)$, which is invertible over F if and only if $p^m \not\equiv 4 \pmod 5$

  (so for $p = 2$, if and only if $m \not\equiv 2 \pmod 4$)

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$, $m \not\equiv 2 \pmod 4$, and $d = 1 + 3(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 3 \cdot 2^m, 4 \cdot 2^m\}.$$

Building on work of Dobbertin, Felke, Helleseth, Rosendahl (2006), the exact values in the spectrum were determined.

Theorem (Xia-Li-Zeng-Helleseth, 2016)

If $F = \mathbb{F}_{2^{2m}}$, $m \not\equiv 2 \pmod 4$, $m \geq 3$, and $d = 1 + 3(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} = \{-2^m, 0, 2^m, 2 \cdot 2^m, 4 \cdot 2^m\} \quad \text{if } m \text{ is even,}$$

$$\{W_{F,d}(a) : a \in F^*\} = \{-2^m, 0, 2^m, 2 \cdot 2^m, 3 \cdot 2^m, 4 \cdot 2^m\} \quad \text{if } m \text{ is odd.}$$

Weil Spectra for Some Niho Exponents ($s = 4$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$ and $d = 1 + s(p^m - 1)$ is a Niho exponent

Weil Spectra for Some Niho Exponents ($s = 4$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$ and $d = 1 + s(p^m - 1)$ is a Niho exponent

- $s = 4$ produces $d = 1 + 4(p^m - 1)$, which is invertible over F if and only if $p^m \not\equiv 6 \pmod 7$

  (so for $p = 2$, always invertible over F)

Weil Spectra for Some Niho Exponents ($s = 4$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$
and $d = 1 + s(p^m - 1)$ is a Niho exponent

- $s = 4$ produces $d = 1 + 4(p^m - 1)$, which is invertible over F if and only if $p^m \not\equiv 6 \pmod 7$

  (so for $p = 2$, always invertible over F)

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$ and $d = 1 + 4(2^m - 1)$, then

$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2\cdot 2^m, 3\cdot 2^m, 4\cdot 2^m, 5\cdot 2^m, 6\cdot 2^m\}$.

Weil Spectra for Some Niho Exponents ($s = 4$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$
and $d = 1 + s(p^m - 1)$ is a Niho exponent

- $s = 4$ produces $d = 1 + 4(p^m - 1)$, which is invertible over F if and only if $p^m \not\equiv 6 \pmod 7$

  (so for $p = 2$, always invertible over F)

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$ and $d = 1 + 4(2^m - 1)$, then

$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2\cdot 2^m, 3\cdot 2^m, 4\cdot 2^m, 5\cdot 2^m, 6\cdot 2^m\}$.

So there are at most 8 distinct values.

Weil Spectra for Some Niho Exponents ($s = 4$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$ and $d = 1 + s(p^m - 1)$ is a Niho exponent

- $s = 4$ produces $d = 1 + 4(p^m - 1)$, which is invertible over F if and only if $p^m \not\equiv 6 \pmod 7$

  (so for $p = 2$, always invertible over F)

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$ *and* $d = 1 + 4(2^m - 1)$, *then*

$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2\cdot 2^m, 3\cdot 2^m, 4\cdot 2^m, 5\cdot 2^m, 6\cdot 2^m\}$.

So there are at most 8 distinct values. The very last conjecture in Niho's thesis concerns this spectrum when m is even.

Weil Spectra for Some Niho Exponents ($s = 4$)

$F = \mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_{p^{2m}}$ is a field of characteristic p and order $q = p^n$ and $d = 1 + s(p^m - 1)$ is a Niho exponent

- $s = 4$ produces $d = 1 + 4(p^m - 1)$, which is invertible over F if and only if $p^m \not\equiv 6 \pmod 7$

  (so for $p = 2$, always invertible over F)

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$ and $d = 1 + 4(2^m - 1)$, then

$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2\cdot 2^m, 3\cdot 2^m, 4\cdot 2^m, 5\cdot 2^m, 6\cdot 2^m\}$.

So there are at most 8 distinct values. The very last conjecture in Niho's thesis concerns this spectrum when m is even.

Niho's Last Conjecture (1972)

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 4(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \text{ contains at most 5 distinct values.}$$

The New Result

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$ *and* $d = 1 + 4(2^m - 1)$*, then*

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 3 \cdot 2^m, 4 \cdot 2^m, 5 \cdot 2^m, 6 \cdot 2^m\}.$$

Niho's Last Conjecture (1972)

If $F = \mathbb{F}_{2^{2m}}$*,* m *is even, and* $d = 1 + 4(2^m - 1)$*, then*

$\{W_{F,d}(a) : a \in F^*\}$ *contains at most* 5 *distinct values.*

The New Result

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$ *and* $d = 1 + 4(2^m - 1)$, *then*

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 3 \cdot 2^m, 4 \cdot 2^m, 5 \cdot 2^m, 6 \cdot 2^m\}.$$

Niho's Last Conjecture (1972)

If $F = \mathbb{F}_{2^{2m}}$, m *is even, and* $d = 1 + 4(2^m - 1)$, *then*

$\{W_{F,d}(a) : a \in F^*\}$ *contains at most* 5 *distinct values.*

We proved

Theorem (Helleseth-K.-Li)

If $F = \mathbb{F}_{2^{2m}}$, m *is even, and* $d = 1 + 4(2^m - 1)$, *then*

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 4 \cdot 2^m\}.$$

How to Begin: with the Unit Circle

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$.

How to Begin: with the Unit Circle

$$F = \mathbb{F}_{p^{2m}} \text{ is a finite field}$$

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$.

$\mathrm{Gal}(F/H_F)$ is a cyclic group of order 2 generated by the automorphism $\tau_F \colon F \to F$ with $\tau_F(x) = x^{|H_F|} = x^{p^m}$

How to Begin: with the Unit Circle

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$.

$\mathrm{Gal}(F/H_F)$ is a cyclic group of order 2 generated by the automorphism $\tau_F \colon F \to F$ with $\tau_F(x) = x^{|H_F|} = x^{p^m}$

$$H_F = \{x \in F : \tau_F(x) = x\}$$

How to Begin: with the Unit Circle

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$.

$\mathrm{Gal}(F/H_F)$ is a cyclic group of order 2 generated by the automorphism $\tau_F \colon F \to F$ with $\tau_F(x) = x^{|H_F|} = x^{p^m}$

$$H_F = \{x \in F : \tau_F(x) = x\}$$

We also define the unit circle of F, which is

$$U_F = \{x \in F^* : \tau_F(x) = 1/x\} = \{x \in F^* : x^{p^m+1} = 1\}$$

How to Begin: with the Unit Circle

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$.

$\mathrm{Gal}(F/H_F)$ is a cyclic group of order 2 generated by the automorphism $\tau_F\colon F \to F$ with $\tau_F(x) = x^{|H_F|} = x^{p^m}$

$$H_F = \{x \in F : \tau_F(x) = x\}$$

We also define the unit circle of F, which is

$$U_F = \{x \in F^* : \tau_F(x) = 1/x\} = \{x \in F^* : x^{p^m+1} = 1\}$$

This is the unique cyclic subgroup of order $p^m + 1$ in F^*

How to Begin: with the Unit Circle

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$.

$\mathrm{Gal}(F/H_F)$ is a cyclic group of order 2 generated by the automorphism $\tau_F \colon F \to F$ with $\tau_F(x) = x^{|H_F|} = x^{p^m}$

$$H_F = \{x \in F : \tau_F(x) = x\}$$

We also define the unit circle of F, which is

$$U_F = \{x \in F^* : \tau_F(x) = 1/x\} = \{x \in F^* : x^{p^m+1} = 1\}$$

This is the unique cyclic subgroup of order $p^m + 1$ in F^*

We sometimes call τ_F the conjugation map and abbreviate $\tau_F(x)$ as $\overline{x}$, so then

$$U_F = \{x \in F^* : x\overline{x} = 1\}.$$

Niho's Theorem

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$

$\tau_F \colon F \to F$ with $\tau_F(x) = x^{p^m}$ generates $\mathrm{Gal}(F/H_F)$

The unit circle $U_F = \{x \in F^* : \tau_F(x) = 1/x\}$

Niho's Theorem

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$

$\tau_F : F \to F$ with $\tau_F(x) = x^{p^m}$ generates $\mathrm{Gal}(F/H_F)$

The unit circle $U_F = \{x \in F^* : \tau_F(x) = 1/x\}$

Theorem

Let $F = \mathbb{F}_{p^{2m}}$ and $d = s(p^m - 1) + 1$ and for $a \in F$, let $Z_{F,a}$ be the number of distinct roots of the polynomial

$$g_{F,a}(x) = x^{2s-1} - ax^s - \tau_F(a)x^{s-1} + 1$$

that lie on U_F. Then

$$W_{F,d}(a) = (Z_{F,a} - 1)p^m.$$

Niho's Theorem

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$

$\tau_F \colon F \to F$ with $\tau_F(x) = x^{p^m}$ generates $\mathrm{Gal}(F/H_F)$

The unit circle $U_F = \{x \in F^* : \tau_F(x) = 1/x\}$

Theorem

Let $F = \mathbb{F}_{p^{2m}}$ and $d = s(p^m - 1) + 1$ and for $a \in F$, let $Z_{F,a}$ be the number of distinct roots of the polynomial

$$g_{F,a}(x) = x^{2s-1} - ax^s - \tau_F(a)x^{s-1} + 1$$

that lie on U_F. Then

$$W_{F,d}(a) = (Z_{F,a} - 1)p^m.$$

Originally proved by Niho (1972) for $p = 2$

Niho's Theorem

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$

$\tau_F \colon F \to F$ with $\tau_F(x) = x^{p^m}$ generates $\mathrm{Gal}(F/H_F)$

The unit circle $U_F = \{x \in F^* : \tau_F(x) = 1/x\}$

Theorem

Let $F = \mathbb{F}_{p^{2m}}$ and $d = s(p^m - 1) + 1$ and for $a \in F$, let $Z_{F,a}$ be the number of distinct roots of the polynomial

$$g_{F,a}(x) = x^{2s-1} - ax^s - \tau_F(a)x^{s-1} + 1$$

that lie on U_F. Then

$$W_{F,d}(a) = (Z_{F,a} - 1)p^m.$$

Originally proved by Niho (1972) for $p = 2$

Generalized by Rosendahl (2006) to all p

Niho's Proof that the Spectrum is at Most 8-Valued

Niho's Theorem: Let $F = \mathbb{F}_{p^{2m}}$ and $d = s(p^m - 1) + 1$ and for $a \in F$, let $Z_{F,a}$ be the number of distinct roots of the polynomial

$$g_{F,a}(x) = x^{2s-1} - ax^s - \tau_F(a)x^{s-1} + 1$$

that lie on U_F. Then $W_{F,d}(a) = (Z_{F,a} - 1)p^m$.

