Differential Spectra of Power Permutations

Daniel J. Katz[*,†], Kyle Pacheco[*,†], and Yakov Sapozhnikov[*]
Department of Mathematics, California State University, Northridge

[*]Supported by National Science Foundation Award DMS-1500856
[†]Supported by National Science Foundation Award CCF-1815487

Boolean Functions and their Applications (BFA) 2019
Villa Finaly, Florence, Italy
17 June 2019

Power Permutations

Power function on $\mathbb{F}_q$: $f: \mathbb{F}_q \to \mathbb{F}_q$ with $f(x) = x^d$ for some positive integer d

Power Permutations

Power function on $\mathbb{F}_q$: $f : \mathbb{F}_q \to \mathbb{F}_q$ with $f(x) = x^d$ for some positive integer d

Power permutation of $\mathbb{F}_q$: a power function $f(x) = x^d$ on $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$

Power Permutations

Power function on $\mathbb{F}_q$: $f : \mathbb{F}_q \to \mathbb{F}_q$ with $f(x) = x^d$ for some positive integer d

Power permutation of $\mathbb{F}_q$: a power function $f(x) = x^d$ on $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$

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

Power Permutations

Power function on $\mathbb{F}_q$: $f : \mathbb{F}_q \to \mathbb{F}_q$ with $f(x) = x^d$ for some positive integer d

Power permutation of $\mathbb{F}_q$: a power function $f(x) = x^d$ on $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$

If $\gcd(d, q-1) = 1$, we say that d is an invertible exponent over $\mathbb{F}_q$: if $e = 1/d \pmod{q-1}$, 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

Power function on $\mathbb{F}_q$: $f : \mathbb{F}_q \to \mathbb{F}_q$ with $f(x) = x^d$ for some positive integer d

Power permutation of $\mathbb{F}_q$: a power function $f(x) = x^d$ on $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$

If $\gcd(d, q-1) = 1$, we say that d is an invertible exponent over $\mathbb{F}_q$: if $e = 1/d \pmod{q-1}$, 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 and differential cryptanalysis

Linear Functionals

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

Linear Functionals

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

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

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

Linear Functionals

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

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

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

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

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

Linear Functionals

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

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

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

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

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

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

Linear Functionals

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

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

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

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

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

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

If $a_1, \ldots, a_n$ form an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^n}$, then we have the $\mathbb{F}_p$-linear isomorphism:

$$\begin{aligned} \mathbb{F}_q = \mathbb{F}_{p^n} &\to \mathbb{F}_p^n \\ x &\mapsto \left(\mathrm{Tr}(a_1 x), \ldots, \mathrm{Tr}(a_n x)\right), \end{aligned}$$

Linear Functionals

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

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

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

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

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

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

If $a_1, \ldots, a_n$ form an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^n}$, then we have the $\mathbb{F}_p$-linear isomorphism:

$$\begin{aligned} \mathbb{F}_q = \mathbb{F}_{p^n} &\to \mathbb{F}_p^n \\ x &\mapsto (\mathrm{Tr}(a_1 x), \ldots, \mathrm{Tr}(a_n x)), \end{aligned}$$

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

Nonlinearity

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

Nonlinearity

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

If $f : \mathbb{F}_q \to \mathbb{F}_q$, then for each $a \in \mathbb{F}_q^\times$, we get a component function of f:

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

Nonlinearity

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

If $f : \mathbb{F}_q \to \mathbb{F}_q$, then for each $a \in \mathbb{F}_q^\times$, we get a component function of f:

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

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

Nonlinearity

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

If $f\colon \mathbb{F}_q \to \mathbb{F}_q$, then for each $a \in \mathbb{F}_q^\times$, we get a component function of f:

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

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

When $p = 2$, $\displaystyle\sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(af(x)) - \mathrm{Tr}(bx)}$

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

Nonlinearity

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

If $f : \mathbb{F}_q \to \mathbb{F}_q$, then for each $a \in \mathbb{F}_q^\times$, we get a component function of f:

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

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

When $p = 2$, $\displaystyle\sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(af(x)) - \mathrm{Tr}(bx)}$

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

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

Walsh Transform

If $\mathbb{F}_q$ has characteristic 2, want $\sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(af(x)) - \mathrm{Tr}(bx)}$ to be about 0

Walsh Transform

If $\mathbb{F}_q$ has characteristic 2, want $\sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(af(x)) - \mathrm{Tr}(bx)}$ to be about 0

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

$$\psi_q : \mathbb{F}_q \to \langle \zeta_p \rangle \subseteq \mathbb{C}^\times$$

$$\psi_q(x) = \zeta_p^{\mathrm{Tr}(x)} = \zeta_p^{x + x^p + \cdots + x^{q/p}}$$

Walsh Transform

If $\mathbb{F}_q$ has characteristic 2, want $\sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(af(x)) - \mathrm{Tr}(bx)}$ to be about 0

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

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

We define the Walsh Transform of f to be the function

$$W_f : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{C}$$
$$W_f(a, b) = \sum_{x \in \mathbb{F}_q} \psi_q(af(x) - bx) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(af(x)) - \mathrm{Tr}(bx)}$$

Walsh Transform

If $\mathbb{F}_q$ has characteristic 2, want $\sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(af(x)) - \mathrm{Tr}(bx)}$ to be about 0

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

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

We define the Walsh Transform of f to be the function

$$W_f : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{C}$$
$$W_f(a,b) = \sum_{x \in \mathbb{F}_q} \psi_q(af(x) - bx) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(af(x)) - \mathrm{Tr}(bx)}$$

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

Walsh Transform

If $\mathbb{F}_q$ has characteristic 2, want $\sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(af(x)) - \mathrm{Tr}(bx)}$ to be about 0

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

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

We define the Walsh Transform of f to be the function

$$W_f : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{C}$$
$$W_f(a, b) = \sum_{x \in \mathbb{F}_q} \psi_q(af(x) - bx) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(af(x)) - \mathrm{Tr}(bx)}$$

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

Want every element of this spectrum to have small magnitude

Walsh Spectrum of a Power Permutation

$\psi_q : \mathbb{F}_q \to \mathbb{C}^\times$ is the canonical additive character of $\mathbb{F}_q$

Walsh Spectrum of a Power Permutation

$\psi_q \colon \mathbb{F}_q \to \mathbb{C}^\times$ is the canonical additive character of $\mathbb{F}_q$

$f(x) = x^d$ is a power permutation of $\mathbb{F}_q$ (so $\gcd(d, q-1) = 1$)

Walsh Spectrum of a Power Permutation

$\psi_q \colon \mathbb{F}_q \to \mathbb{C}^\times$ is the canonical additive character of $\mathbb{F}_q$

$f(x) = x^d$ is a power permutation of $\mathbb{F}_q$ (so $\gcd(d, q-1) = 1$)

For $a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q$, the Walsh transform is

$$W_f(a, b) = \sum_{x \in \mathbb{F}_q} \psi_q(ax^d - bx),$$

which is a Weil sum of a binomial

Walsh Spectrum of a Power Permutation

$\psi_q \colon \mathbb{F}_q \to \mathbb{C}^\times$ is the canonical additive character of $\mathbb{F}_q$

$f(x) = x^d$ is a power permutation of $\mathbb{F}_q$ (so $\gcd(d, q-1) = 1$)

For $a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q$, the Walsh transform is

$$W_f(a, b) = \sum_{x \in \mathbb{F}_q} \psi_q(ax^d - bx),$$

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

$$W_f(a, b) = \sum_{y \in \mathbb{F}_q} \psi_q(y^d - ba^{-1/d} y) = W_f(1, a^{-1/d} b)$$

