Differential analysis through a double cover using the unit circle in a finite field

Daniel J. Katz[1], Kathleen R. O'Connor[1],
Kyle Pacheco[1], and Yakov Sapozhnikov[1,2]

[1]Department of Mathematics
California State University, Northridge

[2]Department of Mathematics and Statistical Science
University of Idaho

Supported by National Science Foundation
Awards 1500856, 1815487 and 2206454

Finite Geometries 2025
Seventh Irsee Conference
Kloster Irsee
02 September 2025

Power functions

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

Power functions

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

A power function on F is an $f\colon F \to F$ where there is a positive integer d such that $f(x) = x^d$ for all $x \in F$.

Power functions

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

A power function on F is an $f\colon F \to F$ where there is a positive integer d such that $f(x) = x^d$ for all $x \in F$.

Our power function f is bijective if and only if $\gcd(d, q-1) = 1$. Then we say that d is invertible over F (or that f is a power permutation) and we let $e \in \mathbb{Z}_+$ with $e \equiv d^{-1} \pmod{q-1}$ so that $x \mapsto x^e$ is the inverse function of $x \mapsto x^d$.

Power functions

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

A power function on F is an $f \colon F \to F$ where there is a positive integer d such that $f(x) = x^d$ for all $x \in F$.

Our power function f is bijective if and only if $\gcd(d, q-1) = 1$. Then we say that d is invertible over F (or that f is a power permutation) and we let $e \in \mathbb{Z}_+$ with $e \equiv d^{-1} \pmod{q-1}$ so that $x \mapsto x^e$ is the inverse function of $x \mapsto x^d$.

If $r \in \mathbb{Q}_+$, then we can think of r as an exponent over F if r in reduced form is d_1/d_2 with $\gcd(d_2, q-1) = 1$; then $r = d_1/d_2$ is regarded as a positive integer d with $d \equiv d_1 d_2^{-1} \pmod{q-1}$.

Power functions

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

A power function on F is an $f\colon F \to F$ where there is a positive integer d such that $f(x) = x^d$ for all $x \in F$.

Our power function f is bijective if and only if $\gcd(d, q-1) = 1$. Then we say that d is invertible over F (or that f is a power permutation) and we let $e \in \mathbb{Z}_+$ with $e \equiv d^{-1} \pmod{q-1}$ so that $x \mapsto x^e$ is the inverse function of $x \mapsto x^d$.

If $r \in \mathbb{Q}_+$, then we can think of r as an exponent over F if r in reduced form is d_1/d_2 with $\gcd(d_2, q-1) = 1$; then $r = d_1/d_2$ is regarded as a positive integer d with $d \equiv d_1 d_2^{-1} \pmod{q-1}$.

Cryptographic significance: $x \mapsto x^d$ is arithmetically easy to implement and can be used to scramble data in substitution-boxes in a symmetric cipher.

Earlier encounter with the unit circle

Earlier encounter with the unit circle

The Walsh spectrum of a power function measures its correlation with linear functions (important for linear cryptanalysis).

Earlier encounter with the unit circle

The Walsh spectrum of a power function measures its correlation with linear functions (important for linear cryptanalysis).

For the power function $f\colon F \to F$ with $f(x) = x^d$, this amounts to looking at the character sums

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

for all $a \in F^*$, where $\psi\colon (F,+) \to \mathbb{C}^*$ is the canonical additive character $\psi(x) = \exp(2\pi i \operatorname{Tr}_{F/\mathbb{F}_p}(x)/p)$.

Earlier encounter with the unit circle

The Walsh spectrum of a power function measures its correlation with linear functions (important for linear cryptanalysis).

For the power function $f\colon F \to F$ with $f(x) = x^d$, this amounts to looking at the character sums

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

for all $a \in F^*$, where $\psi\colon (F,+) \to \mathbb{C}^*$ is the canonical additive character $\psi(x) = \exp(2\pi i \operatorname{Tr}_{F/\mathbb{F}_p}(x)/p)$.

Niho's Last Conjecture (1972)

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

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

Earlier encounter with the unit circle (continued)

Helleseth–K.–Li (2021) proved Niho's Last Conjecture by showing that for each $a \in F$, the polynomial

$$g_a(x) = x^7 - ax^4 - a^{2^m} x^3 + 1$$

has 0, 1, 2, 3, or 5 (not 4, 6, or 7) roots on the unit circle of F (the unique subgroup of order $2^m + 1$ in $F^* = \mathbb{F}_{2^{2m}}^*$).