Niho's Proof that the Spectrum is at Most 8-Valued

Niho's Theorem: Let $F = \mathbb{F}_{p^{2m}}$ and $d = s(p^m - 1) + 1$ and for $a \in F$, let $Z_{F,a}$ be the number of distinct roots of the polynomial

$$g_{F,a}(x) = x^{2s-1} - ax^s - \tau_F(a)x^{s-1} + 1$$

that lie on U_F. Then $W_{F,d}(a) = (Z_{F,a} - 1)p^m$.

When $p = 2$ and $s = 4$, the polynomial $g_{F,a}$ has degree 7; this is Niho's proof that the Weil spectrum is at most 8-valued

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$ *and* $d = 1 + 4(2^m - 1)$, *then*

$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 3 \cdot 2^m, 4 \cdot 2^m, 5 \cdot 2^m, 6 \cdot 2^m\}.$

Niho's Proof that the Spectrum is at Most 8-Valued

Niho's Theorem: Let $F = \mathbb{F}_{p^{2m}}$ and $d = s(p^m - 1) + 1$ and for $a \in F$, let $Z_{F,a}$ be the number of distinct roots of the polynomial

$$g_{F,a}(x) = x^{2s-1} - ax^s - \tau_F(a)x^{s-1} + 1$$

that lie on U_F. Then $W_{F,d}(a) = (Z_{F,a} - 1)p^m$.

When $p = 2$ and $s = 4$, the polynomial $g_{F,a}$ has degree 7; this is Niho's proof that the Weil spectrum is at most 8-valued

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$ and $d = 1 + 4(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 3 \cdot 2^m, 4 \cdot 2^m, 5 \cdot 2^m, 6 \cdot 2^m\}.$$

Our result states that $3 \cdot 2^m$, $5 \cdot 2^m$, and $6 \cdot 2^m$ do not occur in the Weil spectrum,

Niho's Proof that the Spectrum is at Most 8-Valued

Niho's Theorem: Let $F = \mathbb{F}_{p^{2m}}$ and $d = s(p^m - 1) + 1$ and for $a \in F$, let $Z_{F,a}$ be the number of distinct roots of the polynomial

$$g_{F,a}(x) = x^{2s-1} - ax^s - \tau_F(a)x^{s-1} + 1$$

that lie on U_F. Then $W_{F,d}(a) = (Z_{F,a} - 1)p^m$.

When $p = 2$ and $s = 4$, the polynomial $g_{F,a}$ has degree 7; this is Niho's proof that the Weil spectrum is at most 8-valued

Theorem (Niho, 1972)

If $F = \mathbb{F}_{2^{2m}}$ *and* $d = 1 + 4(2^m - 1)$, *then*

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 3 \cdot 2^m, 4 \cdot 2^m, 5 \cdot 2^m, 6 \cdot 2^m\}.$$

Our result states that $3 \cdot 2^m$, $5 \cdot 2^m$, and $6 \cdot 2^m$ do not occur in the Weil spectrum, so it suffices to prove that $Z_{F,a}$ is never 4, 6, or 7.

Equivalent Formulation of Our Result

Theorem (Helleseth-K.-Li, restated)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, and for each $a \in F$,

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

Equivalent Formulation of Our Result

Theorem (Helleseth-K.-Li, restated)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, and for each $a \in F$,

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

We call $g_{F,a}$ the key polynomial for a over F.

Equivalent Formulation of Our Result

Theorem (Helleseth-K.-Li, restated)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, and for each $a \in F$,

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

We call $g_{F,a}$ the key polynomial for a over F.

Lemma

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 4(2^m - 1)$, then the key polynomial $g_{F,a}$ in inseparable if and only if $a \in U_F$.

Equivalent Formulation of Our Result

Theorem (Helleseth-K.-Li, restated)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, and for each $a \in F$,

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

We call $g_{F,a}$ the key polynomial for a over F.

Lemma

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 4(2^m - 1)$, then the key polynomial $g_{F,a}$ in inseparable if and only if $a \in U_F$.

- *If $a = 1$, then $g_{F,a}(x) = (x+1)^5(x^2 + x + 1)$ and 1 is the only root of $g_{F,a}$ on U_F.*

Equivalent Formulation of Our Result

Theorem (Helleseth-K.-Li, restated)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, and for each $a \in F$,

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

We call $g_{F,a}$ the key polynomial for a over F.

Lemma

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 4(2^m - 1)$, then the key polynomial $g_{F,a}$ in inseparable if and only if $a \in U_F$.

- *If $a = 1$, then $g_{F,a}(x) = (x+1)^5(x^2 + x + 1)$ and 1 is the only root of $g_{F,a}$ on U_F.*
- *If $a \in U_F \setminus \{1\}$, then $g_{F,a}(x) = (x^3 + a)(x^4 + 1/a)$ has three simple roots at the cube roots of a, exactly one of which lies on U_F, along with a root of multiplicity 4 at $a^{-1/4} \in U_F$. So there are two distinct roots on U_F.*

Conjugate-Reciprocal Polynomials

Suffices to Show (Only the Separable Case Remains)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

Conjugate-Reciprocal Polynomials

Suffices to Show (Only the Separable Case Remains)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

If $f(x) = f_0 + f_1x + \cdots + f_dx^d \in F[x]$ with $f_0, f_d \neq 0$, then the conjugate-reciprocal of f is the polynomial

$$f^\dagger(x) = \tau_F(f_d) + \tau_F(f_{d-1})x + \cdots + \tau_F(f_0)x^d.$$

Conjugate-Reciprocal Polynomials

Suffices to Show (Only the Separable Case Remains)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

If $f(x) = f_0 + f_1 x + \cdots + f_d x^d \in F[x]$ with $f_0, f_d \neq 0$, then the conjugate-reciprocal of f is the polynomial

$$f^\dagger(x) = \tau_F(f_d) + \tau_F(f_{d-1})x + \cdots + \tau_F(f_0)x^d.$$

If $f^\dagger(x) = f(x)$, we say that $f(x)$ is self-conjugate-reciprocal

Conjugate-Reciprocal Polynomials

Suffices to Show (Only the Separable Case Remains)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

If $f(x) = f_0 + f_1 x + \cdots + f_d x^d \in F[x]$ with $f_0, f_d \neq 0$, then the conjugate-reciprocal of f is the polynomial

$$f^\dagger(x) = \tau_F(f_d) + \tau_F(f_{d-1})x + \cdots + \tau_F(f_0)x^d.$$

If $f^\dagger(x) = f(x)$, we say that $f(x)$ is self-conjugate-reciprocal

Notice that our key polynomials $g_{F,a}$ are self-conjugate-reciprocal

Conjugate-Reciprocal Polynomials

Suffices to Show (Only the Separable Case Remains)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

If $f(x) = f_0 + f_1 x + \cdots + f_d x^d \in F[x]$ with $f_0, f_d \neq 0$, then the conjugate-reciprocal of f is the polynomial

$$f^\dagger(x) = \tau_F(f_d) + \tau_F(f_{d-1})x + \cdots + \tau_F(f_0)x^d.$$

If $f^\dagger(x) = f(x)$, we say that $f(x)$ is self-conjugate-reciprocal

Notice that our key polynomials $g_{F,a}$ are self-conjugate-reciprocal

If r is a root of a self-conjugate-reciprocal polynomial, then so is $1/\tau_F(r)$.

Conjugate-Reciprocal Action

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$

$\tau_F : F \to F$ with $\tau_F(x) = x^{p^m}$ generates $\mathrm{Gal}(F/H_F)$

The unit circle $U_F = \{x \in F^* : \tau_F(x) = 1/x\}$

Conjugate-Reciprocal Action

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$

$\tau_F \colon F \to F$ with $\tau_F(x) = x^{p^m}$ generates $\mathrm{Gal}(F/H_F)$

The unit circle $U_F = \{x \in F^* : \tau_F(x) = 1/x\}$

Let $\overline{F}$ be the algebraic closure of F

Conjugate-Reciprocal Action

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$

$\tau_F \colon F \to F$ with $\tau_F(x) = x^{p^m}$ generates $\mathrm{Gal}(F/H_F)$

The unit circle $U_F = \{x \in F^* : \tau_F(x) = 1/x\}$

Let $\overline{F}$ be the algebraic closure of F

Extend $\tau_F \colon \overline{F} \to \overline{F}$ with $\tau_F(x) = x^{p^m}$ for all $x \in \overline{F}$

Conjugate-Reciprocal Action

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$

$\tau_F \colon F \to F$ with $\tau_F(x) = x^{p^m}$ generates $\mathrm{Gal}(F/H_F)$

The unit circle $U_F = \{x \in F^* : \tau_F(x) = 1/x\}$

Let $\overline{F}$ be the algebraic closure of F

Extend $\tau_F \colon \overline{F} \to \overline{F}$ with $\tau_F(x) = x^{p^m}$ for all $x \in \overline{F}$

Define the conjugate-reciprocal map $\pi_F \colon \overline{F}^* \to \overline{F}^*$ by

$$\pi_F(x) = 1/\tau_F(x) = x^{-p^m}$$

Conjugate-Reciprocal Action

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$

$\tau_F \colon F \to F$ with $\tau_F(x) = x^{p^m}$ generates $\mathrm{Gal}(F/H_F)$

The unit circle $U_F = \{x \in F^* : \tau_F(x) = 1/x\}$

Let $\overline{F}$ be the algebraic closure of F

Extend $\tau_F \colon \overline{F} \to \overline{F}$ with $\tau_F(x) = x^{p^m}$ for all $x \in \overline{F}$

Define the conjugate-reciprocal map $\pi_F \colon \overline{F}^* \to \overline{F}^*$ by

$$\pi_F(x) = 1/\tau_F(x) = x^{-p^m}$$

Then $H_F = \{x \in \overline{F} : \tau_F(x) = x\}$ and $U_F = \{x \in \overline{F}^* : \pi_F(x) = x\}$

Conjugate-Reciprocal Action

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$

$\tau_F \colon F \to F$ with $\tau_F(x) = x^{p^m}$ generates $\mathrm{Gal}(F/H_F)$

The unit circle $U_F = \{x \in F^* : \tau_F(x) = 1/x\}$

Let $\overline{F}$ be the algebraic closure of F

Extend $\tau_F \colon \overline{F} \to \overline{F}$ with $\tau_F(x) = x^{p^m}$ for all $x \in \overline{F}$