Walsh Spectrum of a Power Permutation

$\psi_q \colon \mathbb{F}_q \to \mathbb{C}^\times$ is the canonical additive character of $\mathbb{F}_q$

$f(x) = x^d$ is a power permutation of $\mathbb{F}_q$ (so $\gcd(d, q-1) = 1$)

For $a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q$, the Walsh transform is

$$W_f(a, b) = \sum_{x \in \mathbb{F}_q} \psi_q(ax^d - bx),$$

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

$$W_f(a, b) = \sum_{y \in \mathbb{F}_q} \psi_q(y^d - ba^{-1/d} y) = W_f(1, a^{-1/d} b)$$

So define

$$W_{q,d}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - bx),$$

Walsh Spectrum of a Power Permutation

$\psi_q\colon \mathbb{F}_q \to \mathbb{C}^\times$ is the canonical additive character of $\mathbb{F}_q$

$f(x) = x^d$ is a power permutation of $\mathbb{F}_q$ (so $\gcd(d, q-1) = 1$)

For $a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q$, the Walsh transform is

$$W_f(a,b) = \sum_{x \in \mathbb{F}_q} \psi_q(ax^d - bx),$$

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

$$W_f(a,b) = \sum_{y \in \mathbb{F}_q} \psi_q(y^d - ba^{-1/d}y) = W_f(1, a^{-1/d}b)$$

So define

$$W_{q,d}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - bx),$$

and then the Walsh spectrum of $f(x) = x^d$ over $\mathbb{F}_q$ is

$$\{W_{q,d}(b) : b \in \mathbb{F}_q\}$$

Equivalent Exponents

Suppose $\mathrm{char}(\mathbb{F}_q) = p$, $d \in \mathbb{Z}_+$, and $b \in \mathbb{F}_q$. Then

$$W_{q,pd}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^{pd} - bx) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - bx) = W_{q,d}(b),$$

so that Walsh spectrum for pd is the same as that for d

Equivalent Exponents

Suppose $\mathrm{char}(\mathbb{F}_q) = p$, $d \in \mathbb{Z}_+$, and $b \in \mathbb{F}_q$. Then

$$W_{q,pd}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^{pd} - bx) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - bx) = W_{q,d}(b),$$

so that Walsh spectrum for pd is the same as that for d

If d has an inverse modulo $q-1$ ($x \mapsto x^d$ is a power permutation),

$$\begin{aligned} W_{q,1/d}(b) &= \sum_{x \in \mathbb{F}_q} \psi_q(x^{1/d} - bx) \\ &= \sum_{y \in \mathbb{F}_q} \psi_q((-b^{-1}y^d)^{1/d} - b(-b^{-1}y^d)) \\ &= \sum_{y \in \mathbb{F}_q} \psi_q(y^d - b^{-1/d}y) = W_{q,d}(b^{-1/d}), \end{aligned}$$

(and $W_{q,1/d}(0) = 0 = W_{q,d}(0)$), so the Walsh spectrum for $1/d$ is the same as that for d.

Equivalent Exponents

Suppose $\mathrm{char}(\mathbb{F}_q) = p$, $d \in \mathbb{Z}_+$, and $b \in \mathbb{F}_q$. Then

$$W_{q,pd}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^{pd} - bx) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - bx) = W_{q,d}(b),$$

so that Walsh spectrum for pd is the same as that for d

If d has an inverse modulo $q-1$ ($x \mapsto x^d$ is a power permutation),

$$\begin{aligned} W_{q,1/d}(b) &= \sum_{x \in \mathbb{F}_q} \psi_q(x^{1/d} - bx) \\ &= \sum_{y \in \mathbb{F}_q} \psi_q((-b^{-1}y^d)^{1/d} - b(-b^{-1}y^d)) \\ &= \sum_{y \in \mathbb{F}_q} \psi_q(y^d - b^{-1/d}y) = W_{q,d}(b^{-1/d}), \end{aligned}$$

(and $W_{q,1/d}(0) = 0 = W_{q,d}(0)$), so the Walsh spectrum for $1/d$ is the same as that for d.

Two exponents d, d' are equivalent if $d' \equiv p^k d \pmod{q-1}$ or $d' \equiv p^k d^{-1} \pmod{q-1}$ (when the inverse exists).

Number of Values in the Walsh Spectrum

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

Number of Values in the Walsh Spectrum

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

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

$$W_{q,d}(b) = W_{q,1}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^1 - bx) = \begin{cases} q & \text{if } b = 1 \\ 0 & \text{otherwise} \end{cases}$$

Number of Values in the Walsh Spectrum

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

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

$$W_{q,d}(b) = W_{q,1}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^1 - bx) = \begin{cases} q & \text{if } b = 1 \\ 0 & \text{otherwise} \end{cases}$$

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

Number of Values in the Walsh Spectrum

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

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

$$W_{q,d}(b) = W_{q,1}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^1 - bx) = \begin{cases} q & \text{if } b = 1 \\ 0 & \text{otherwise} \end{cases}$$

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

Helleseth: spectrum of power permutation (with $W_{q,d}(0)$ removed) has at least three distinct values when d is nondegenerate

Number of Values in the Walsh Spectrum

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

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

$$W_{q,d}(b) = W_{q,1}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^1 - bx) = \begin{cases} q & \text{if } b = 1 \\ 0 & \text{otherwise} \end{cases}$$

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

Helleseth: spectrum of power permutation (with $W_{q,d}(0)$ removed) has at least three distinct values when d is nondegenerate

If $\mathbb{F}_q$ is of characteristic p and order p^n:

Number of Values in the Walsh Spectrum

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

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

$$W_{q,d}(b) = W_{q,1}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^1 - bx) = \begin{cases} q & \text{if } b = 1 \\ 0 & \text{otherwise} \end{cases}$$

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

Helleseth: spectrum of power permutation (with $W_{q,d}(0)$ removed) has at least three distinct values when d is nondegenerate

If $\mathbb{F}_q$ is of characteristic p and order p^n:

- if n not a power of 2, we know a d that produces a Walsh spectrum ($W_{q,d}(0)$ removed) with exactly three values

Number of Values in the Walsh Spectrum

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

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

$$W_{q,d}(b) = W_{q,1}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^1 - bx) = \begin{cases} q & \text{if } b = 1 \\ 0 & \text{otherwise} \end{cases}$$

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

Helleseth: spectrum of power permutation (with $W_{q,d}(0)$ removed) has at least three distinct values when d is nondegenerate

If $\mathbb{F}_q$ is of characteristic p and order p^n:

- if n not a power of 2, we know a d that produces a Walsh spectrum ($W_{q,d}(0)$ removed) with exactly three values
- Conjecture (Helleseth 1971): if n is a power of 2, then no d has spectrum ($W_{q,d}(0)$ removed) with exactly three values

Number of Values in the Walsh Spectrum

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

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

$$W_{q,d}(b) = W_{q,1}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^1 - bx) = \begin{cases} q & \text{if } b = 1 \\ 0 & \text{otherwise} \end{cases}$$

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

Helleseth: spectrum of power permutation (with $W_{q,d}(0)$ removed) has at least three distinct values when d is nondegenerate

If $\mathbb{F}_q$ is of characteristic p and order p^n:

- if n not a power of 2, we know a d that produces a Walsh spectrum ($W_{q,d}(0)$ removed) with exactly three values
- Conjecture (Helleseth 1971): if n is a power of 2, then no d has spectrum ($W_{q,d}(0)$ removed) with exactly three values
- This conjecture has been proved when $p = 2$ (K., 2012) or $p = 3$ (K., 2015), but is open for $p \geq 5$

Differential Multiplicities

Let $f : \mathbb{F}_q \to \mathbb{F}_q$

Differential Multiplicities

Let $f\colon \mathbb{F}_q \to \mathbb{F}_q$

For $a, b \in \mathbb{F}_q$, the differential multiplicity of f with respect to a and b is the number $\delta_f(a, b)$ of solutions $(x, y) \in \mathbb{F}_q^2$ of the system

$$\begin{aligned} y - x &= a \\ f(y) - f(x) &= b, \end{aligned}$$

Differential Multiplicities

Let $f : \mathbb{F}_q \to \mathbb{F}_q$

For $a, b \in \mathbb{F}_q$, the differential multiplicity of f with respect to a and b is the number $\delta_f(a, b)$ of solutions $(x, y) \in \mathbb{F}_q^2$ of the system

$$\begin{aligned} y - x &= a \\ f(y) - f(x) &= b, \end{aligned}$$

or equivalently

$$\delta_f(a, b) = \#\{x \in \mathbb{F}_q : f(x + a) - f(x) = b\}.$$

Differential Multiplicities

Let $f\colon \mathbb{F}_q \to \mathbb{F}_q$

For $a, b \in \mathbb{F}_q$, the differential multiplicity of f with respect to a and b is the number $\delta_f(a, b)$ of solutions $(x, y) \in \mathbb{F}_q^2$ of the system

$$\begin{aligned} y - x &= a \\ f(y) - f(x) &= b, \end{aligned}$$

or equivalently

$$\delta_f(a, b) = \#\{x \in \mathbb{F}_q : f(x + a) - f(x) = b\}.$$

We do not typically consider $a = 0$ because

$$\delta_f(0, b) = \begin{cases} q & \text{if } b = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Differential Spectrum

$f : \mathbb{F}_q \to \mathbb{F}_q$

differential mult.: $\delta_f(a, b) = \#\{x \in \mathbb{F}_q : f(x + a) - f(x) = b\}$

Differential Spectrum

$f : \mathbb{F}_q \to \mathbb{F}_q$

differential mult.: $\delta_f(a, b) = \#\{x \in \mathbb{F}_q : f(x + a) - f(x) = b\}$

The differential spectrum of f is

$$\Delta_f = \{\delta_f(a, b) : a \in F^\times, b \in F\}.$$

Differential Spectrum

$f : \mathbb{F}_q \to \mathbb{F}_q$

differential mult.: $\delta_f(a, b) = \#\{x \in \mathbb{F}_q : f(x + a) - f(x) = b\}$

The differential spectrum of f is

$$\Delta_f = \{\delta_f(a, b) : a \in F^\times, b \in F\}.$$

The differential uniformity of f is

$$\delta_f = \max \Delta_f = \max_{a \in F^\times, b \in F} \delta_f(a, b)$$

Differential Spectrum

$f : \mathbb{F}_q \to \mathbb{F}_q$

differential mult.: $\delta_f(a, b) = \#\{x \in \mathbb{F}_q : f(x + a) - f(x) = b\}$

The differential spectrum of f is

$$\Delta_f = \{\delta_f(a, b) : a \in F^\times, b \in F\}.$$

The differential uniformity of f is

$$\delta_f = \max \Delta_f = \max_{a \in F^\times, b \in F} \delta_f(a, b)$$

Want δ_f as as small as possible to counter differential cryptanalysis

Differential Spectrum

$f : \mathbb{F}_q \to \mathbb{F}_q$

differential mult.: $\delta_f(a, b) = \#\{x \in \mathbb{F}_q : f(x + a) - f(x) = b\}$

The differential spectrum of f is

$$\Delta_f = \{\delta_f(a, b) : a \in F^\times, b \in F\}.$$

The differential uniformity of f is

$$\delta_f = \max \Delta_f = \max_{a \in F^\times, b \in F} \delta_f(a, b)$$

Want δ_f as as small as possible to counter differential cryptanalysis

Perfect nonlinear (PN) or planar function: $x \mapsto f(x + a) - f(x)$ is a permutation for every $a \in F^\times$, so $\Delta_f = \{1\}$ and $\delta_f = 1$

Differential Spectrum

$f : \mathbb{F}_q \to \mathbb{F}_q$

differential mult.: $\delta_f(a,b) = \#\{x \in \mathbb{F}_q : f(x+a) - f(x) = b\}$

The differential spectrum of f is

$$\Delta_f = \{\delta_f(a,b) : a \in F^\times, b \in F\}.$$

The differential uniformity of f is

$$\delta_f = \max \Delta_f = \max_{a \in F^\times, b \in F} \delta_f(a,b)$$

Want δ_f as as small as possible to counter differential cryptanalysis

Perfect nonlinear (PN) or planar function: $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \in F^\times$, so $\Delta_f = \{1\}$ and $\delta_f = 1$

PN functions exist only if char($\mathbb{F}_q$) is odd; are never permutations

Differential Spectrum

$f : \mathbb{F}_q \to \mathbb{F}_q$

differential mult.: $\delta_f(a,b) = \#\{x \in \mathbb{F}_q : f(x+a) - f(x) = b\}$

The differential spectrum of f is

$$\Delta_f = \{\delta_f(a,b) : a \in F^\times, b \in F\}.$$

The differential uniformity of f is

$$\delta_f = \max \Delta_f = \max_{a \in F^\times, b \in F} \delta_f(a,b)$$

Want δ_f as as small as possible to counter differential cryptanalysis

Perfect nonlinear (PN) or planar function: $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \in F^\times$, so $\Delta_f = \{1\}$ and $\delta_f = 1$

PN functions exist only if char($\mathbb{F}_q$) is odd; are never permutations

In characteristic 2, each $\delta_f(a,b)$ is even, so the best possible is an almost perfect nonlinear (APN) function: $\Delta_f = \{0,2\}$ and $\delta_f = 2$

Differential Spectrum of a Power Function

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$

Differential Spectrum of a Power Function

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$

For $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$,

$$\begin{aligned}
\delta_f(a, b) &= \#\{x \in \mathbb{F}_q : (x + a)^d - x^d = b\} \\
&= \#\{y \in \mathbb{F}_q : (y + 1)^d - y^d = b/a^d\} \\
&= \delta_f(1, b/a^d).
\end{aligned}$$

Differential Spectrum of a Power Function

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$

For $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$,

$$\begin{aligned}\delta_f(a, b) &= \#\{x \in \mathbb{F}_q : (x + a)^d - x^d = b\} \\ &= \#\{y \in \mathbb{F}_q : (y + 1)^d - y^d = b/a^d\} \\ &= \delta_f(1, b/a^d).\end{aligned}$$

So for each $c \in \mathbb{F}_q$, define the differential multiplicity for x^d over $\mathbb{F}_q$ at c to be

$$N_{q,d}(c) = \delta_{x \mapsto x^d}(1, c) = \#\{x \in \mathbb{F}_q : (x + 1)^d - x^d = c\},$$

Differential Spectrum of a Power Function

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$

For $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$,

$$\begin{aligned}\delta_f(a,b) &= \#\{x \in \mathbb{F}_q : (x+a)^d - x^d = b\} \\ &= \#\{y \in \mathbb{F}_q : (y+1)^d - y^d = b/a^d\} \\ &= \delta_f(1, b/a^d).\end{aligned}$$