Earlier encounter with the unit circle (continued)

Helleseth–K.–Li (2021) proved Niho's Last Conjecture by showing that for each $a \in F$, the polynomial

$$g_a(x) = x^7 - ax^4 - a^{2^m}x^3 + 1$$

has 0, 1, 2, 3, or 5 (not 4, 6, or 7) roots on the unit circle of F (the unique subgroup of order $2^m + 1$ in $F^* = \mathbb{F}_{2^{2m}}^*$).

Method: organize the roots of $g_a(x)$ in $\overline{F}$ into orbits under a strange action, where a root lies on the unit circle if and only if it is in a singleton orbit.

Earlier encounter with the unit circle (continued)

Helleseth–K.–Li (2021) proved Niho's Last Conjecture by showing that for each $a \in F$, the polynomial

$$g_a(x) = x^7 - ax^4 - a^{2^m}x^3 + 1$$

has 0, 1, 2, 3, or 5 (not 4, 6, or 7) roots on the unit circle of F (the unique subgroup of order $2^m + 1$ in $F^* = \mathbb{F}_{2^{2m}}^*$).

Method: organize the roots of $g_a(x)$ in $\overline{F}$ into orbits under a strange action, where a root lies on the unit circle if and only if it is in a singleton orbit.

Prove that the total number of orbits is even by calculating a strange quantity associated with the orbits—involves expressing a degree 42 symmetric polynomial in seven variables as a sum of 218 products of elementary symmetric polynomials.

Earlier encounter with the unit circle (continued)

Helleseth–K.–Li (2021) proved Niho's Last Conjecture by showing that for each $a \in F$, the polynomial

$$g_a(x) = x^7 - ax^4 - a^{2^m} x^3 + 1$$

has 0, 1, 2, 3, or 5 (not 4, 6, or 7) roots on the unit circle of F (the unique subgroup of order $2^m + 1$ in $F^* = \mathbb{F}_{2^{2m}}^*$).

Method: organize the roots of $g_a(x)$ in $\overline{F}$ into orbits under a strange action, where a root lies on the unit circle if and only if it is in a singleton orbit.

Prove that the total number of orbits is even by calculating a strange quantity associated with the orbits—involves expressing a degree 42 symmetric polynomial in seven variables as a sum of 218 products of elementary symmetric polynomials.

Having precisely 4, 6, or 7 singleton orbits is impossible because the total number of orbits is even.

Differential multiplicities

Let $f\colon F \to F$ be a function (e.g., the power function $f(x) = x^d$).

Differential multiplicities

Let $f\colon F \to F$ be a function (e.g., the power function $f(x) = x^d$).

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

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

Differential multiplicities

Let $f\colon F \to F$ be a function (e.g., the power function $f(x) = x^d$).

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

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

or equivalently

$$\begin{aligned} \delta_f(a, b) &= |\{x \in F : f(x+a) - f(x) = b\}| \\ &= |\{x \in F : (\Delta_a f)(x) = b\}| \\ &= |(\Delta_a f)^{-1}(\{b\})|, \end{aligned}$$

where Δ_a is the discrete derivative in direction a, i.e., $\Delta_a f\colon F \to F$ is the function with $(\Delta_a f)(x) = f(x+a) - f(x)$.

Differential multiplicities

Let $f\colon F \to F$ be a function (e.g., the power function $f(x) = x^d$).

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

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

or equivalently

$$\begin{aligned} \delta_f(a, b) &= |\{x \in F : f(x + a) - f(x) = b\}| \\ &= |\{x \in F : (\Delta_a f)(x) = b\}| \\ &= |(\Delta_a f)^{-1}(\{b\})|, \end{aligned}$$

where Δ_a is the discrete derivative in direction a, i.e., $\Delta_a f\colon F \to F$ is the function with $(\Delta_a f)(x) = f(x + a) - f(x)$.

We do not typically consider $a = 0$ because $\Delta_0 f$ is the zero function.