Define the conjugate-reciprocal map $\pi_F \colon \overline{F}^* \to \overline{F}^*$ by

$$\pi_F(x) = 1/\tau_F(x) = x^{-p^m}$$

Then $H_F = \{x \in \overline{F} : \tau_F(x) = x\}$ and $U_F = \{x \in \overline{F}^* : \pi_F(x) = x\}$

Let the conjugate-reciprocal group $\Pi_F = \{\pi_F^k : k \in \mathbb{Z}\}$ be the cyclic group of permutations of $\overline{F}^*$ generated by π_F

Conjugate-Reciprocal Action

$F = \mathbb{F}_{p^{2m}}$ is a finite field

The half field $H_F = \mathbb{F}_{p^m}$ is the unique subfield with $[F : H_F] = 2$

$\tau_F \colon F \to F$ with $\tau_F(x) = x^{p^m}$ generates $\mathrm{Gal}(F/H_F)$

The unit circle $U_F = \{x \in F^* : \tau_F(x) = 1/x\}$

Let $\overline{F}$ be the algebraic closure of F

Extend $\tau_F \colon \overline{F} \to \overline{F}$ with $\tau_F(x) = x^{p^m}$ for all $x \in \overline{F}$

Define the conjugate-reciprocal map $\pi_F \colon \overline{F}^* \to \overline{F}^*$ by

$$\pi_F(x) = 1/\tau_F(x) = x^{-p^m}$$

Then $H_F = \{x \in \overline{F} : \tau_F(x) = x\}$ and $U_F = \{x \in \overline{F}^* : \pi_F(x) = x\}$

Let the conjugate-reciprocal group $\Pi_F = \{\pi_F^k : k \in \mathbb{Z}\}$ be the cyclic group of permutations of $\overline{F}^*$ generated by π_F

The set of roots of a self-conjugate-reciprocal polynomial is Π_F-closed

Orbits of the Conjugate-Reciprocal Action

$F = \mathbb{F}_{p^{2m}}$ is a finite field

$\tau_F \colon \overline{F} \to \overline{F}$ with $\tau_F(x) = x^{p^m}$ and

$\pi_F \colon \overline{F}^* \to \overline{F}^*$ with $\pi_F(x) = x^{-p^m}$

$\Pi_F = \{\pi_F^k : k \in \mathbb{Z}\}$ acts on $\overline{F}^*$

The unit circle $U_F = \{x \in \overline{F}^* : \pi_F(x) = x\}$

Orbits of the Conjugate-Reciprocal Action

$$F = \mathbb{F}_{p^{2m}} \text{ is a finite field}$$
$$\tau_F \colon \overline{F} \to \overline{F} \text{ with } \tau_F(x) = x^{p^m} \text{ and}$$
$$\pi_F \colon \overline{F}^* \to \overline{F}^* \text{ with } \pi_F(x) = x^{-p^m}$$
$$\Pi_F = \{\pi_F^k : k \in \mathbb{Z}\} \text{ acts on } \overline{F}^*$$
$$\text{The unit circle } U_F = \{x \in \overline{F}^* : \pi_F(x) = x\}$$

If $r \in \overline{F}^*$, then we write $\Pi_F \cdot r$ for the orbit $\{\pi_F^k(r) : k \in \mathbb{Z}\}$ of r under the conjugate-reciprocal action

Orbits of the Conjugate-Reciprocal Action

$F = \mathbb{F}_{p^{2m}}$ is a finite field
$\tau_F \colon \overline{F} \to \overline{F}$ with $\tau_F(x) = x^{p^m}$ and
$\pi_F \colon \overline{F}^* \to \overline{F}^*$ with $\pi_F(x) = x^{-p^m}$
$\Pi_F = \{\pi_F^k : k \in \mathbb{Z}\}$ acts on $\overline{F}^*$
The unit circle $U_F = \{x \in \overline{F}^* : \pi_F(x) = x\}$

If $r \in \overline{F}^*$, then we write $\Pi_F \cdot r$ for the orbit $\{\pi_F^k(r) : k \in \mathbb{Z}\}$ of r under the conjugate-reciprocal action

The set of roots of a self-conjugate-reciprocal polynomial is a union of such orbits

Orbits of the Conjugate-Reciprocal Action

$F = \mathbb{F}_{p^{2m}}$ is a finite field
$\tau_F \colon \overline{F} \to \overline{F}$ with $\tau_F(x) = x^{p^m}$ and
$\pi_F \colon \overline{F}^* \to \overline{F}^*$ with $\pi_F(x) = x^{-p^m}$
$\Pi_F = \{\pi_F^k : k \in \mathbb{Z}\}$ acts on $\overline{F}^*$
The unit circle $U_F = \{x \in \overline{F}^* : \pi_F(x) = x\}$

If $r \in \overline{F}^*$, then we write $\Pi_F \cdot r$ for the orbit $\{\pi_F^k(r) : k \in \mathbb{Z}\}$ of r under the conjugate-reciprocal action

The set of roots of a self-conjugate-reciprocal polynomial is a union of such orbits

Two main facts:

Orbits of the Conjugate-Reciprocal Action

$$F = \mathbb{F}_{p^{2m}} \text{ is a finite field}$$
$$\tau_F \colon \overline{F} \to \overline{F} \text{ with } \tau_F(x) = x^{p^m} \text{ and}$$
$$\pi_F \colon \overline{F}^* \to \overline{F}^* \text{ with } \pi_F(x) = x^{-p^m}$$
$$\Pi_F = \{\pi_F^k : k \in \mathbb{Z}\} \text{ acts on } \overline{F}^*$$
$$\text{The unit circle } U_F = \{x \in \overline{F}^* : \pi_F(x) = x\}$$

If $r \in \overline{F}^*$, then we write $\Pi_F \cdot r$ for the orbit $\{\pi_F^k(r) : k \in \mathbb{Z}\}$ of r under the conjugate-reciprocal action

The set of roots of a self-conjugate-reciprocal polynomial is a union of such orbits

Two main facts:

- All orbits are finite

Orbits of the Conjugate-Reciprocal Action

$F = \mathbb{F}_{p^{2m}}$ is a finite field
$\tau_F \colon \overline{F} \to \overline{F}$ with $\tau_F(x) = x^{p^m}$ and
$\pi_F \colon \overline{F}^* \to \overline{F}^*$ with $\pi_F(x) = x^{-p^m}$
$\Pi_F = \{\pi_F^k : k \in \mathbb{Z}\}$ acts on $\overline{F}^*$
The unit circle $U_F = \{x \in \overline{F}^* : \pi_F(x) = x\}$

If $r \in \overline{F}^*$, then we write $\Pi_F \cdot r$ for the orbit $\{\pi_F^k(r) : k \in \mathbb{Z}\}$ of r under the conjugate-reciprocal action

The set of roots of a self-conjugate-reciprocal polynomial is a union of such orbits

Two main facts:

- All orbits are finite
- An element $x \in \overline{F}^*$ lies in a singleton orbit (orbit of cardinality 1) if and only if $x \in U_F$

Counting Singleton Orbits

Suffices to Show (Only the Separable Case Remains)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

Counting Singleton Orbits

Suffices to Show (Only the Separable Case Remains)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

Let $R_{F,a}$ denote the set of roots in $\overline{F}^*$ of the key polynomial $g_{F,a}$

Counting Singleton Orbits

Suffices to Show (Only the Separable Case Remains)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

Let $R_{F,a}$ denote the set of roots in $\overline{F}^*$ of the key polynomial $g_{F,a}$

Since $g_{F,a}$ is self-conjugate-reciprocal, $R_{F,a}$ is a union of Π_F-orbits.

Counting Singleton Orbits

Suffices to Show (Only the Separable Case Remains)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, then $g_{F,a}$ does not have precisely 4, 6, or 7 distinct roots on U_F.

Let $R_{F,a}$ denote the set of roots in $\overline{F}^*$ of the key polynomial $g_{F,a}$

Since $g_{F,a}$ is self-conjugate-reciprocal, $R_{F,a}$ is a union of Π_F-orbits.

Suffices to Show (Equivalent Orbital Formulation)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, the partition of the set $R_{F,a}$ of roots of $g_{F,a}$ in $\overline{F}^*$ into Π_F-orbits does not have precisely 4, 6, or 7 singleton orbits.

A Sum Attached to a Π_F-closed Set

Let $F = \mathbb{F}_{p^{2m}}$, let R be a finite Π_F-closed subset of $\overline{F}^*$ and let

$$S = \sum_{\substack{\{u,v\} \subseteq R \\ u \neq v}} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$.

A Sum Attached to a Π_F-closed Set

Let $F = \mathbb{F}_{p^{2m}}$, let R be a finite Π_F-closed subset of $\overline{F}^*$ and let

$$S = \sum_{\substack{\{u,v\} \subseteq R \\ u \neq v}} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$.

Proof: Recall that $x \in H_F$ if and only if $\tau_F(x) = x$,

A Sum Attached to a Π_F-closed Set

Let $F = \mathbb{F}_{p^{2m}}$, let R be a finite Π_F-closed subset of $\overline{F}^*$ and let

$$S = \sum_{\substack{\{u,v\} \subseteq R \\ u \neq v}} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$.

Proof: Recall that $x \in H_F$ if and only if $\tau_F(x) = x$, and note that

$$\tau_F\left(\frac{uv}{(u-v)^2}\right)$$

A Sum Attached to a Π_F-closed Set

Let $F = \mathbb{F}_{p^{2m}}$, let R be a finite Π_F-closed subset of $\overline{F}^*$ and let

$$S = \sum_{\substack{\{u,v\}\subseteq R \\ u\neq v}} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$.

Proof: Recall that $x \in H_F$ if and only if $\tau_F(x) = x$, and note that

$$\tau_F\left(\frac{uv}{(u-v)^2}\right) = \frac{\tau_F(u)\tau_F(v)}{(\tau_F(u) - \tau_F(v))^2}$$

A Sum Attached to a Π_F-closed Set

Let $F = \mathbb{F}_{p^{2m}}$, let R be a finite Π_F-closed subset of $\overline{F}^*$ and let

$$S = \sum_{\substack{\{u,v\}\subseteq R \\ u\neq v}} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$.

Proof: Recall that $x \in H_F$ if and only if $\tau_F(x) = x$, and note that

$$\begin{aligned} \tau_F\left(\frac{uv}{(u-v)^2}\right) &= \frac{\tau_F(u)\tau_F(v)}{(\tau_F(u)-\tau_F(v))^2} \\ &= \frac{\pi_F(u)^{-1}\pi_F(v)^{-1}}{(\pi_F(u)^{-1}-\pi_F(v)^{-1})^2} \end{aligned}$$

A Sum Attached to a Π_F-closed Set

Let $F = \mathbb{F}_{p^{2m}}$, let R be a finite Π_F-closed subset of $\overline{F}^*$ and let

$$S = \sum_{\substack{\{u,v\}\subseteq R \\ u\neq v}} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$.