So for each $c \in \mathbb{F}_q$, define the differential multiplicity for x^d over $\mathbb{F}_q$ at c to be

$$N_{q,d}(c) = \delta_{x \mapsto x^d}(1,c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\},$$

so the power function $f(x) = x^d$ on $\mathbb{F}_q$ has differential spectrum (Δ_f) equal to

$$\Delta_{q,d} = \{N_{q,d}(c) : c \in \mathbb{F}_q\}$$

Differential Spectrum of a Power Function

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$

For $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$,

$$\begin{aligned}\delta_f(a,b) &= \#\{x \in \mathbb{F}_q : (x+a)^d - x^d = b\} \\ &= \#\{y \in \mathbb{F}_q : (y+1)^d - y^d = b/a^d\} \\ &= \delta_f(1, b/a^d).\end{aligned}$$

So for each $c \in \mathbb{F}_q$, define the differential multiplicity for x^d over $\mathbb{F}_q$ at c to be

$$N_{q,d}(c) = \delta_{x \mapsto x^d}(1,c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\},$$

so the power function $f(x) = x^d$ on $\mathbb{F}_q$ has differential spectrum (Δ_f) equal to

$$\Delta_{q,d} = \{N_{q,d}(c) : c \in \mathbb{F}_q\}$$

Important observation: $\sum_{c \in \mathbb{F}_q} N_{q,d}(c) = q$

Equivalent Exponents

Suppose $\mathrm{char}(\mathbb{F}_q) = p$, $d \in \mathbb{Z}_+$, and $c \in \mathbb{F}_q$. Then

$$\begin{aligned} N_{q,pd}(c^p) &= \#\{x \in \mathbb{F}_q : (x+1)^{pd} - x^{pd} = c^p\} \\ &= \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\} = N_{q,d}(c), \end{aligned}$$

so that $\Delta_{q,pd} = \Delta_{q,d}$.

Equivalent Exponents

Suppose $\mathrm{char}(\mathbb{F}_q) = p$, $d \in \mathbb{Z}_+$, and $c \in \mathbb{F}_q$. Then

$$\begin{aligned} N_{q,pd}(c^p) &= \#\{x \in \mathbb{F}_q : (x+1)^{pd} - x^{pd} = c^p\} \\ &= \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\} = N_{q,d}(c), \end{aligned}$$

so that $\Delta_{q,pd} = \Delta_{q,d}$.

If d has an inverse modulo $q-1$ ($x \mapsto x^d$ is a power permutation),

$$\begin{aligned} N_{q,1/d}(1/c^d) &= \#\{x \in \mathbb{F}_q : (x+1)^{1/d} - x^{1/d} = c^{-1/d}\} \\ &= \#\{x \in \mathbb{F}_q : (x^{1/d} + c^{-1/d})^d - x = 1\} \\ &= \#\{y \in \mathbb{F}_q : (c^{-1/d}y + c^{-1/d})^d - (c^{-1/d}y)^d = 1\} \\ &= \#\{y \in \mathbb{F}_q : (y+1)^d - y^d = c\} = N_{q,d}(c), \end{aligned}$$

(and $N_{q,1/d}(0) = 0 = N_{q,d}(0)$), so then $\Delta_{q,1/d} = \Delta_{q,d}$.

Equivalent Exponents

Suppose $\mathrm{char}(\mathbb{F}_q) = p$, $d \in \mathbb{Z}_+$, and $c \in \mathbb{F}_q$. Then

$$\begin{aligned} N_{q,pd}(c^p) &= \#\{x \in \mathbb{F}_q : (x+1)^{pd} - x^{pd} = c^p\} \\ &= \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\} = N_{q,d}(c), \end{aligned}$$

so that $\Delta_{q,pd} = \Delta_{q,d}$.

If d has an inverse modulo $q-1$ ($x \mapsto x^d$ is a power permutation),

$$\begin{aligned} N_{q,1/d}(1/c^d) &= \#\{x \in \mathbb{F}_q : (x+1)^{1/d} - x^{1/d} = c^{-1/d}\} \\ &= \#\{x \in \mathbb{F}_q : (x^{1/d} + c^{-1/d})^d - x = 1\} \\ &= \#\{y \in \mathbb{F}_q : (c^{-1/d}y + c^{-1/d})^d - (c^{-1/d}y)^d = 1\} \\ &= \#\{y \in \mathbb{F}_q : (y+1)^d - y^d = c\} = N_{q,d}(c), \end{aligned}$$

(and $N_{q,1/d}(0) = 0 = N_{q,d}(0)$), so then $\Delta_{q,1/d} = \Delta_{q,d}$.

Recall: Two exponents d, d' are **equivalent** if $d' \equiv p^k d \pmod{q-1}$ or $d' \equiv p^k d^{-1} \pmod{q-1}$ (when the inverse exists).

Degeneracy

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}_q) = p$

Degeneracy

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}_q) = p$

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

$$N_{q,d}(c^d) = N_{q,1}(c^1) = \#\{x \in \mathbb{F}_q : (x+1)^1 - x^1 = c\} = \begin{cases} q & \text{if } c = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Degeneracy

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}_q) = p$

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

$$N_{q,d}(c^d) = N_{q,1}(c^1) = \#\{x \in \mathbb{F}_q : (x+1)^1 - x^1 = c\} = \begin{cases} q & \text{if } c = 1, \\ 0 & \text{otherwise.} \end{cases}$$

so

$$\Delta_{q,d} = \{0, q\}$$

Degeneracy

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}_q) = p$

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

$$N_{q,d}(c^d) = N_{q,1}(c^1) = \#\{x \in \mathbb{F}_q : (x+1)^1 - x^1 = c\} = \begin{cases} q & \text{if } c = 1, \\ 0 & \text{otherwise.} \end{cases}$$

so

$$\Delta_{q,d} = \{0, q\}$$

Conversely, if $\Delta_{q,d} = \{0, q\}$,

Degeneracy

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}_q) = p$

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

$$N_{q,d}(c^d) = N_{q,1}(c^1) = \#\{x \in \mathbb{F}_q : (x+1)^1 - x^1 = c\} = \begin{cases} q & \text{if } c = 1, \\ 0 & \text{otherwise.} \end{cases}$$

so

$$\Delta_{q,d} = \{0, q\}$$

Conversely, if $\Delta_{q,d} = \{0, q\}$,

then $(x+1)^d - x^d = 1$ must have q solutions

Degeneracy

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}_q) = p$

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

$$N_{q,d}(c^d) = N_{q,1}(c^1) = \#\{x \in \mathbb{F}_q : (x+1)^1 - x^1 = c\} = \begin{cases} q & \text{if } c = 1, \\ 0 & \text{otherwise.} \end{cases}$$

so

$$\Delta_{q,d} = \{0, q\}$$

Conversely, if $\Delta_{q,d} = \{0, q\}$,

then $(x+1)^d - x^d = 1$ must have q solutions

so $(x+1)^d - x^d - 1 \pmod{x^q - x}$ vanishes, and

Degeneracy

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}_q) = p$

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

$$N_{q,d}(c^d) = N_{q,1}(c^1) = \#\{x \in \mathbb{F}_q : (x+1)^1 - x^1 = c\} = \begin{cases} q & \text{if } c = 1, \\ 0 & \text{otherwise.} \end{cases}$$

so

$$\Delta_{q,d} = \{0, q\}$$

Conversely, if $\Delta_{q,d} = \{0, q\}$,

then $(x+1)^d - x^d = 1$ must have q solutions

so $(x+1)^d - x^d - 1 \pmod{x^q - x}$ vanishes, and

this forces d to be degenerate

Degeneracy

Let f be a power function $f(x) = x^d$ on $\mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}_q) = p$