Differential spectrum

$f\colon F \to F$ and $\Delta_a f\colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$

differential multiplicity: $\delta_f(a,b) = |(\Delta_a f)^{-1}(\{b\})|$

Differential spectrum

$f\colon F \to F$ and $\Delta_a f\colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$

differential multiplicity: $\delta_f(a,b) = |(\Delta_a f)^{-1}(\{b\})|$

The differential spectrum of f is the multiset

$$[\![\delta_f(a,b) : (a,b) \in F^* \times F]\!].$$

Differential spectrum

$f\colon F \to F$ and $\Delta_a f\colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$

differential multiplicity: $\delta_f(a,b) = |(\Delta_a f)^{-1}(\{b\})|$

The differential spectrum of f is the multiset

$$[\![\delta_f(a,b) : (a,b) \in F^* \times F]\!].$$

The differential uniformity of f is the largest element of the differential spectrum

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

Differential spectrum

$f\colon F \to F$ and $\Delta_a f\colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$

differential multiplicity: $\delta_f(a, b) = |(\Delta_a f)^{-1}(\{b\})|$

The differential spectrum of f is the multiset

$$[\![\delta_f(a, b) : (a, b) \in F^* \times F]\!].$$

The differential uniformity of f is the largest element of the differential spectrum

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

Want δ_f as as small as possible to counter differential cryptanalysis.

Functions with low differential uniformity

$f\colon F \to F$ and $\Delta_a f\colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$

differential multiplicity: $\delta_f(a,b) = |(\Delta_a f)^{-1}(\{b\})|$

differential uniformity: $\delta_f = \max_{(a,b)\in F^*\times F} \delta_f(a,b)$

Functions with low differential uniformity

$f\colon F \to F$ and $\Delta_a f\colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$

differential multiplicity: $\delta_f(a,b) = |(\Delta_a f)^{-1}(\{b\})|$

differential uniformity: $\delta_f = \max_{(a,b)\in F^*\times F} \delta_f(a,b)$

Perfect nonlinear (PN) or planar function: $\Delta_a f$ is a permutation for every $a \in F^*$, so $\delta_f = 1$.

Functions with low differential uniformity

$f\colon F \to F$ and $\Delta_a f\colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$

differential multiplicity: $\delta_f(a,b) = |(\Delta_a f)^{-1}(\{b\})|$

differential uniformity: $\delta_f = \max_{(a,b)\in F^*\times F} \delta_f(a,b)$

Perfect nonlinear (PN) or planar function: $\Delta_a f$ is a permutation for every $a \in F^*$, so $\delta_f = 1$.

A planar function $f\colon F \to F$ yields an affine plane with set of points $F \times F$ and lines $L_{a,b} = \{(x, f(x-a)+b) : x \in F\}$ and $L_a = \{(a,y) : y \in F\}$ for all $a, b \in F$.

Functions with low differential uniformity

$f\colon F \to F$ and $\Delta_a f\colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$

differential multiplicity: $\delta_f(a,b) = |(\Delta_a f)^{-1}(\{b\})|$

differential uniformity: $\delta_f = \max_{(a,b)\in F^*\times F} \delta_f(a,b)$

Perfect nonlinear (PN) or planar function: $\Delta_a f$ is a permutation for every $a \in F^*$, so $\delta_f = 1$.

A planar function $f\colon F \to F$ yields an affine plane with set of points $F \times F$ and lines $L_{a,b} = \{(x, f(x-a)+b) : x \in F\}$ and $L_a = \{(a,y) : y \in F\}$ for all $a, b \in F$.

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

Functions with low differential uniformity

$f\colon F \to F$ and $\Delta_a f\colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$

differential multiplicity: $\delta_f(a,b) = |(\Delta_a f)^{-1}(\{b\})|$

differential uniformity: $\delta_f = \max_{(a,b)\in F^* \times F} \delta_f(a,b)$

Perfect nonlinear (PN) or planar function: $\Delta_a f$ is a permutation for every $a \in F^*$, so $\delta_f = 1$.

A planar function $f\colon F \to F$ yields an affine plane with set of points $F \times F$ and lines $L_{a,b} = \{(x, f(x-a)+b) : x \in F\}$ and $L_a = \{(a,y) : y \in F\}$ for all $a, b \in F$.

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

The next best possible is an almost perfect nonlinear (APN) function: $\delta_f = 2$.

Functions with low differential uniformity

$f\colon F \to F$ and $\Delta_a f\colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$

differential multiplicity: $\delta_f(a,b) = |(\Delta_a f)^{-1}(\{b\})|$

differential uniformity: $\delta_f = \max_{(a,b)\in F^*\times F} \delta_f(a,b)$

Perfect nonlinear (PN) or planar function: $\Delta_a f$ is a permutation for every $a \in F^*$, so $\delta_f = 1$.