Proof: Recall that $x \in H_F$ if and only if $\tau_F(x) = x$, and note that

$$\begin{aligned}
\tau_F\left(\frac{uv}{(u-v)^2}\right) &= \frac{\tau_F(u)\tau_F(v)}{(\tau_F(u)-\tau_F(v))^2} \\
&= \frac{\pi_F(u)^{-1}\pi_F(v)^{-1}}{(\pi_F(u)^{-1}-\pi_F(v)^{-1})^2} \\
&= \frac{\pi_F(u)\pi_F(v)}{(\pi_F(v)-\pi_F(u))^2}
\end{aligned}$$

A Sum Attached to a Π_F-closed Set

Let $F = \mathbb{F}_{p^{2m}}$, let R be a finite Π_F-closed subset of $\overline{F}^*$ and let

$$S = \sum_{\substack{\{u,v\}\subseteq R \\ u\neq v}} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$.

Proof: Recall that $x \in H_F$ if and only if $\tau_F(x) = x$, and note that

$$\begin{aligned}
\tau_F\left(\frac{uv}{(u-v)^2}\right) &= \frac{\tau_F(u)\tau_F(v)}{(\tau_F(u)-\tau_F(v))^2} \\
&= \frac{\pi_F(u)^{-1}\pi_F(v)^{-1}}{(\pi_F(u)^{-1}-\pi_F(v)^{-1})^2} \\
&= \frac{\pi_F(u)\pi_F(v)}{(\pi_F(v)-\pi_F(u))^2} \\
&= \frac{\pi_F(u)\pi_F(v)}{(\pi_F(u)-\pi_F(v))^2}
\end{aligned}$$

A Sum Attached to a Π_F-closed Set

Let $F = \mathbb{F}_{p^{2m}}$, let R be a finite Π_F-closed subset of $\overline{F}^*$ and let

$$S = \sum_{\substack{\{u,v\}\subseteq R \\ u\neq v}} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$.

Proof: Recall that $x \in H_F$ if and only if $\tau_F(x) = x$, and note that

$$\begin{aligned}
\tau_F\left(\frac{uv}{(u-v)^2}\right) &= \frac{\tau_F(u)\tau_F(v)}{(\tau_F(u)-\tau_F(v))^2} \\
&= \frac{\pi_F(u)^{-1}\pi_F(v)^{-1}}{(\pi_F(u)^{-1}-\pi_F(v)^{-1})^2} \\
&= \frac{\pi_F(u)\pi_F(v)}{(\pi_F(v)-\pi_F(u))^2} \\
&= \frac{\pi_F(u)\pi_F(v)}{(\pi_F(u)-\pi_F(v))^2}
\end{aligned}$$

So $\tau_F(S) = S$, and so $S \in H_F$ $\square$

A Sum Attached to Two Π_F-closed Sets

Let $F = \mathbb{F}_{p^{2m}}$, let Q, R be finite Π_F-closed subsets of $\overline{F}^*$ and let

$$S = \sum_{(u,v)\in Q\times R} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$.

A Sum Attached to Two Π_F-closed Sets

Let $F = \mathbb{F}_{p^{2m}}$, let Q, R be finite Π_F-closed subsets of $\overline{F}^*$ and let

$$S = \sum_{(u,v)\in Q\times R} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$.

Proof: As previously

$$\tau_F\left(\frac{uv}{(u-v)^2}\right) = \frac{\pi_F(u)\pi_F(v)}{(\pi_F(u)-\pi_F(v))^2}.$$

A Sum Attached to Two Π_F-closed Sets

Let $F = \mathbb{F}_{p^{2m}}$, let Q, R be finite Π_F-closed subsets of $\overline{F}^*$ and let

$$S = \sum_{(u,v)\in Q\times R} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$.

Proof: As previously

$$\tau_F\left(\frac{uv}{(u-v)^2}\right) = \frac{\pi_F(u)\pi_F(v)}{(\pi_F(u)-\pi_F(v))^2}.$$

So $\tau_F(S) = S$, and so $S \in H_F$. $\square$

Trace of the Sum with a Single Orbit

Let $F = \mathbb{F}_{2^{2m}}$, let $r \in \overline{F}^*$, and let $S = \sum_{\substack{\{u,v\} \subseteq \Pi_F \cdot r \\ u \neq v}} \frac{uv}{(u-v)^2}$.

Then $S \in H_F$

Trace of the Sum with a Single Orbit

Let $F = \mathbb{F}_{2^{2m}}$, let $r \in \overline{F}^*$, and let $S = \sum_{\substack{\{u,v\} \subseteq \Pi_F \cdot r \\ u \neq v}} \frac{uv}{(u-v)^2}$.

Then $S \in H_F$ and $\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \binom{|\Pi_F \cdot r| - 1}{2} \pmod{2}$.

Trace of the Sum with a Single Orbit

Let $F = \mathbb{F}_{2^{2m}}$, let $r \in \overline{F}^*$, and let $S = \sum_{\substack{\{u,v\} \subseteq \Pi_F \cdot r \\ u \neq v}} \frac{uv}{(u-v)^2}$.

Then $S \in H_F$ and $\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \binom{|\Pi_F \cdot r| - 1}{2} \pmod{2}$.

Proof: Notice that $T = \frac{uv}{(u-v)^2} = \frac{u}{u-v} + \left(\frac{u}{u-v}\right)^2$.

Trace of the Sum with a Single Orbit

Let $F = \mathbb{F}_{2^{2m}}$, let $r \in \overline{F}^*$, and let $S = \sum_{\substack{\{u,v\} \subseteq \Pi_F \cdot r \\ u \neq v}} \frac{uv}{(u-v)^2}$.

Then $S \in H_F$ and $\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \binom{|\Pi_F \cdot r|-1}{2} \pmod{2}$.

Proof: Notice that $T = \frac{uv}{(u-v)^2} = \frac{u}{u-v} + \left(\frac{u}{u-v}\right)^2$.

So $T + T^2 + \cdots + T^{2^{m-1}} = \frac{u}{u-v} + \tau_F\left(\frac{u}{u-v}\right) = \frac{u}{u-v} + \frac{\pi_F(v)}{\pi_F(v) - \pi_F(u)}$.

Trace of the Sum with a Single Orbit

Let $F = \mathbb{F}_{2^{2m}}$, let $r \in \overline{F}^*$, and let $S = \sum_{\substack{\{u,v\} \subseteq \Pi_F \cdot r \\ u \neq v}} \frac{uv}{(u-v)^2}$.

Then $S \in H_F$ and $\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \binom{|\Pi_F \cdot r| - 1}{2} \pmod 2$.

Proof: Notice that $T = \frac{uv}{(u-v)^2} = \frac{u}{u-v} + \left(\frac{u}{u-v}\right)^2$.

So $T + T^2 + \cdots + T^{2^{m-1}} = \frac{u}{u-v} + \tau_F\left(\frac{u}{u-v}\right) = \frac{u}{u-v} + \frac{\pi_F(v)}{\pi_F(v) - \pi_F(u)}$.

If we let $M = |\Pi_F \cdot r|$ and set $r_k = \pi_F^k(r)$, so that our orbit is $\{r_0 = r, r_1, \ldots, r_{M-1}\}$, then

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \sum_{0 \leq i < j < M} \left(\frac{r_i}{r_i - r_j} + \frac{r_{j+1}}{r_{j+1} - r_{i+1}} \right).$$

Trace of the Sum with a Single Orbit

Let $F = \mathbb{F}_{2^{2m}}$, let $r \in \overline{F}^*$, and let $S = \sum_{\substack{\{u,v\} \subseteq \Pi_F \cdot r \\ u \neq v}} \frac{uv}{(u-v)^2}$.

Then $S \in H_F$ and $\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \binom{|\Pi_F \cdot r| - 1}{2} \pmod{2}$.

Proof: Notice that $T = \frac{uv}{(u-v)^2} = \frac{u}{u-v} + \left(\frac{u}{u-v}\right)^2$.

So $T + T^2 + \cdots + T^{2^{m-1}} = \frac{u}{u-v} + \tau_F\left(\frac{u}{u-v}\right) = \frac{u}{u-v} + \frac{\pi_F(v)}{\pi_F(v) - \pi_F(u)}$.

If we let $M = |\Pi_F \cdot r|$ and set $r_k = \pi_F^k(r)$, so that our orbit is $\{r_0 = r, r_1, \ldots, r_{M-1}\}$, then

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \sum_{0 \leq i < j < M} \left(\frac{r_i}{r_i - r_j} + \frac{r_{j+1}}{r_{j+1} - r_{i+1}}\right).$$

For the $\binom{M-1}{2}$ pairs (k, ℓ) with $0 < k < \ell < M$ both $r_k/(r_k - r_\ell)$ and $r_\ell/(r_\ell - r_k)$ occur, which sum to 1.

Trace of the Sum with a Single Orbit

Let $F = \mathbb{F}_{2^{2m}}$, let $r \in \overline{F}^*$, and let $S = \sum_{\substack{\{u,v\} \subseteq \Pi_F \cdot r \\ u \neq v}} \frac{uv}{(u-v)^2}$.

Then $S \in H_F$ and $\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \binom{|\Pi_F \cdot r|-1}{2} \pmod 2$.

Proof: Notice that $T = \frac{uv}{(u-v)^2} = \frac{u}{u-v} + \left(\frac{u}{u-v}\right)^2$.

So $T + T^2 + \cdots + T^{2^{m-1}} = \frac{u}{u-v} + \tau_F\left(\frac{u}{u-v}\right) = \frac{u}{u-v} + \frac{\pi_F(v)}{\pi_F(v)-\pi_F(u)}$.

If we let $M = |\Pi_F \cdot r|$ and set $r_k = \pi_F^k(r)$, so that our orbit is $\{r_0 = r, r_1, \ldots, r_{M-1}\}$, then

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \sum_{0 \leq i < j < M} \left(\frac{r_i}{r_i - r_j} + \frac{r_{j+1}}{r_{j+1} - r_{i+1}}\right).$$

For the $\binom{M-1}{2}$ pairs (k, ℓ) with $0 < k < \ell < M$ both $r_k/(r_k - r_\ell)$ and $r_\ell/(r_\ell - r_k)$ occur, which sum to 1.