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

$$N_{q,d}(c^d) = N_{q,1}(c^1) = \#\{x \in \mathbb{F}_q : (x+1)^1 - x^1 = c\} = \begin{cases} q & \text{if } c = 1, \\ 0 & \text{otherwise.} \end{cases}$$

so

$$\Delta_{q,d} = \{0, q\}$$

Conversely, if $\Delta_{q,d} = \{0, q\}$,

then $(x+1)^d - x^d = 1$ must have q solutions

so $(x+1)^d - x^d - 1 \pmod{x^q - x}$ vanishes, and

this forces d to be degenerate

Conclusion: d is degenerate $\Leftrightarrow \Delta_{q,d} = \{0, q\}$

Differential Multiplicities and the Walsh Transform

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$ ($\gcd(d, q-1) = 1$)

Differential Multiplicities and the Walsh Transform

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$ ($\gcd(d, q-1) = 1$)

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$

$W_{q,d}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - bx)$

Differential Multiplicities and the Walsh Transform

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$ ($\gcd(d, q-1) = 1$)

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$
$W_{q,d}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - bx)$

Power moments of the Walsh Transform:

Differential Multiplicities and the Walsh Transform

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$ $(\gcd(d, q-1) = 1)$

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$
$W_{q,d}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - bx)$

Power moments of the Walsh Transform:

- $\sum_{b \in \mathbb{F}_q} W_{q,d}(b)^1 = q$

Differential Multiplicities and the Walsh Transform

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$ ($\gcd(d, q-1) = 1$)

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$
$W_{q,d}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - bx)$

Power moments of the Walsh Transform:

- $\sum_{b \in \mathbb{F}_q} W_{q,d}(b)^1 = q$
- $\sum_{b \in \mathbb{F}_q} W_{q,d}(b)^2 = q^2$

Differential Multiplicities and the Walsh Transform

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$ $(\gcd(d, q-1) = 1)$

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$
$W_{q,d}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - bx)$

Power moments of the Walsh Transform:

- $\sum_{b \in \mathbb{F}_q} W_{q,d}(b)^1 = q$
- $\sum_{b \in \mathbb{F}_q} W_{q,d}(b)^2 = q^2$
- $\sum_{b \in \mathbb{F}_q} W_{q,d}(b)^3 = q^2 N_{q,d}(1)$

Differential Multiplicities and the Walsh Transform

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$ ($\gcd(d, q-1) = 1$)

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$
$W_{q,d}(b) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - bx)$

Power moments of the Walsh Transform:

- $\sum_{b \in \mathbb{F}_q} W_{q,d}(b)^1 = q$
- $\sum_{b \in \mathbb{F}_q} W_{q,d}(b)^2 = q^2$
- $\sum_{b \in \mathbb{F}_q} W_{q,d}(b)^3 = q^2 N_{q,d}(1)$
- $\sum_{b \in \mathbb{F}_q} W_{q,d}(b)^4 = q^2 \sum_{c \in \mathbb{F}_q} N_{q,d}(c)^2$

Differential Spectrum of a Power Permutation

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$

So $\gcd(d, q-1) = 1$; this makes d odd when $\mathrm{char}(\mathbb{F}_q)$ is odd

Differential Spectrum of a Power Permutation

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$

So $\gcd(d, q-1) = 1$; this makes d odd when $\mathrm{char}(\mathbb{F}_q)$ is odd

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$

$$\Delta_{q,d} = \{N_{q,d}(c) : c \in \mathbb{F}_q\}$$

Differential Spectrum of a Power Permutation

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$

So $\gcd(d, q-1) = 1$; this makes d odd when $\mathrm{char}(\mathbb{F}_q)$ is odd

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$

$$\Delta_{q,d} = \{N_{q,d}(c) : c \in \mathbb{F}_q\}$$

Basic results:

Differential Spectrum of a Power Permutation

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$

So $\gcd(d, q-1) = 1$; this makes d odd when $\mathrm{char}(\mathbb{F}_q)$ is odd

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$

$$\Delta_{q,d} = \{N_{q,d}(c) : c \in \mathbb{F}_q\}$$

Basic results:

- $N_{q,d}(0) = 0$: $(x+1)^d \neq x^d$ since f is a permutation

Differential Spectrum of a Power Permutation

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$

So $\gcd(d, q-1) = 1$; this makes d odd when $\mathrm{char}(\mathbb{F}_q)$ is odd

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$

$$\Delta_{q,d} = \{N_{q,d}(c) : c \in \mathbb{F}_q\}$$

Basic results:

- $N_{q,d}(0) = 0$: $(x+1)^d \neq x^d$ since f is a permutation
- $N_{q,d}(1) \geq 2$: $(0+1)^d - 0^d = 1$ and $((-1)+1)^d - (-1)^d = 1$

Differential Spectrum of a Power Permutation

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$

So $\gcd(d, q-1) = 1$; this makes d odd when $\mathrm{char}(\mathbb{F}_q)$ is odd

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$

$$\Delta_{q,d} = \{N_{q,d}(c) : c \in \mathbb{F}_q\}$$

Basic results:

- $N_{q,d}(0) = 0$: $(x+1)^d \neq x^d$ since f is a permutation
- $N_{q,d}(1) \geq 2$: $(0+1)^d - 0^d = 1$ and $((-1)+1)^d - (-1)^d = 1$
- If $\mathrm{char}(\mathbb{F}_q)$ is 2, then $N_{q,d}(c)$ is even for all c
- If $\mathrm{char}(\mathbb{F}_q)$ is odd, then $N_{q,d}(2^{1-d})$ is odd, and all other $N_{q,d}(c)$ are even
  - $(x+1)^d - x^d = ((-x-1)+1)^d - (-1-x)^d$, and
  - $x = (-1-x)$ if and only if $x = -1/2$

Differential Spectrum of a Power Permutation

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$

So $\gcd(d, q-1) = 1$; this makes d odd when $\mathrm{char}(\mathbb{F}_q)$ is odd

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$
$\Delta_{q,d} = \{N_{q,d}(c) : c \in \mathbb{F}_q\}$

Basic results:

- $N_{q,d}(0) = 0$: $(x+1)^d \neq x^d$ since f is a permutation
- $N_{q,d}(1) \geq 2$: $(0+1)^d - 0^d = 1$ and $((-1)+1)^d - (-1)^d = 1$
- If $\mathrm{char}(\mathbb{F}_q)$ is 2, then $N_{q,d}(c)$ is even for all c
- If $\mathrm{char}(\mathbb{F}_q)$ is odd, then $N_{q,d}(2^{1-d})$ is odd, and all other $N_{q,d}(c)$ are even
  - $(x+1)^d - x^d = ((-x-1)+1)^d - (-1-x)^d$, and
  - $x = (-1-x)$ if and only if $x = -1/2$
- So $|\Delta_{q,d}| \geq 2$ always

Differential Spectrum of a Power Permutation

Let f be a power permutation $f(x) = x^d$ on $\mathbb{F}_q$

So $\gcd(d, q-1) = 1$; this makes d odd when $\mathrm{char}(\mathbb{F}_q)$ is odd