A planar function $f\colon F \to F$ yields an affine plane with set of points $F \times F$ and lines $L_{a,b} = \{(x, f(x-a)+b) : x \in F\}$ and $L_a = \{(a,y) : y \in F\}$ for all $a, b \in F$.

PN functions exist only if char(F) is odd; are never permutations.

The next best possible is an almost perfect nonlinear (APN) function: $\delta_f = 2$.

There are APN functions in both even and odd characteristics, and some are permutations.

Reduced differential spectrum of a power function

For f a power function $f(x) = x^d$ on F and $a \in F^*$ and $b \in F$,

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

Reduced differential spectrum of a power function

For f a power function $f(x) = x^d$ on F and $a \in F^*$ and $b \in F$,

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

So we define the discrete derivative $\Delta = \Delta_1$ with

$$(\Delta f)(x) = f(x + 1) - f(x)$$

Reduced differential spectrum of a power function

For f a power function $f(x) = x^d$ on F and $a \in F^*$ and $b \in F$,

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

So we define the discrete derivative $\Delta = \Delta_1$ with

$$(\Delta f)(x) = f(x+1) - f(x)$$

and for each $c \in F$, we define the differential multiplicity for $f(x) = x^d$ over F at c to be

$$\delta_f(c) = \delta_f(1, c) = |(\Delta_1 f)^{-1}(\{c\})| = |(\Delta f)^{-1}(\{c\})|,$$

Reduced differential spectrum of a power function

For f a power function $f(x) = x^d$ on F and $a \in F^*$ and $b \in F$,

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

So we define the discrete derivative $\Delta = \Delta_1$ with

$$(\Delta f)(x) = f(x+1) - f(x)$$

and for each $c \in F$, we define the differential multiplicity for $f(x) = x^d$ over F at c to be

$$\delta_f(c) = \delta_f(1,c) = |(\Delta_1 f)^{-1}(\{c\})| = |(\Delta f)^{-1}(\{c\})|,$$

and we define the the reduced differential spectrum of $f(x) = x^d$ over F to be the multiset

$$[\![\delta_f(c) : c \in F]\!] = [\![|(\Delta f)^{-1}(\{c\})| : c \in F]\!],$$

Reduced differential spectrum of a power function

For f a power function $f(x) = x^d$ on F and $a \in F^*$ and $b \in F$,

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

So we define the discrete derivative $\Delta = \Delta_1$ with

$$(\Delta f)(x) = f(x+1) - f(x)$$

and for each $c \in F$, we define the differential multiplicity for $f(x) = x^d$ over F at c to be

$$\delta_f(c) = \delta_f(1,c) = |(\Delta_1 f)^{-1}(\{c\})| = |(\Delta f)^{-1}(\{c\})|,$$

and we define the the reduced differential spectrum of $f(x) = x^d$ over F to be the multiset

$$[\![\delta_f(c) : c \in F]\!] = [\![|(\Delta f)^{-1}(\{c\})| : c \in F]\!],$$

and if you scale up all the frequencies by $|F^*|$, then you obtain the differential spectrum of f ($[\![\delta_f(a,b) : (a,b) \in F^* \times F]\!]$).

Reduced differential spectra of APN power functions

The reduced differential spectrum of $f(x) = x^d$ over F is $[\![|(\Delta f)^{-1}(\{c\})| : c \in F]\!]$, so it has $|F| = q$ elements.

Reduced differential spectra of APN power functions

The reduced differential spectrum of $f(x) = x^d$ over F is $\llbracket |(\Delta f)^{-1}(\{c\})| : c \in F \rrbracket$, so it has $|F| = q$ elements.

Since the fibers $(\Delta f)^{-1}(\{c\})$ disjointly cover the domain F of Δf, summing the reduced differential spectrum also yields $|F| = q$.

Reduced differential spectra of APN power functions

The reduced differential spectrum of $f(x) = x^d$ over F is $[\![|(\Delta f)^{-1}(\{c\})| : c \in F]\!]$, so it has $|F| = q$ elements.

Since the fibers $(\Delta f)^{-1}(\{c\})$ disjointly cover the domain F of Δf, summing the reduced differential spectrum also yields $|F| = q$.