For the remaining $M - 1$ pairs (k, ℓ) with $0 = k < \ell < M$, $r_0/(r_0 - r_\ell)$ occurs twice, which sums to 0. $\square$

Trace of the Sum with Two Orbits

Let $F = \mathbb{F}_{2^{2m}}$, let $r, s \in \overline{F}^*$ belong to different Π_F-orbits, and let

$$S = \sum_{(u,v) \in \Pi_F \cdot r \times \Pi_F \cdot s} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$

Trace of the Sum with Two Orbits

Let $F = \mathbb{F}_{2^{2m}}$, let $r, s \in \overline{F}^*$ belong to different Π_F-orbits, and let

$$S = \sum_{(u,v) \in \Pi_F \cdot r \times \Pi_F \cdot s} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$ and

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = |\Pi_F \cdot r||\Pi_F \cdot s| \pmod{2}.$$

Trace of the Sum with Two Orbits

Let $F = \mathbb{F}_{2^{2m}}$, let $r, s \in \overline{F}^*$ belong to different Π_F-orbits, and let

$$S = \sum_{(u,v) \in \Pi_F \cdot r \times \Pi_F \cdot s} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$ and

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = |\Pi_F \cdot r||\Pi_F \cdot s| \pmod 2.$$

Proof: As previously, if $T = \frac{uv}{(u-v)^2}$, then

$$T + T^2 + \cdots + T^{2^{m-1}} = \frac{u}{u-v} + \frac{\pi_F(v)}{\pi_F(v) - \pi_F(u)},$$

Trace of the Sum with Two Orbits

Let $F = \mathbb{F}_{2^{2m}}$, let $r, s \in \overline{F}^*$ belong to different Π_F-orbits, and let

$$S = \sum_{(u,v) \in \Pi_F \cdot r \times \Pi_F \cdot s} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$ and

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = |\Pi_F \cdot r||\Pi_F \cdot s| \pmod 2.$$

Proof: As previously, if $T = \frac{uv}{(u-v)^2}$, then

$$T + T^2 + \cdots + T^{2^{m-1}} = \frac{u}{u-v} + \frac{\pi_F(v)}{\pi_F(v) - \pi_F(u)},$$

and so

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \sum_{(u,v) \in \Pi_F \cdot r \times \Pi_F \cdot s} \left(\frac{u}{u-v} + \frac{\pi_F(v)}{\pi_F(v) - \pi_F(u)} \right),$$

Trace of the Sum with Two Orbits

Let $F = \mathbb{F}_{2^{2m}}$, let $r, s \in \overline{F}^*$ belong to different Π_F-orbits, and let

$$S = \sum_{(u,v) \in \Pi_F \cdot r \times \Pi_F \cdot s} \frac{uv}{(u-v)^2}.$$

Then $S \in H_F$ and

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = |\Pi_F \cdot r||\Pi_F \cdot s| \pmod 2.$$

Proof: As previously, if $T = \frac{uv}{(u-v)^2}$, then

$$T + T^2 + \cdots + T^{2^{m-1}} = \frac{u}{u-v} + \frac{\pi_F(v)}{\pi_F(v) - \pi_F(u)},$$

and so

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \sum_{(u,v) \in \Pi_F \cdot r \times \Pi_F \cdot s} \left(\frac{u}{u-v} + \frac{\pi_F(v)}{\pi_F(v) - \pi_F(u)} \right),$$

For each of the $|\Pi_F \cdot r||\Pi \cdot s|$ pairs $(u, v) \in \Pi_F \cdot r \times \Pi_F \cdot s$, both $\frac{u}{u-v}$ and $\frac{v}{v-u}$ occur, which sum to 1. $\square$

Trace of the Sum over a Union of Orbits

Let $F = \mathbb{F}_{2^{2m}}$, and let R be the union of N distinct Π_F-orbits in $\overline{F}^*$, and let $S = \sum_{\substack{\{u,v\}\subseteq R\\ u\neq v}} \frac{uv}{(u-v)^2}$. Then $S \in H_F$ and

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \binom{|R|+1}{2} + N \pmod{2}.$$

Trace of the Sum over a Union of Orbits

Let $F = \mathbb{F}_{2^{2m}}$, and let R be the union of N distinct Π_F-orbits in $\overline{F}^*$, and let $S = \sum_{\substack{\{u,v\}\subseteq R \\ u\neq v}} \frac{uv}{(u-v)^2}$. Then $S \in H_F$ and

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \binom{|R|+1}{2} + N \pmod{2}.$$

Proof: Let $\mathcal{P}$ be the partition of R into Π_F-orbits, so

Trace of the Sum over a Union of Orbits

Let $F = \mathbb{F}_{2^{2m}}$, and let R be the union of N distinct Π_F-orbits in $\overline{F}^*$, and let $S = \sum_{\substack{\{u,v\}\subseteq R \\ u \neq v}} \frac{uv}{(u-v)^2}$. Then $S \in H_F$ and

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \binom{|R|+1}{2} + N \pmod 2.$$

Proof: Let $\mathcal{P}$ be the partition of R into Π_F-orbits, so

$$S = \sum_{P\in\mathcal{P}} \sum_{\substack{\{u,v\}\subseteq P \\ u\neq v}} \frac{uv}{(u-v)^2} + \sum_{\substack{\{P,Q\}\subseteq\mathcal{P} \\ P\neq Q}} \sum_{(u,v)\in P\times Q} \frac{uv}{(u-v)^2}.$$

If we apply $\mathrm{Tr}_{H_F/\mathbb{F}_2}$ to S, then by previous results

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \sum_{P\in\mathcal{P}} \binom{|P|-1}{2} + \sum_{\substack{\{P,Q\}\subseteq\mathcal{P} \\ P\neq Q}} |P||Q|.$$

Trace of the Sum over a Union of Orbits

Let $F = \mathbb{F}_{2^{2m}}$, and let R be the union of N distinct Π_F-orbits in $\overline{F}^*$, and let $S = \sum_{\substack{\{u,v\}\subseteq R \\ u\neq v}} \frac{uv}{(u-v)^2}$. Then $S \in H_F$ and

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \binom{|R|+1}{2} + N \pmod 2.$$

Proof: Let $\mathcal{P}$ be the partition of R into Π_F-orbits, so

$$S = \sum_{P\in\mathcal{P}} \sum_{\substack{\{u,v\}\subseteq P \\ u\neq v}} \frac{uv}{(u-v)^2} + \sum_{\substack{\{P,Q\}\subseteq\mathcal{P} \\ P\neq Q}} \sum_{(u,v)\in P\times Q} \frac{uv}{(u-v)^2}.$$

If we apply $\mathrm{Tr}_{H_F/\mathbb{F}_2}$ to S, then by previous results

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \sum_{P\in\mathcal{P}} \binom{|P|-1}{2} + \sum_{\substack{\{P,Q\}\subseteq\mathcal{P} \\ P\neq Q}} |P||Q|.$$

If we had $\binom{|P|}{2}$ instead of $\binom{|P|-1}{2}$, this would count all $\binom{|R|}{2}$ pairs of elements from R,

Trace of the Sum over a Union of Orbits

Let $F = \mathbb{F}_{2^{2m}}$, and let R be the union of N distinct Π_F-orbits in $\overline{F}^*$, and let $S = \sum_{\substack{\{u,v\} \subseteq R \\ u \neq v}} \frac{uv}{(u-v)^2}$. Then $S \in H_F$ and

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \binom{|R|+1}{2} + N \pmod{2}.$$

Proof: Let $\mathcal{P}$ be the partition of R into Π_F-orbits, so

$$S = \sum_{P \in \mathcal{P}} \sum_{\substack{\{u,v\} \subseteq P \\ u \neq v}} \frac{uv}{(u-v)^2} + \sum_{\substack{\{P,Q\} \subseteq \mathcal{P} \\ P \neq Q}} \sum_{(u,v) \in P \times Q} \frac{uv}{(u-v)^2}.$$

If we apply $\mathrm{Tr}_{H_F/\mathbb{F}_2}$ to S, then by previous results

$$\mathrm{Tr}_{H_F/\mathbb{F}_2}(S) = \sum_{P \in \mathcal{P}} \binom{|P|-1}{2} + \sum_{\substack{\{P,Q\} \subseteq \mathcal{P} \\ P \neq Q}} |P||Q|.$$

If we had $\binom{|P|}{2}$ instead of $\binom{|P|-1}{2}$, this would count all $\binom{|R|}{2}$ pairs of elements from R, but we have $\sum_{P \in \mathcal{P}}(|P|-1) = |R| - N$ fewer pairs, so we get $\binom{|R|}{2} - |R| + N$. $\square$

Where were we?

Suffices to Show (Equivalent Orbital Formulation)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, the partition of the set $R_{F,a}$ of roots of $g_{F,a}$ in $\overline{F}^*$ into Π_F-orbits does not have precisely 4, 6, or 7 singleton orbits.

Where were we?

Suffices to Show (Equivalent Orbital Formulation)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, the partition of the set $R_{F,a}$ of roots of $g_{F,a}$ in $\overline{F}^*$ into Π_F-orbits does not have precisely 4, 6, or 7 singleton orbits.

$R_{F,a}$ is a union of Π_F-orbits: let $N_{F,a}$ be the number of orbits.

Where were we?

Suffices to Show (Equivalent Orbital Formulation)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, the partition of the set $R_{F,a}$ of roots of $g_{F,a}$ in $\overline{F}^*$ into Π_F-orbits does not have precisely 4, 6, or 7 singleton orbits.

$R_{F,a}$ is a union of Π_F-orbits: let $N_{F,a}$ be the number of orbits. Let

$$S_{F,a} = \sum_{\substack{\{u,v\} \subseteq R_{F,a} \\ u \neq v}} \frac{uv}{(u-v)^2},$$

Where were we?

Suffices to Show (Equivalent Orbital Formulation)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, the partition of the set $R_{F,a}$ of roots of $g_{F,a}$ in $\overline{F}^*$ into Π_F-orbits does not have precisely 4, 6, or 7 singleton orbits.