Recall: $N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^d - x^d = c\}$

$$\Delta_{q,d} = \{N_{q,d}(c) : c \in \mathbb{F}_q\}$$

Basic results:

- $N_{q,d}(0) = 0$: $(x+1)^d \neq x^d$ since f is a permutation
- $N_{q,d}(1) \geq 2$: $(0+1)^d - 0^d = 1$ and $((-1)+1)^d - (-1)^d = 1$
- If $\mathrm{char}(\mathbb{F}_q)$ is 2, then $N_{q,d}(c)$ is even for all c
- If $\mathrm{char}(\mathbb{F}_q)$ is odd, then $N_{q,d}(2^{1-d})$ is odd, and all other $N_{q,d}(c)$ are even
  - $(x+1)^d - x^d = ((-x-1)+1)^d - (-1-x)^d$, and
  - $x = (-1-x)$ if and only if $x = -1/2$
- So $|\Delta_{q,d}| \geq 2$ always
- If $\mathrm{char}(\mathbb{F}_q)$ is odd and d is nondegenerate, then $|\Delta_{q,d}| \geq 3$

Nice Exponent

A nice exponent over $\mathbb{F}_q$ is a positive integer d with:

- d is invertible ($\gcd(d, q-1) = 1$, so $x \mapsto x^d$ is a power permutation of $\mathbb{F}_q$), and
- $|\Delta_{q,d}| \leq 3$ (this includes degenerate exponents).

Nice Exponent

A nice exponent over $\mathbb{F}_q$ is a positive integer d with:

- d is invertible ($\gcd(d, q-1) = 1$, so $x \mapsto x^d$ is a power permutation of $\mathbb{F}_q$), and
- $|\Delta_{q,d}| \leq 3$ (this includes degenerate exponents).

Examples of nice exponents when $\mathrm{char}(\mathbb{F}_q) = 2$:

- Exponents producing APN permutations have $\Delta_{q,d} = \{0, 2\}$
- $d = 5$ when $q = 64$ produces $\Delta_{q,d} = \{0, 4\}$
- $d = q - 2$ when $q = 2^{2m}$ produces $\Delta = \{0, 2, 4\}$

Nice Exponent

A nice exponent over $\mathbb{F}_q$ is a positive integer d with:

- d is invertible ($\gcd(d, q-1) = 1$, so $x \mapsto x^d$ is a power permutation of $\mathbb{F}_q$), and
- $|\Delta_{q,d}| \leq 3$ (this includes degenerate exponents).

Examples of nice exponents when $\operatorname{char}(\mathbb{F}_q) = 2$:

- Exponents producing APN permutations have $\Delta_{q,d} = \{0, 2\}$
- $d = 5$ when $q = 64$ produces $\Delta_{q,d} = \{0, 4\}$
- $d = q - 2$ when $q = 2^{2m}$ produces $\Delta = \{0, 2, 4\}$

Nice exponents when $\operatorname{char}(\mathbb{F}_q)$ is odd:

- $N_{q,d}(2^{1-d})$ is odd,
- at least one $N_{q,d}(c)$ is zero (e.g., when $c = 0$), and
- the remaining $N_{q,d}(c)$'s (when d is nondegenerate) have a common positive even value.

Nice Exponent

A nice exponent over $\mathbb{F}_q$ is a positive integer d with:

- d is invertible ($\gcd(d, q-1) = 1$, so $x \mapsto x^d$ is a power permutation of $\mathbb{F}_q$), and
- $|\Delta_{q,d}| \leq 3$ (this includes degenerate exponents).

Examples of nice exponents when $\mathrm{char}(\mathbb{F}_q) = 2$:

- Exponents producing APN permutations have $\Delta_{q,d} = \{0, 2\}$
- $d = 5$ when $q = 64$ produces $\Delta_{q,d} = \{0, 4\}$
- $d = q - 2$ when $q = 2^{2m}$ produces $\Delta = \{0, 2, 4\}$

Nice exponents when $\mathrm{char}(\mathbb{F}_q)$ is odd:

- $N_{q,d}(2^{1-d})$ is odd,
- at least one $N_{q,d}(c)$ is zero (e.g., when $c = 0$), and
- the remaining $N_{q,d}(c)$'s (when d is nondegenerate) have a common positive even value.

Significance: nice exponents have a close connection to power permutations with three-valued Walsh transforms

Nice Exponents and Three-Valued Walsh Transforms

Conjecture (Helleseth Three-Valued Conjecture, 1971)

If $\mathbb{F}_q$ is a field of characteristic p and order $q = p^{2^s}$, then no power permutation $f(x) = x^d$ of $\mathbb{F}_q$ has a three-valued Walsh spectrum (when $W_{q,d}(0)$ is removed).

Nice Exponents and Three-Valued Walsh Transforms

Conjecture (Helleseth Three-Valued Conjecture, 1971)

If $\mathbb{F}_q$ is a field of characteristic p and order $q = p^{2^s}$, then no power permutation $f(x) = x^d$ of $\mathbb{F}_q$ has a three-valued Walsh spectrum (when $W_{q,d}(0)$ is removed).

Proved by K. (2012, 2015) when $p = 2, 3$

Nice Exponents and Three-Valued Walsh Transforms

Conjecture (Helleseth Three-Valued Conjecture, 1971)

If $\mathbb{F}_q$ is a field of characteristic p and order $q = p^{2^s}$, then no power permutation $f(x) = x^d$ of $\mathbb{F}_q$ has a three-valued Walsh spectrum (when $W_{q,d}(0)$ is removed).

Proved by K. (2012, 2015) when $p = 2, 3$

Conjecture (K.-Langevin Nice Exponent Conjecture, 2016)

If $\operatorname{char}(\mathbb{F}_q)$ is odd and d is a nice exponent over $\mathbb{F}_q$, then 2 is in its differential spectrum (i.e., $N_{q,d}(c) = 2$ for some $c \in \mathbb{F}_q$)

Nice Exponents and Three-Valued Walsh Transforms

Conjecture (Helleseth Three-Valued Conjecture, 1971)

If $\mathbb{F}_q$ is a field of characteristic p and order $q = p^{2^s}$, then no power permutation $f(x) = x^d$ of $\mathbb{F}_q$ has a three-valued Walsh spectrum (when $W_{q,d}(0)$ is removed).

Proved by K. (2012, 2015) when $p = 2, 3$

Conjecture (K.-Langevin Nice Exponent Conjecture, 2016)

If $\operatorname{char}(\mathbb{F}_q)$ is odd and d is a nice exponent over $\mathbb{F}_q$, then 2 is in its differential spectrum (i.e., $N_{q,d}(c) = 2$ for some $c \in \mathbb{F}_q$)

Conjecture (K.-Langevin Optimist Conjecture, 2016)

If $\operatorname{char}(\mathbb{F}_q)$ is odd and d is an invertible exponent over $\mathbb{F}_q$ (i.e., $\gcd(d, q-1) = 1$), then 2 is in its differential spectrum

Nice Exponents and Three-Valued Walsh Transforms

Conjecture (Helleseth Three-Valued Conjecture, 1971)

If $\mathbb{F}_q$ is a field of characteristic p and order $q = p^{2^s}$, then no power permutation $f(x) = x^d$ of $\mathbb{F}_q$ has a three-valued Walsh spectrum (when $W_{q,d}(0)$ is removed).