If we write a reduced differential spectrum as $n_1[a_1] + \cdots + n_t[a_t]$ (meaning that it has n_j instances of a_j for each j), then

$$\sum_{j=1}^{t} n_j = q \quad \text{and} \quad \sum_{j=1}^{t} n_j a_j = q,$$

so the average differential multiplicity is 1.

Reduced differential spectra of APN power functions

The reduced differential spectrum of $f(x) = x^d$ over F is $[\![|(\Delta f)^{-1}(\{c\})| : c \in F]\!]$, so it has $|F| = q$ elements.

Since the fibers $(\Delta f)^{-1}(\{c\})$ disjointly cover the domain F of Δf, summing the reduced differential spectrum also yields $|F| = q$.

If we write a reduced differential spectrum as $n_1[a_1] + \cdots + n_t[a_t]$ (meaning that it has n_j instances of a_j for each j), then

$$\sum_{j=1}^{t} n_j = q \quad \text{and} \quad \sum_{j=1}^{t} n_j a_j = q,$$

so the average differential multiplicity is 1.

So an APN power function f over F has reduced spectrum

$$\frac{q-N}{2}\,[0] + N\,[1] + \frac{q-N}{2}\,[2],$$

where $N = 0$ when if $\mathrm{char}(F) = 2$. When $\mathrm{char}(F)$ is odd, N is odd, with $N = 1$ when d is odd, but N can be larger when d is even.

Our main result

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ *and let* $f\colon F \to F$ *with* $f(x) = x^{(3^n+1)/(3^k+1)}$, *where* $n > 1$ *is odd,* k *is nonnegative and even, and* $\gcd(n,k) = 1$.

Our main result

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ *and let* $f \colon F \to F$ *with* $f(x) = x^{(3^n+1)/(3^k+1)}$*, where* $n > 1$ *is odd,* k *is nonnegative and even, and* $\gcd(n, k) = 1$*. Then for every* $c \in F$*, we have*

$$\left|(\Delta f)^{-1}(\{c\})\right| = \begin{cases} 1 & \text{if } c \in \mathbb{F}_3, \\ 1 + \eta(1 - c^{3^k+1}) & \text{otherwise,} \end{cases}$$

where η *is the quadratic character for* F*: so* $\eta(1 - c^{3^k+1})$ *modulo* 3 *is* $(1 - c^{3^k+1})^{(q-1)/2}$*.*

Our main result

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ *and let* $f\colon F \to F$ *with* $f(x) = x^{(3^n+1)/(3^k+1)}$, *where* $n > 1$ *is odd,* k *is nonnegative and even, and* $\gcd(n, k) = 1$. *Then for every* $c \in F$, *we have*

$$\left|(\Delta f)^{-1}(\{c\})\right| = \begin{cases} 1 & \text{if } c \in \mathbb{F}_3, \\ 1 + \eta(1 - c^{3^k+1}) & \text{otherwise,} \end{cases}$$

where η *is the quadratic character for* F*: so* $\eta(1 - c^{3^k+1})$ *modulo* 3 *is* $(1 - c^{3^k+1})^{(q-1)/2}$.

So f *is an APN function with reduced differential spectrum*

$$\frac{3^n - 3}{2}\,[0] + 3\,[1] + \frac{3^n - 3}{2}\,[2].$$

Our main result

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ *and let* $f \colon F \to F$ *with* $f(x) = x^{(3^n+1)/(3^k+1)}$, *where* $n > 1$ *is odd,* k *is nonnegative and even, and* $\gcd(n, k) = 1$. *Then for every* $c \in F$, *we have*

$$\left|(\Delta f)^{-1}(\{c\})\right| = \begin{cases} 1 & \text{if } c \in \mathbb{F}_3, \\ 1 + \eta(1 - c^{3^k+1}) & \text{otherwise,} \end{cases}$$

where η *is the quadratic character for* F*: so* $\eta(1 - c^{3^k+1})$ *modulo 3 is* $(1 - c^{3^k+1})^{(q-1)/2}$.