$R_{F,a}$ is a union of Π_F-orbits: let $N_{F,a}$ be the number of orbits. Let

$$S_{F,a} = \sum_{\substack{\{u,v\} \subseteq R_{F,a} \\ u \neq v}} \frac{uv}{(u-v)^2},$$

and then our recent result tells us that $S_{F,a} \in H_F$ and

$$\begin{aligned} \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) &= \binom{|R_{F,a}|+1}{2} + N_{F,a} \\ &= \binom{7+1}{2} + N_{F,a} = N_{F,a} \pmod 2 \end{aligned}$$

$S_{F,a}$ in Terms of Symmetric Functions

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable,
whose set $R_{F,a}$ of roots is partitioned into $N_{F,a}$ orbits,
$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where $S_{F,a} = \sum_{\substack{\{u,v\} \subseteq R_{F,a} \\ u \neq v}} \frac{uv}{(u-v)^2}$

$S_{F,a}$ in Terms of Symmetric Functions

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable,
whose set $R_{F,a}$ of roots is partitioned into $N_{F,a}$ orbits,
$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where $S_{F,a} = \sum_{\substack{\{u,v\} \subseteq R_{F,a} \\ u \neq v}} \frac{uv}{(u-v)^2}$

Let $b(x) = \prod_{1 \leq i < j \leq 7}(x_i - x_j) \in \mathbb{F}_2[x_1, \ldots, x_7]$ and let

$$c(x_1, \ldots, x_7) = b(x_1, \ldots, x_7)^2 \sum_{1 \leq i < j \leq 7} \frac{x_i x_j}{(x_i - x_j)^2}.$$

$S_{F,a}$ in Terms of Symmetric Functions

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable,
whose set $R_{F,a}$ of roots is partitioned into $N_{F,a}$ orbits,
$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where $S_{F,a} = \sum_{\substack{\{u,v\} \subseteq R_{F,a} \\ u \neq v}} \frac{uv}{(u-v)^2}$

Let $b(x) = \prod_{1 \le i < j \le 7}(x_i - x_j) \in \mathbb{F}_2[x_1, \ldots, x_7]$ and let

$$c(x_1, \ldots, x_7) = b(x_1, \ldots, x_7)^2 \sum_{1 \le i < j \le 7} \frac{x_i x_j}{(x_i - x_j)^2}.$$

Write $R_{F,a} = \{r_1, \ldots, r_7\}$ so that $S_{F,a} = \frac{c(r_1, \ldots, r_7)}{b(r_1, \ldots, r_7)^2}$.

$S_{F,a}$ in Terms of Symmetric Functions

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable,
whose set $R_{F,a}$ of roots is partitioned into $N_{F,a}$ orbits,
$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where $S_{F,a} = \sum_{\substack{\{u,v\}\subseteq R_{F,a} \\ u\neq v}} \frac{uv}{(u-v)^2}$

Let $b(x) = \prod_{1\leq i<j\leq 7}(x_i - x_j) \in \mathbb{F}_2[x_1, \ldots, x_7]$ and let

$$c(x_1, \ldots, x_7) = b(x_1, \ldots, x_7)^2 \sum_{1\leq i<j\leq 7} \frac{x_i x_j}{(x_i - x_j)^2}.$$

Write $R_{F,a} = \{r_1, \ldots, r_7\}$ so that $S_{F,a} = \frac{c(r_1,\ldots,r_7)}{b(r_1,\ldots,r_7)^2}$.

$c(x_1, \ldots, x_7)$ is homogeneous symmetric of degree 42

$S_{F,a}$ in Terms of Symmetric Functions

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable,
whose set $R_{F,a}$ of roots is partitioned into $N_{F,a}$ orbits,
$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where $S_{F,a} = \sum_{\substack{\{u,v\}\subseteq R_{F,a} \\ u \neq v}} \frac{uv}{(u-v)^2}$

Let $b(x) = \prod_{1\le i<j\le 7}(x_i - x_j) \in \mathbb{F}_2[x_1, \ldots, x_7]$ and let

$$c(x_1, \ldots, x_7) = b(x_1, \ldots, x_7)^2 \sum_{1\le i<j\le 7} \frac{x_i x_j}{(x_i - x_j)^2}.$$

Write $R_{F,a} = \{r_1, \ldots, r_7\}$ so that $S_{F,a} = \frac{c(r_1,\ldots,r_7)}{b(r_1,\ldots,r_7)^2}$.

$c(x_1, \ldots, x_7)$ is homogeneous symmetric of degree 42

Let $\sigma_k(x_1, \ldots, x_7)$ be the degree k elementary symmetric poly., so

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} {\sigma_1}^{e_1} {\sigma_2}^{e_2} \cdots {\sigma_7}^{e_7},$$

with each $\lambda_{(e_1,\ldots,e_7)} \in \mathbb{F}_2$ (and $0 \in \mathbb{N}$).

$S_{F,a}$ in Terms of Symmetric Functions

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits,

$$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2, \text{ where}$$

$$S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2 \text{ with}$$

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1} \sigma_2^{e_2} \cdots \sigma_7^{e_7},$$

$S_{F,a}$ in Terms of Symmetric Functions

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits,

$$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2, \text{ where}$$

$$S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2 \text{ with}$$

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1} \sigma_2^{e_2} \cdots \sigma_7^{e_7},$$

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	0	0	0	0	2	3	2
2	0	0	0	0	3	1	3
3	0	0	0	0	6	2	0
4	0	0	0	0	7	0	1
5	0	0	0	1	4	3	0
6	0	0	0	1	5	1	1

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
7	0	0	1	0	1	1	4
8	0	0	1	0	5	0	2
9	0	0	1	1	3	1	2
10	0	0	2	0	2	2	2
11	0	0	2	0	3	0	3
12	0	0	2	1	0	3	2
13	0	0	2	1	1	1	3
14	0	0	3	0	3	3	0
15	0	0	3	2	1	1	2
16	0	0	4	0	0	5	0
17	0	0	4	0	1	3	1
18	0	0	4	2	2	2	0
19	0	0	4	2	3	0	1
20	0	0	4	3	0	3	0
21	0	0	4	3	1	1	1
22	0	0	5	0	3	2	0

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
23	0	0	5	1	1	3	0
24	0	1	0	0	0	2	4
25	0	1	0	0	1	0	5
26	0	1	0	1	2	2	2
27	0	1	0	1	3	0	3
28	0	1	1	0	5	2	0
29	0	1	1	1	1	0	4
30	0	1	1	2	3	0	2
31	0	1	2	0	2	4	0
32	0	1	2	0	3	2	1
33	0	1	2	2	0	2	2
34	0	1	2	2	1	0	3
35	0	1	3	0	1	2	2
36	0	1	3	1	3	2	0
37	0	1	3	3	1	0	2
38	0	1	4	1	0	4	0

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
39	0	1	4	1	1	2	1
40	0	2	0	0	2	0	4
41	0	2	0	0	4	3	0
42	0	2	0	1	0	1	4
43	0	2	0	2	2	1	2
44	0	2	2	0	1	1	3
45	0	2	2	0	5	0	1
46	0	2	2	1	3	1	1
47	0	2	2	2	2	0	2
48	0	2	2	3	0	1	2
49	0	2	3	0	3	0	2
50	0	2	3	1	1	1	2
51	0	3	0	0	2	2	2
52	0	3	0	1	4	2	0
53	0	3	0	2	0	0	4
54	0	3	0	3	2	0	2

Term Number	$(e_1,\ldots,e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
55	0	3	1	0	1	0	4
56	0	3	2	1	1	0	3
57	0	3	2	2	2	2	0
58	0	3	2	4	0	0	2
59	0	3	4	0	0	4	0
60	0	4	0	0	0	1	4
61	0	5	0	0	4	2	0
62	0	5	0	1	0	0	4
63	0	5	0	2	2	0	2
64	0	7	0	0	0	0	4
65	1	0	0	0	0	1	5
66	1	0	0	0	4	0	3
67	1	0	0	1	2	1	3
68	1	0	1	0	2	0	4
69	1	0	1	0	4	3	0
70	1	0	1	1	0	1	4

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
71	1	0	1	2	2	1	2
72	1	0	2	0	2	3	1
73	1	0	2	2	0	1	3
74	1	0	3	0	0	3	2
75	1	0	3	0	4	2	0
76	1	0	3	1	2	3	0
77	1	0	3	2	2	0	2
78	1	0	3	3	0	1	2
79	1	0	4	0	2	2	1
80	1	0	4	1	0	3	1
81	1	1	0	0	4	2	1
82	1	1	0	1	0	0	5
83	1	1	0	2	2	0	3
84	1	1	1	0	2	2	2
85	1	1	1	1	4	2	0
86	1	1	1	2	0	0	4

Term Number	$(e_1, \dots, e_7)$ such that $\lambda_{(e_1,\dots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
87	1	1	1	3	2	0	2
88	1	1	2	0	0	2	3
89	1	1	2	1	2	2	1
90	1	1	2	3	0	0	3
91	1	1	3	1	0	2	2
92	1	1	3	2	2	2	0
93	1	1	3	4	0	0	2
94	1	1	5	0	0	4	0
95	1	2	1	0	0	1	4
96	1	2	2	0	2	0	3
97	1	2	2	1	0	1	3
98	1	3	0	0	0	0	5
99	1	3	1	0	4	2	0
100	1	3	1	1	0	0	4
101	1	3	1	2	2	0	2
102	1	5	1	0	0	0	4

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
103	2	0	0	0	0	2	4
104	2	0	0	0	1	0	5
105	2	0	0	0	2	5	0
106	2	0	0	0	3	3	1
107	2	0	0	2	0	3	2
108	2	0	0	2	1	1	3
109	2	0	1	1	3	3	0
110	2	0	1	3	1	1	2
111	2	0	2	1	0	5	0
112	2	0	2	1	1	3	1
113	2	0	2	2	0	2	2
114	2	0	2	2	1	0	3
115	2	0	3	0	1	2	2
116	2	1	0	1	2	4	0
117	2	1	0	1	3	2	1
118	2	1	0	3	0	2	2

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
119	2	1	0	3	1	0	3
120	2	1	1	2	3	2	0
121	2	1	1	4	1	0	2
122	2	1	3	0	1	4	0
123	2	2	0	0	3	0	3
124	2	2	0	1	0	3	2
125	2	2	0	1	1	1	3
126	2	2	0	2	0	0	4
127	2	2	0	2	2	3	0
128	2	2	0	4	0	1	2
129	2	2	1	0	1	0	4
130	2	2	1	0	3	3	0
131	2	2	1	2	1	1	2
132	2	2	2	0	1	3	1
133	2	2	2	2	3	0	1
134	2	2	2	3	0	3	0

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
135	2	2	2	3	1	1	1
136	2	2	2	4	0	0	2
137	2	2	3	0	3	2	0
138	2	2	3	1	1	3	0
139	2	2	4	0	0	4	0
140	2	3	0	0	3	2	1
141	2	3	0	2	1	0	3
142	2	3	0	3	2	2	0
143	2	3	0	5	0	0	2
144	2	3	1	0	1	2	2
145	2	3	1	1	3	2	0
146	2	3	1	3	1	0	2
147	2	3	2	1	1	2	1
148	2	4	0	0	1	1	3
149	2	4	0	0	4	2	0
150	2	4	0	0	5	0	1

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
151	2	4	0	1	3	1	1
152	2	4	0	3	0	1	2
153	2	4	1	0	3	0	2
154	2	4	1	1	1	1	2
155	2	5	0	1	1	0	3
156	2	6	0	0	0	0	4
157	3	0	0	1	2	3	1
158	3	0	0	3	0	1	3
159	3	0	1	0	2	2	2
160	3	0	1	2	0	0	4
161	3	0	1	2	2	3	0
162	3	0	1	4	0	1	2
163	3	0	2	0	0	2	3
164	3	0	3	0	0	5	0
165	3	0	3	2	2	2	0
166	3	0	3	4	0	0	2