Proved by K. (2012, 2015) when $p = 2, 3$

Conjecture (K.-Langevin Nice Exponent Conjecture, 2016)

If $\operatorname{char}(\mathbb{F}_q)$ is odd and d is a nice exponent over $\mathbb{F}_q$, then 2 is in its differential spectrum (i.e., $N_{q,d}(c) = 2$ for some $c \in \mathbb{F}_q$)

Conjecture (K.-Langevin Optimist Conjecture, 2016)

If $\operatorname{char}(\mathbb{F}_q)$ is odd and d is an invertible exponent over $\mathbb{F}_q$ (i.e., $\gcd(d, q-1) = 1$), then 2 is in its differential spectrum

Optimist

Nice Exponents and Three-Valued Walsh Transforms

Conjecture (Helleseth Three-Valued Conjecture, 1971)

If $\mathbb{F}_q$ is a field of characteristic p and order $q = p^{2^s}$, then no power permutation $f(x) = x^d$ of $\mathbb{F}_q$ has a three-valued Walsh spectrum (when $W_{q,d}(0)$ is removed).

Proved by K. (2012, 2015) when $p = 2, 3$

Conjecture (K.-Langevin Nice Exponent Conjecture, 2016)

If $\mathrm{char}(\mathbb{F}_q)$ is odd and d is a nice exponent over $\mathbb{F}_q$, then 2 is in its differential spectrum (i.e., $N_{q,d}(c) = 2$ for some $c \in \mathbb{F}_q$)

Conjecture (K.-Langevin Optimist Conjecture, 2016)

If $\mathrm{char}(\mathbb{F}_q)$ is odd and d is an invertible exponent over $\mathbb{F}_q$ (i.e., $\gcd(d, q-1) = 1$), then 2 is in its differential spectrum

Optimist $\Rightarrow$ Nice Exponent

Nice Exponents and Three-Valued Walsh Transforms

Conjecture (Helleseth Three-Valued Conjecture, 1971)

If $\mathbb{F}_q$ is a field of characteristic p and order $q = p^{2^s}$, then no power permutation $f(x) = x^d$ of $\mathbb{F}_q$ has a three-valued Walsh spectrum (when $W_{q,d}(0)$ is removed).

Proved by K. (2012, 2015) when $p = 2, 3$

Conjecture (K.-Langevin Nice Exponent Conjecture, 2016)

If $\mathrm{char}(\mathbb{F}_q)$ is odd and d is a nice exponent over $\mathbb{F}_q$, then 2 is in its differential spectrum (i.e., $N_{q,d}(c) = 2$ for some $c \in \mathbb{F}_q$)

Conjecture (K.-Langevin Optimist Conjecture, 2016)

If $\mathrm{char}(\mathbb{F}_q)$ is odd and d is an invertible exponent over $\mathbb{F}_q$ (i.e., $\gcd(d, q-1) = 1$), then 2 is in its differential spectrum

Optimist $\Rightarrow$ Nice Exponent $\Rightarrow$ Three-Valued

The Exponent $d = 3$

$d = 3$ is invertible over $\mathbb{F}_q \Leftrightarrow \gcd(3, q-1) = 1 \Leftrightarrow q \not\equiv 1 \pmod 3$

The Exponent $d = 3$

$d = 3$ is invertible over $\mathbb{F}_q \Leftrightarrow \gcd(3, q-1) = 1 \Leftrightarrow q \not\equiv 1 \pmod 3$

For $q \equiv 0 \pmod 3$ (fields of characteristic 3):

3 is degenerate, so $\Delta_{q,d} = \{0, q\}$ and 3 is nice

The Exponent $d = 3$

$d = 3$ is invertible over $\mathbb{F}_q \Leftrightarrow \gcd(3, q-1) = 1 \Leftrightarrow q \not\equiv 1 \pmod 3$

For $q \equiv 0 \pmod 3$ (fields of characteristic 3):

3 is degenerate, so $\Delta_{q,d} = \{0, q\}$ and 3 is nice

For $q \equiv 2 \pmod 3$

$$(x+1)^3 - x^3 = 3x^2 + 3x + 1$$

is quadratic and so

$$N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^3 - x^3 = c\} \leq 2$$

so $\Delta_{q,d} \subseteq \{0, 1, 2\}$ and 3 is nice over $\mathbb{F}_q$

The Exponent $d = 3$

$d = 3$ is invertible over $\mathbb{F}_q \Leftrightarrow \gcd(3, q-1) = 1 \Leftrightarrow q \not\equiv 1 \pmod 3$

For $q \equiv 0 \pmod 3$ (fields of characteristic 3):

3 is degenerate, so $\Delta_{q,d} = \{0, q\}$ and 3 is nice

For $q \equiv 2 \pmod 3$

$$(x+1)^3 - x^3 = 3x^2 + 3x + 1$$

is quadratic and so

$$N_{q,d}(c) = \#\{x \in \mathbb{F}_q : (x+1)^3 - x^3 = c\} \leq 2$$

so $\Delta_{q,d} \subseteq \{0, 1, 2\}$ and 3 is nice over $\mathbb{F}_q$

Summary (K.-Langevin, 2016): 3 is nice over $\mathbb{F}_q$ if and only if $q \not\equiv 1 \pmod 3$

The Exponent $d = q - 2$

$q - 2$ is always invertible over $\mathbb{F}_q$ and $x^{q-2} = x^{-1}$ for $x \neq 0$

The Exponent $d = q - 2$

$q - 2$ is always invertible over $\mathbb{F}_q$ and $x^{q-2} = x^{-1}$ for $x \neq 0$

For $x \notin \{0, -1\}$, we have $(x+1)^{q-2} - x^{q-2} = -\frac{1}{x(x+1)}$

The Exponent $d = q - 2$

$q - 2$ is always invertible over $\mathbb{F}_q$ and $x^{q-2} = x^{-1}$ for $x \neq 0$

For $x \notin \{0, -1\}$, we have $(x+1)^{q-2} - x^{q-2} = -\frac{1}{x(x+1)}$

So for $x \notin \{0, -1\}$,

$$(x+1)^{q-2} - x^{q-2} = c \Leftrightarrow cx^2 + cx + 1 = 0$$

The Exponent $d = q - 2$

$q - 2$ is always invertible over $\mathbb{F}_q$ and $x^{q-2} = x^{-1}$ for $x \neq 0$

For $x \notin \{0, -1\}$, we have $(x+1)^{q-2} - x^{q-2} = -\frac{1}{x(x+1)}$

So for $x \notin \{0, -1\}$,

$$(x+1)^{q-2} - x^{q-2} = c \Leftrightarrow cx^2 + cx + 1 = 0$$

- $(x+1)^{q-2} - x^{q-2} = 1$ for $x = 0, -1$, or a root of $x^2 + x + 1$:

$$N_{q,d}(1) = \begin{cases} 3 & \text{if } q \equiv 0 \pmod 3, \\ 4 & \text{if } q \equiv 1 \pmod 3, \\ 2 & \text{if } q \equiv 2 \pmod 3) \end{cases}$$

The Exponent $d = q - 2$

$q-2$ is always invertible over $\mathbb{F}_q$ and $x^{q-2} = x^{-1}$ for $x \neq 0$

For $x \notin \{0, -1\}$, we have $(x+1)^{q-2} - x^{q-2} = -\frac{1}{x(x+1)}$

So for $x \notin \{0, -1\}$,

$$(x+1)^{q-2} - x^{q-2} = c \Leftrightarrow cx^2 + cx + 1 = 0$$

- $(x+1)^{q-2} - x^{q-2} = 1$ for $x = 0, -1$, or a root of $x^2 + x + 1$:

$$N_{q,d}(1) = \begin{cases} 3 & \text{if } q \equiv 0 \pmod 3, \\ 4 & \text{if } q \equiv 1 \pmod 3, \\ 2 & \text{if } q \equiv 2 \pmod 3) \end{cases}$$