So f *is an APN function with reduced differential spectrum*

$$\frac{3^n - 3}{2}\,[0] + 3\,[1] + \frac{3^n - 3}{2}\,[2].$$

Given any $c \in F$, *there is a algorithm for determining which elements lie in* $(\Delta f)^{-1}(\{c\})$ *using* $O(n) = O(\log q)$ *operations (where an operation is either one the four field operations of* F *or an exponentiation of an element of* F *to some power).*

Permuting fibers

Lemma

Let $g\colon A \to B$, let σ be a permutation of A, and let $f = g \circ \sigma$. Then for each $b \in B$ we have

$$f^{-1}(\{b\}) = \sigma^{-1}(g^{-1}(\{b\})),$$

so that the multiset of cardinalities of fibers of f is the same as the multiset of cardinalities of fibers of g.

Permuting fibers

Lemma

Let $g \colon A \to B$, let σ be a permutation of A, and let $f = g \circ \sigma$. Then for each $b \in B$ we have

$$f^{-1}(\{b\}) = \sigma^{-1}(g^{-1}(\{b\})),$$

so that the multiset of cardinalities of fibers of f is the same as the multiset of cardinalities of fibers of g.

Lemma

Let $g \colon A \to B$, let π be a permutation of B, and let $f = \pi \circ g$. Then for each $b \in B$ we have

$$f^{-1}(\{b\}) = g^{-1}(\{\pi^{-1}(b)\}),$$

so that the multiset of cardinalities of fibers of f is the same as the multiset of cardinalities of fibers of g.

Permuting fibers of power functions with fractional powers

Let $f(x) = x^d$ be a power function over F where $d = d_1/d_2$ for positive integers d_1, d_2 with $\gcd(d_2, q-1) = 1$.

Permuting fibers of power functions with fractional powers

Let $f(x) = x^d$ be a power function over F where $d = d_1/d_2$ for positive integers d_1, d_2 with $\gcd(d_2, q-1) = 1$.

Let $\pi\colon F \to F$ and $\sigma\colon F \to F$ be the permutations with $\pi(x) = x^{q-2} + 1$ and $\sigma(x) = x^{d_2}$.

Permuting fibers of power functions with fractional powers

Let $f(x) = x^d$ be a power function over F where $d = d_1/d_2$ for positive integers d_1, d_2 with $\gcd(d_2, q-1) = 1$.

Let $\pi \colon F \to F$ and $\sigma \colon F \to F$ be the permutations with $\pi(x) = x^{q-2} + 1$ and $\sigma(x) = x^{d_2}$.

Let $f_1 = (\Delta f) \circ \pi^{-1}$ and $f_2 = \sigma \circ f_1 \circ \sigma$ and $f_3 = f_2 \circ \pi$.

Permuting fibers of power functions with fractional powers

Let $f(x) = x^d$ be a power function over F where $d = d_1/d_2$ for positive integers d_1, d_2 with $\gcd(d_2, q-1) = 1$.

Let $\pi\colon F \to F$ and $\sigma\colon F \to F$ be the permutations with $\pi(x) = x^{q-2} + 1$ and $\sigma(x) = x^{d_2}$.

Let $f_1 = (\Delta f) \circ \pi^{-1}$ and $f_2 = \sigma \circ f_1 \circ \sigma$ and $f_3 = f_2 \circ \pi$.

Hertel and Pott (2008) inspire the transformation to f_1 and f_2, and

Permuting fibers of power functions with fractional powers

Let $f(x) = x^d$ be a power function over F where $d = d_1/d_2$ for positive integers d_1, d_2 with $\gcd(d_2, q-1) = 1$.

Let $\pi\colon F \to F$ and $\sigma\colon F \to F$ be the permutations with $\pi(x) = x^{q-2} + 1$ and $\sigma(x) = x^{d_2}$.

Let $f_1 = (\Delta f) \circ \pi^{-1}$ and $f_2 = \sigma \circ f_1 \circ \sigma$ and $f_3 = f_2 \circ \pi$.

Hertel and Pott (2008) inspire the transformation to f_1 and f_2, and

$$f_1(x) = \frac{x^d - 1}{(x-1)^d}$$
$$f_2(x) = \frac{(x^{d_1} - 1)^{d_2}}{(x^{d_2} - 1)^{d_1}}$$
$$f_3(x) = \frac{((x+1)^{d_1} - x^{d_1})^{d_2}}{((x+1)^{d_2} - x^{d_2})^{d_1}}.$$

Permuting fibers of power functions with fractional powers

Let $f(x) = x^d$ be a power function over F where $d = d_1/d_2$ for positive integers d_1, d_2 with $\gcd(d_2, q-1) = 1$.