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
167	3	0	5	0	0	4	0
168	3	1	0	2	2	2	1
169	3	1	0	4	0	0	3
170	3	1	1	0	2	4	0
171	3	1	1	2	0	2	2
172	3	1	1	3	2	2	0
173	3	1	1	5	0	0	2
174	3	1	2	0	0	4	1
175	3	1	3	1	0	4	0
176	3	2	0	0	0	0	5
177	3	2	0	0	2	3	1
178	3	2	0	2	0	1	3
179	3	2	1	0	0	3	2
180	3	2	1	1	2	3	0
181	3	2	1	3	0	1	2
182	3	2	2	0	2	2	1

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
183	3	2	2	1	0	3	1
184	3	3	0	0	0	2	3
185	3	3	0	1	2	2	1
186	3	3	0	3	0	0	3
187	3	3	1	1	0	2	2
188	3	4	0	0	2	0	3
189	3	4	0	1	0	1	3
190	3	4	1	0	0	0	4
191	4	0	0	2	0	5	0
192	4	0	0	2	1	3	1
193	4	0	0	4	2	2	0
194	4	0	0	4	3	0	1
195	4	0	0	5	0	3	0
196	4	0	0	5	1	1	1
197	4	0	1	0	1	5	0
198	4	0	1	3	1	3	0

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
199	4	0	1	4	1	0	2
200	4	0	3	0	1	4	0
201	4	1	0	0	0	6	0
202	4	1	0	0	1	4	1
203	4	1	0	3	0	4	0
204	4	1	0	3	1	2	1
205	4	1	1	1	1	4	0
206	4	2	0	1	1	3	1
207	4	2	0	2	1	0	3
208	4	2	1	0	1	2	2
209	5	0	0	0	0	5	1
210	5	0	0	3	0	3	1
211	5	0	0	4	0	0	3
212	5	0	1	1	0	5	0
213	5	0	1	2	0	2	2
214	5	0	2	0	0	4	1

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
215	5	1	0	1	0	4	1
216	5	2	0	0	0	2	3
217	6	0	0	0	0	6	0
218	6	0	0	0	1	4	1

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits, $N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where $S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2$ with

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1}\sigma_2^{e_2}\cdots\sigma_7^{e_7},$$

Term Number	$(e_1,\ldots,e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
215	5	1	0	1	0	4	1
216	5	2	0	0	0	2	3
217	6	0	0	0	0	6	0
218	6	0	0	0	1	4	1

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits, $N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where $S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2$ with

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1}\sigma_2^{e_2}\cdots\sigma_7^{e_7},$$

Key fact: if $\lambda_{(e_1,\ldots,e_7)} \neq 0$, then at least one of e_1, e_2, e_5, or e_6 is positive.

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
215	5	1	0	1	0	4	1
216	5	2	0	0	0	2	3
217	6	0	0	0	0	6	0
218	6	0	0	0	1	4	1

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits, $N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where $S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2$ with

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1} \sigma_2^{e_2} \cdots \sigma_7^{e_7},$$

Key fact: if $\lambda_{(e_1,\ldots,e_7)} \neq 0$, then at least one of e_1, e_2, e_5, or e_6 is positive.

Term Number	$(e_1,\ldots,e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
199	4	0	1	4	1	0	2
200	4	0	3	0	1	4	0
201	4	1	0	0	0	6	0
202	4	1	0	0	1	4	1
203	4	1	0	3	0	4	0
204	4	1	0	3	1	2	1
205	4	1	1	1	1	4	0
206	4	2	0	1	1	3	1
207	4	2	0	2	1	0	3
208	4	2	1	0	1	2	2
209	5	0	0	0	0	5	1
210	5	0	0	3	0	3	1
211	5	0	0	4	0	0	3
212	5	0	1	1	0	5	0
213	5	0	1	2	0	2	2
214	5	0	2	0	0	4	1

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
183	3	2	2	1	0	3	1
184	3	3	0	0	0	2	3
185	3	3	0	1	2	2	1
186	3	3	0	3	0	0	3
187	3	3	1	1	0	2	2
188	3	4	0	0	2	0	3
189	3	4	0	1	0	1	3
190	3	4	1	0	0	0	4
191	4	0	0	2	0	5	0
192	4	0	0	2	1	3	1
193	4	0	0	4	2	2	0
194	4	0	0	4	3	0	1
195	4	0	0	5	0	3	0
196	4	0	0	5	1	1	1
197	4	0	1	0	1	5	0
198	4	0	1	3	1	3	0

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
167	3	0	5	0	0	4	0
168	3	1	0	2	2	2	1
169	3	1	0	4	0	0	3
170	3	1	1	0	2	4	0
171	3	1	1	2	0	2	2
172	3	1	1	3	2	2	0
173	3	1	1	5	0	0	2
174	3	1	2	0	0	4	1
175	3	1	3	1	0	4	0
176	3	2	0	0	0	0	5
177	3	2	0	0	2	3	1
178	3	2	0	2	0	1	3
179	3	2	1	0	0	3	2
180	3	2	1	1	2	3	0
181	3	2	1	3	0	1	2
182	3	2	2	0	2	2	1

Term Number	$(e_1,\ldots,e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
151	2	4	0	1	3	1	1
152	2	4	0	3	0	1	2
153	2	4	1	0	3	0	2
154	2	4	1	1	1	1	2
155	2	5	0	1	1	0	3
156	2	6	0	0	0	0	4
157	3	0	0	1	2	3	1
158	3	0	0	3	0	1	3
159	3	0	1	0	2	2	2
160	3	0	1	2	0	0	4
161	3	0	1	2	2	3	0
162	3	0	1	4	0	1	2
163	3	0	2	0	0	2	3
164	3	0	3	0	0	5	0
165	3	0	3	2	2	2	0
166	3	0	3	4	0	0	2

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
135	2	2	2	3	1	1	1
136	2	2	2	4	0	0	2
137	2	2	3	0	3	2	0
138	2	2	3	1	1	3	0
139	2	2	4	0	0	4	0
140	2	3	0	0	3	2	1
141	2	3	0	2	1	0	3
142	2	3	0	3	2	2	0
143	2	3	0	5	0	0	2
144	2	3	1	0	1	2	2
145	2	3	1	1	3	2	0
146	2	3	1	3	1	0	2
147	2	3	2	1	1	2	1
148	2	4	0	0	1	1	3
149	2	4	0	0	4	2	0
150	2	4	0	0	5	0	1

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
119	2	1	0	3	1	0	3
120	2	1	1	2	3	2	0
121	2	1	1	4	1	0	2
122	2	1	3	0	1	4	0
123	2	2	0	0	3	0	3
124	2	2	0	1	0	3	2
125	2	2	0	1	1	1	3
126	2	2	0	2	0	0	4
127	2	2	0	2	2	3	0
128	2	2	0	4	0	1	2
129	2	2	1	0	1	0	4
130	2	2	1	0	3	3	0
131	2	2	1	2	1	1	2
132	2	2	2	0	1	3	1
133	2	2	2	2	3	0	1
134	2	2	2	3	0	3	0

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
103	2	0	0	0	0	2	4
104	2	0	0	0	1	0	5
105	2	0	0	0	2	5	0
106	2	0	0	0	3	3	1
107	2	0	0	2	0	3	2
108	2	0	0	2	1	1	3
109	2	0	1	1	3	3	0
110	2	0	1	3	1	1	2
111	2	0	2	1	0	5	0
112	2	0	2	1	1	3	1
113	2	0	2	2	0	2	2
114	2	0	2	2	1	0	3
115	2	0	3	0	1	2	2
116	2	1	0	1	2	4	0
117	2	1	0	1	3	2	1
118	2	1	0	3	0	2	2

Term Number	$(e_1,\ldots,e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
87	1	1	1	3	2	0	2
88	1	1	2	0	0	2	3
89	1	1	2	1	2	2	1
90	1	1	2	3	0	0	3
91	1	1	3	1	0	2	2
92	1	1	3	2	2	2	0
93	1	1	3	4	0	0	2
94	1	1	5	0	0	4	0
95	1	2	1	0	0	1	4
96	1	2	2	0	2	0	3
97	1	2	2	1	0	1	3
98	1	3	0	0	0	0	5
99	1	3	1	0	4	2	0
100	1	3	1	1	0	0	4
101	1	3	1	2	2	0	2
102	1	5	1	0	0	0	4

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
71	1	0	1	2	2	1	2
72	1	0	2	0	2	3	1
73	1	0	2	2	0	1	3
74	1	0	3	0	0	3	2
75	1	0	3	0	4	2	0
76	1	0	3	1	2	3	0
77	1	0	3	2	2	0	2
78	1	0	3	3	0	1	2
79	1	0	4	0	2	2	1
80	1	0	4	1	0	3	1
81	1	1	0	0	4	2	1
82	1	1	0	1	0	0	5
83	1	1	0	2	2	0	3
84	1	1	1	0	2	2	2
85	1	1	1	1	4	2	0
86	1	1	1	2	0	0	4

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
55	0	3	1	0	1	0	4
56	0	3	2	1	1	0	3
57	0	3	2	2	2	2	0
58	0	3	2	4	0	0	2
59	0	3	4	0	0	4	0
60	0	4	0	0	0	1	4
61	0	5	0	0	4	2	0
62	0	5	0	1	0	0	4
63	0	5	0	2	2	0	2
64	0	7	0	0	0	0	4
65	1	0	0	0	0	1	5
66	1	0	0	0	4	0	3
67	1	0	0	1	2	1	3
68	1	0	1	0	2	0	4
69	1	0	1	0	4	3	0
70	1	0	1	1	0	1	4

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
39	0	1	4	1	1	2	1
40	0	2	0	0	2	0	4
41	0	2	0	0	4	3	0
42	0	2	0	1	0	1	4
43	0	2	0	2	2	1	2
44	0	2	2	0	1	1	3
45	0	2	2	0	5	0	1
46	0	2	2	1	3	1	1
47	0	2	2	2	2	0	2
48	0	2	2	3	0	1	2
49	0	2	3	0	3	0	2
50	0	2	3	1	1	1	2
51	0	3	0	0	2	2	2
52	0	3	0	1	4	2	0
53	0	3	0	2	0	0	4
54	0	3	0	3	2	0	2

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
23	0	0	5	1	1	3	0
24	0	1	0	0	0	2	4
25	0	1	0	0	1	0	5
26	0	1	0	1	2	2	2
27	0	1	0	1	3	0	3
28	0	1	1	0	5	2	0
29	0	1	1	1	1	0	4
30	0	1	1	2	3	0	2
31	0	1	2	0	2	4	0
32	0	1	2	0	3	2	1
33	0	1	2	2	0	2	2
34	0	1	2	2	1	0	3
35	0	1	3	0	1	2	2
36	0	1	3	1	3	2	0
37	0	1	3	3	1	0	2
38	0	1	4	1	0	4	0