- For $c \neq 1$, we have $N_{q,d}(c) \leq 2$

The Exponent $d = q - 2$

$q - 2$ is always invertible over $\mathbb{F}_q$ and $x^{q-2} = x^{-1}$ for $x \neq 0$

For $x \notin \{0, -1\}$, we have $(x+1)^{q-2} - x^{q-2} = -\frac{1}{x(x+1)}$

So for $x \notin \{0, -1\}$,

$$(x+1)^{q-2} - x^{q-2} = c \Leftrightarrow cx^2 + cx + 1 = 0$$

- $(x+1)^{q-2} - x^{q-2} = 1$ for $x = 0, -1$, or a root of $x^2 + x + 1$:

$$N_{q,d}(1) = \begin{cases} 3 & \text{if } q \equiv 0 \pmod 3, \\ 4 & \text{if } q \equiv 1 \pmod 3, \\ 2 & \text{if } q \equiv 2 \pmod 3 \end{cases}$$

- For $c \neq 1$, we have $N_{q,d}(c) \leq 2$

Recall: $N_{q,d}(c)$ is even except for $N_{q,d}(2^{1-d})$ when $q \equiv 1 \pmod 2$

The Exponent $d = q - 2$

$q - 2$ is always invertible over $\mathbb{F}_q$ and $x^{q-2} = x^{-1}$ for $x \neq 0$

For $x \notin \{0, -1\}$, we have $(x+1)^{q-2} - x^{q-2} = -\frac{1}{x(x+1)}$

So for $x \notin \{0, -1\}$,

$$(x+1)^{q-2} - x^{q-2} = c \Leftrightarrow cx^2 + cx + 1 = 0$$

- $(x+1)^{q-2} - x^{q-2} = 1$ for $x = 0, -1$, or a root of $x^2 + x + 1$:

$$N_{q,d}(1) = \begin{cases} 3 & \text{if } q \equiv 0 \pmod{3}, \\ 4 & \text{if } q \equiv 1 \pmod{3}, \\ 2 & \text{if } q \equiv 2 \pmod{3} \end{cases}$$

- For $c \neq 1$, we have $N_{q,d}(c) \leq 2$

Recall: $N_{q,d}(c)$ is even except for $N_{q,d}(2^{1-d})$ when $q \equiv 1 \pmod{2}$

Consequence (K.-Langevin, 2016): $q - 2$ is a nice exponent for $\mathbb{F}_q$ if and only if $q \not\equiv 1 \pmod{6}$

The Exponent $2\sqrt{q} - 1$

On this slide: p is prime and $q = p^n$ with n even

So then $\sqrt{q}$ is an integer

The Exponent $2\sqrt{q} - 1$

On this slide: p is prime and $q = p^n$ with n even

So then $\sqrt{q}$ is an integer

Lemma (K.-Pacheco-Sapozhnikov, 2019)

Suppose $q = p^n$ with n even and $d = 2p^{n/2} - 1 = 2\sqrt{q} - 1$. Then d is invertible over $\mathbb{F}_q$ if and only if $\sqrt{q} \not\equiv 2 \pmod{3}$.

The Exponent $2\sqrt{q} - 1$

On this slide: p is prime and $q = p^n$ with n even

So then $\sqrt{q}$ is an integer

Lemma (K.-Pacheco-Sapozhnikov, 2019)

Suppose $q = p^n$ with n even and $d = 2p^{n/2} - 1 = 2\sqrt{q} - 1$. Then d is invertible over $\mathbb{F}_q$ if and only if $\sqrt{q} \not\equiv 2 \pmod{3}$.

Theorem (K.-Pacheco-Sapozhnikov, 2019)

If $d = 2\sqrt{q} - 1$ is invertible over $\mathbb{F}_q$, then it is nice, with

- $N_{q,d}(1) = \sqrt{q}$, *and*
- *all other $N_{q,d}(c)$'s in $\{0, 2\}$.*

Method of proof: fancy algebra.

A Conjecture

We performed a computer search for nice exponents for fields of characteristics from 2 to 53 and of orders up to around 10^6 (for some characteristics considerably larger than that)

A Conjecture

We performed a computer search for nice exponents for fields of characteristics from 2 to 53 and of orders up to around 10^6 (for some characteristics considerably larger than that)

Conjecture

Let $q = p^n$ with p an odd prime. Then (up to equivalence) the following are the only nice exponents over $\mathbb{F}_q$:

A Conjecture

We performed a computer search for nice exponents for fields of characteristics from 2 to 53 and of orders up to around 10^6 (for some characteristics considerably larger than that)

Conjecture

Let $q = p^n$ with p an odd prime. Then (up to equivalence) the following are the only nice exponents over $\mathbb{F}_q$:

- *$d = 1$ is always nice (it is degenerate),*

A Conjecture

We performed a computer search for nice exponents for fields of characteristics from 2 to 53 and of orders up to around 10^6 (for some characteristics considerably larger than that)

Conjecture

Let $q = p^n$ with p an odd prime. Then (up to equivalence) the following are the only nice exponents over $\mathbb{F}_q$:

- *$d = 1$ is always nice (it is degenerate),*
- *If $d = 3$, then d is nice if $q \not\equiv 1 \pmod 3$,*

A Conjecture

We performed a computer search for nice exponents for fields of characteristics from 2 to 53 and of orders up to around 10^6 (for some characteristics considerably larger than that)

Conjecture

Let $q = p^n$ with p an odd prime. Then (up to equivalence) the following are the only nice exponents over $\mathbb{F}_q$:

- *$d = 1$ is always nice (it is degenerate),*
- *If $d = 3$, then d is nice if $q \not\equiv 1 \pmod 3$,*
- *If $d = q - 2$, then d is nice if $q \not\equiv 1 \pmod 6$,*

A Conjecture

We performed a computer search for nice exponents for fields of characteristics from 2 to 53 and of orders up to around 10^6 (for some characteristics considerably larger than that)

Conjecture

Let $q = p^n$ with p an odd prime. Then (up to equivalence) the following are the only nice exponents over $\mathbb{F}_q$:

- *$d = 1$ is always nice (it is degenerate),*
- *If $d = 3$, then d is nice if $q \not\equiv 1 \pmod 3$,*
- *If $d = q - 2$, then d is nice if $q \not\equiv 1 \pmod 6$,*
- *If n is even, then $d = 2\sqrt{q} - 1$ is nice if $\sqrt{q} \not\equiv 2 \pmod 3$.*

A Conjecture

We performed a computer search for nice exponents for fields of characteristics from 2 to 53 and of orders up to around 10^6 (for some characteristics considerably larger than that)

Conjecture

Let $q = p^n$ with p an odd prime. Then (up to equivalence) the following are the only nice exponents over $\mathbb{F}_q$:

- *$d = 1$ is always nice (it is degenerate),*
- *If $d = 3$, then d is nice if $q \not\equiv 1 \pmod 3$,*
- *If $d = q - 2$, then d is nice if $q \not\equiv 1 \pmod 6$,*
- *If n is even, then $d = 2\sqrt{q} - 1$ is nice if $\sqrt{q} \not\equiv 2 \pmod 3$.*
- *If $p = 5$ and n is odd, then $d = (5^m + 1)/2$ is nice if $m < n$ with m odd and $\gcd(m, n) = 1$.*