Let $\pi\colon F \to F$ and $\sigma\colon F \to F$ be the permutations with $\pi(x) = x^{q-2} + 1$ and $\sigma(x) = x^{d_2}$.

Let $f_1 = (\Delta f) \circ \pi^{-1}$ and $f_2 = \sigma \circ f_1 \circ \sigma$ and $f_3 = f_2 \circ \pi$.

Hertel and Pott (2008) inspire the transformation to f_1 and f_2, and

$$f_1(x) = \frac{x^d - 1}{(x-1)^d}$$

$$f_2(x) = \frac{(x^{d_1} - 1)^{d_2}}{(x^{d_2} - 1)^{d_1}}$$

$$f_3(x) = \frac{((x+1)^{d_1} - x^{d_1})^{d_2}}{((x+1)^{d_2} - x^{d_2})^{d_1}}.$$

The multiset of cardinalities of the fibers of f_1, f_2, or f_3 is the same as the multiset of cardinalities of the fibers of Δf.

Permuting fibers of power functions with fractional powers (continued)

$f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$

$$f_3(x) = (\sigma \circ (\Delta f) \circ \pi^{-1} \circ \sigma \circ \pi)(x) = \frac{((x+1)^{d_1} - x^{d_1})^{d_2}}{((x+1)^{d_2} - x^{d_2})^{d_1}}$$

has the same multiset of cardinalities of fibers as Δf.

Permuting fibers of power functions with fractional powers (continued)

$f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$

$$f_3(x) = (\sigma \circ (\Delta f) \circ \pi^{-1} \circ \sigma \circ \pi)(x) = \frac{((x+1)^{d_1} - x^{d_1})^{d_2}}{((x+1)^{d_2} - x^{d_2})^{d_1}}$$

has the same multiset of cardinalities of fibers as Δf.

Now suppose that $\mathrm{char}(F)$ is odd, and let $\tau\colon F \to F$ be the permutation with $\tau(x) = (x-2)/4$.

Permuting fibers of power functions with fractional powers (continued)

$f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$

$$f_3(x) = (\sigma \circ (\Delta f) \circ \pi^{-1} \circ \sigma \circ \pi)(x) = \frac{((x+1)^{d_1} - x^{d_1})^{d_2}}{((x+1)^{d_2} - x^{d_2})^{d_1}}$$

has the same multiset of cardinalities of fibers as Δf.

Now suppose that $\mathrm{char}(F)$ is odd, and let $\tau \colon F \to F$ be the permutation with $\tau(x) = (x-2)/4$.

Then the function $f_4 = f_3 \circ \tau$ has

Permuting fibers of power functions with fractional powers (continued)

$f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$

$$f_3(x) = (\sigma \circ (\Delta f) \circ \pi^{-1} \circ \sigma \circ \pi)(x) = \frac{((x+1)^{d_1} - x^{d_1})^{d_2}}{((x+1)^{d_2} - x^{d_2})^{d_1}}$$

has the same multiset of cardinalities of fibers as Δf.

Now suppose that $\mathrm{char}(F)$ is odd, and let $\tau \colon F \to F$ be the permutation with $\tau(x) = (x-2)/4$.

Then the function $f_4 = f_3 \circ \tau$ has

$$f_4(x) = \frac{((x+2)^{d_1} - (x-2)^{d_1})^{d_2}}{((x+2)^{d_2} - (x-2)^{d_2})^{d_1}}.$$

Permuting fibers of power functions with fractional powers (continued)

$f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$

$$f_3(x) = (\sigma \circ (\Delta f) \circ \pi^{-1} \circ \sigma \circ \pi)(x) = \frac{((x+1)^{d_1} - x^{d_1})^{d_2}}{((x+1)^{d_2} - x^{d_2})^{d_1}}$$

has the same multiset of cardinalities of fibers as Δf.

Now suppose that $\mathrm{char}(F)$ is odd, and let $\tau \colon F \to F$ be the permutation with $\tau(x) = (x-2)/4$.

Then the function $f_4 = f_3 \circ \tau$ has

$$f_4(x) = \frac{((x+2)^{d_1} - (x-2)^{d_1})^{d_2}}{((x+2)^{d_2} - (x-2)^{d_2})^{d_1}}.$$

The multiset of cardinalities of the fibers of f_4 is the same as the multiset of cardinalities of the fibers of Δf.