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
7	0	0	1	0	1	1	4
8	0	0	1	0	5	0	2
9	0	0	1	1	3	1	2
10	0	0	2	0	2	2	2
11	0	0	2	0	3	0	3
12	0	0	2	1	0	3	2
13	0	0	2	1	1	1	3
14	0	0	3	0	3	3	0
15	0	0	3	2	1	1	2
16	0	0	4	0	0	5	0
17	0	0	4	0	1	3	1
18	0	0	4	2	2	2	0
19	0	0	4	2	3	0	1
20	0	0	4	3	0	3	0
21	0	0	4	3	1	1	1
22	0	0	5	0	3	2	0

$S_{F,a}$ in Terms of Symmetric Functions

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits,

$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where

$S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2$ with

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7\\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1} \sigma_2^{e_2} \cdots \sigma_7^{e_7},$$

Term Number	$(e_1, \ldots, e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	0	0	0	0	2	3	2
2	0	0	0	0	3	1	3
3	0	0	0	0	6	2	0
4	0	0	0	0	7	0	1
5	0	0	0	1	4	3	0
6	0	0	0	1	5	1	1

Term Number	$(e_1,\ldots,e_7)$ such that $\lambda_{(e_1,\ldots,e_7)} \neq 0$						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
215	5	1	0	1	0	4	1
216	5	2	0	0	0	2	3
217	6	0	0	0	0	6	0
218	6	0	0	0	1	4	1

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits, $N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where $S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2$ with

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1}\sigma_2^{e_2}\cdots\sigma_7^{e_7},$$

Key fact: if $\lambda_{(e_1,\ldots,e_7)} \neq 0$, then at least one of e_1, e_2, e_5, or e_6 is positive.

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits,

$$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2, \text{ where}$$

$$S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2 \text{ with}$$

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1}\sigma_2^{e_2}\cdots\sigma_7^{e_7},$$

If $\lambda_{(e_1,\ldots,e_7)} \neq 0$, then at least one of e_1, e_2, e_5, or e_6 is positive.

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits,

$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where

$S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2$ with

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1}\sigma_2^{e_2}\cdots\sigma_7^{e_7},$$

If $\lambda_{(e_1,\ldots,e_7)} \neq 0$, then at least one of e_1, e_2, e_5, or e_6 is positive.

Notice that

$$\begin{aligned} g_{F,a}(x) &= x^7 - ax^4 - \tau_F(a)x^3 + 1 \\ &= (x - r_1)\cdots(x - r_7) \\ &= x^7 - \sigma_1(r_1, \ldots, r_7)x^6 + \sigma_2(r_1, \ldots, r_7)x^5 - \cdots - \sigma_7(r_1, \cdots, r_7). \end{aligned}$$

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits, $N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where $S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2$ with

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1}\sigma_2^{e_2}\cdots\sigma_7^{e_7},$$

If $\lambda_{(e_1,\ldots,e_7)} \neq 0$, then at least one of e_1, e_2, e_5, or e_6 is positive.

Notice that

$$\begin{aligned} g_{F,a}(x) &= x^7 - ax^4 - \tau_F(a)x^3 + 1 \\ &= (x - r_1)\cdots(x - r_7) \\ &= x^7 - \sigma_1(r_1, \ldots, r_7)x^6 + \sigma_2(r_1, \ldots, r_7)x^5 - \cdots - \sigma_7(r_1, \cdots, r_7). \end{aligned}$$

So $\sigma_k(r_1, \ldots, r_7) = 0$ for $k \in \{1, 2, 5, 6\}$.

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits,

$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where

$S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2$ with

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1}\sigma_2^{e_2}\cdots\sigma_7^{e_7},$$

If $\lambda_{(e_1,\ldots,e_7)} \neq 0$, then at least one of e_1, e_2, e_5, or e_6 is positive.

Notice that

$$\begin{aligned} g_{F,a}(x) &= x^7 - ax^4 - \tau_F(a)x^3 + 1 \\ &= (x - r_1)\cdots(x - r_7) \\ &= x^7 - \sigma_1(r_1, \ldots, r_7)x^6 + \sigma_2(r_1, \ldots, r_7)x^5 - \cdots - \sigma_7(r_1, \cdots, r_7). \end{aligned}$$

So $\sigma_k(r_1, \ldots, r_7) = 0$ for $k \in \{1, 2, 5, 6\}$.

Every term in $c(r_1, \ldots, r_7)$ is a product of $\sigma_k(r_1, \ldots, r_7)$'s with at least one $k \in \{1, 2, 5, 6\}$, so $S_{F,a} = 0$,

$F = \mathbb{F}_{2^{2m}}$ and $a \in F$ such that $g_{F,a}$ is separable, whose set $R_{F,a} = \{r_1, \ldots, r_7\}$ of roots is partitioned into $N_{F,a}$ orbits,

$N_{F,a} \equiv \mathrm{Tr}_{H_F/\mathbb{F}_2}(S_{F,a}) \pmod 2$, where

$S_{F,a} = c(r_1, \ldots, r_7)/(b(r_1, \ldots, r_7))^2$ with

$$c(x_1, \ldots, x_n) = \sum_{\substack{(e_1,\ldots,e_7)\in\mathbb{N}^7 \\ e_1+2e_2+\ldots+7e_7=42}} \lambda_{(e_1,\ldots,e_7)} \sigma_1^{e_1}\sigma_2^{e_2}\cdots\sigma_7^{e_7},$$

If $\lambda_{(e_1,\ldots,e_7)} \neq 0$, then at least one of e_1, e_2, e_5, or e_6 is positive.

Notice that

$$\begin{aligned} g_{F,a}(x) &= x^7 - ax^4 - \tau_F(a)x^3 + 1 \\ &= (x - r_1)\cdots(x - r_7) \\ &= x^7 - \sigma_1(r_1, \ldots, r_7)x^6 + \sigma_2(r_1, \ldots, r_7)x^5 - \cdots - \sigma_7(r_1, \cdots, r_7). \end{aligned}$$

So $\sigma_k(r_1, \ldots, r_7) = 0$ for $k \in \{1, 2, 5, 6\}$.

Every term in $c(r_1, \ldots, r_7)$ is a product of $\sigma_k(r_1, \ldots, r_7)$'s with at least one $k \in \{1, 2, 5, 6\}$, so $S_{F,a} = 0$, and so $N_{F,a}$ is even

And Now...

Suffices to Show (Equivalent Orbital Formulation)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, the partition of the set $R_{F,a}$ of roots of $g_{F,a}$ in $\overline{F}^*$ into Π_F-orbits does not have precisely 4, 6, or 7 singleton orbits.

And Now...

Suffices to Show (Equivalent Orbital Formulation)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, the partition of the set $R_{F,a}$ of roots of $g_{F,a}$ in $\overline{F}^*$ into Π_F-orbits does not have precisely 4, 6, or 7 singleton orbits.

Now we know that the set $R_{F,a}$ of seven roots is partitioned into an even number of Π_F-orbits

And Now...

Suffices to Show (Equivalent Orbital Formulation)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, the partition of the set $R_{F,a}$ of roots of $g_{F,a}$ in $\overline{F}^*$ into Π_F-orbits does not have precisely 4, 6, or 7 singleton orbits.

Now we know that the set $R_{F,a}$ of seven roots is partitioned into an even number of Π_F-orbits

- So there cannot be precisely 7 singleton orbits, since that would be 7 total orbits (not even!),

And Now...

Suffices to Show (Equivalent Orbital Formulation)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, the partition of the set $R_{F,a}$ of roots of $g_{F,a}$ in $\overline{F}^*$ into Π_F-orbits does not have precisely 4, 6, or 7 singleton orbits.

Now we know that the set $R_{F,a}$ of seven roots is partitioned into an even number of Π_F-orbits

- So there cannot be precisely 7 singleton orbits, since that would be 7 total orbits (not even!),
- nor can there be 6 singleton orbits, since that would place the final element also into a singleton orbit

And Now...

Suffices to Show (Equivalent Orbital Formulation)

If $F = \mathbb{F}_{2^{2m}}$, m is even, $d = 1 + 4(2^m - 1)$, then for each $a \in F$ such that

$$g_{F,a}(x) = x^7 - ax^4 - \tau_F(a)x^3 + 1,$$

is separable, the partition of the set $R_{F,a}$ of roots of $g_{F,a}$ in $\overline{F}^*$ into Π_F-orbits does not have precisely 4, 6, or 7 singleton orbits.

Now we know that the set $R_{F,a}$ of seven roots is partitioned into an even number of Π_F-orbits

- So there cannot be precisely 7 singleton orbits, since that would be 7 total orbits (not even!),
- nor can there be 6 singleton orbits, since that would place the final element also into a singleton orbit
- nor can there be 4 singleton orbits, since the total number of orbits is even, so the remaining 3 elements would need to be partitioned into an even number of orbits, which would introduce another singleton orbit.

Recap

Niho's Last Conjecture (1972)

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 4(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \text{ contains at most 5 distinct values.}$$

Recap

Niho's Last Conjecture (1972)

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 4(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \text{ contains at most } 5 \text{ distinct values.}$$

Theorem (Helleseth-K.-Li)

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 4(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 4 \cdot 2^m\}.$$

Recap

Niho's Last Conjecture (1972)

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 4(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \text{ contains at most 5 distinct values.}$$

Theorem (Helleseth-K.-Li)

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 4(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 4 \cdot 2^m\}.$$

Theorem (Helleseth-K.-Li)

If $F = \mathbb{F}_{2^{2m}}$, m is odd, $m > 1$, and $d = 1 + 4(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 3 \cdot 2^m, 4 \cdot 2^m\}.$$

Recap

Niho's Last Conjecture (1972)

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 4(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \text{ contains at most 5 distinct values.}$$

Theorem (Helleseth-K.-Li)

If $F = \mathbb{F}_{2^{2m}}$, m is even, and $d = 1 + 4(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 4 \cdot 2^m\}.$$

Theorem (Helleseth-K.-Li)

If $F = \mathbb{F}_{2^{2m}}$, m is odd, $m > 1$, and $d = 1 + 4(2^m - 1)$, then

$$\{W_{F,d}(a) : a \in F^*\} \subseteq \{-2^m, 0, 2^m, 2 \cdot 2^m, 3 \cdot 2^m, 4 \cdot 2^m\}.$$

($m = 1$ makes d degenerate, with Weil spectrum $\{0, 4\}$)