Substituting $x + x^{-1}$

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$

$$f_4(x) = \frac{((x+2)^{d_1} - (x-2)^{d_1})^{d_2}}{((x+2)^{d_2} - (x-2)^{d_2})^{d_1}}.$$

has the same multiset of cardinalities of fibers as Δf.

Substituting $x + x^{-1}$

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$

$$f_4(x) = \frac{((x+2)^{d_1} - (x-2)^{d_1})^{d_2}}{((x+2)^{d_2} - (x-2)^{d_2})^{d_1}}.$$

has the same multiset of cardinalities of fibers as Δf.

Coulter-Matthews (1997) (and ultimately Dickson) inspire us to consider an $x \in \overline{F}$ with $x + x^{-1} \in F$ and obtain

$$\begin{aligned} f_4(x+x^{-1}) &= \frac{((x+2+x^{-1})^{d_1} - (x-2+x^{-1})^{d_1})^{d_2}}{((x+2+x^{-1})^{d_2} - (x-2+x^{-1})^{d_2})^{d_1}} \\ &= \frac{((x^2+2x+1)^{d_1} - (x^2-2x+1)^{d_1})^{d_2}}{((x^2+2x+1)^{d_2} - (x^2-2x+1)^{d_2})^{d_1}} \\ &= \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}. \end{aligned}$$

Substituting $x + x^{-1}$ (continued)

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, and x is such that $x + x^{-1} \in F$

$$f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Substituting $x + x^{-1}$ (continued)

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, and x is such that $x + x^{-1} \in F$

$$f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Useful when d_1 and d_2 are complicated but $2d_1$ and $2d_2$ are simple

Substituting $x + x^{-1}$ (continued)

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, and x is such that $x + x^{-1} \in F$

$$f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Useful when d_1 and d_2 are complicated but $2d_1$ and $2d_2$ are simple

For example, consider our theorem, where the field F is of order 3^n with $n > 1$ odd, and $d = (3^n + 1)/(3^k + 1)$ with k nonnegative and even, and $\gcd(n, k) = 1$.

Substituting $x + x^{-1}$ (continued)

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, and x is such that $x + x^{-1} \in F$

$$f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Useful when d_1 and d_2 are complicated but $2d_1$ and $2d_2$ are simple

For example, consider our theorem, where the field F is of order 3^n with $n > 1$ odd, and $d = (3^n + 1)/(3^k + 1)$ with k nonnegative and even, and $\gcd(n, k) = 1$.

Then $d = d_1/d_2$ with $d_1 = (3^n + 1)/2$ and $d_2 = (3^k + 1)/2$.

Substituting $x + x^{-1}$ (continued)

$\mathrm{char}(F)$ odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, and x is such that $x + x^{-1} \in F$

$$f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Useful when d_1 and d_2 are complicated but $2d_1$ and $2d_2$ are simple

For example, consider our theorem, where the field F is of order 3^n with $n > 1$ odd, and $d = (3^n+1)/(3^k+1)$ with k nonnegative and even, and $\gcd(n, k) = 1$.

Then $d = d_1/d_2$ with $d_1 = (3^n+1)/2$ and $d_2 = (3^k+1)/2$.

Taking an element like $x + 1$ to the d_2th power is complicated while taking $x + 1$ to the $(2d_2)$th power is relatively simple because

$$\begin{aligned}(x+1)^{2d_2} &= (x+1)^{3^k+1} = (x+1)^{3^k}(x+1) \\ &= (x^{3^k}+1)(x+1) = x^{3^k+1} + x^{3^k} + x + 1.\end{aligned}$$

Substituting $x + x^{-1}$ (continued)

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, and x is such that $x + x^{-1} \in F$

$$f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Substituting $x + x^{-1}$ (continued)

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, and x is such that $x + x^{-1} \in F$

$$f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Question: where should x come from to make $x + x^{-1}$ reside in F?

Substituting $x + x^{-1}$ (continued)

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, and x is such that $x + x^{-1} \in F$

$$f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Question: where should x come from to make $x + x^{-1}$ reside in F?

But first...if x and y are nonzero elements of some field K then

$$x + x^{-1} = y + y^{-1}$$

Substituting $x + x^{-1}$ (continued)

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, and x is such that $x + x^{-1} \in F$

$$f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Question: where should x come from to make $x + x^{-1}$ reside in F?

But first...if x and y are nonzero elements of some field K then

$$x + x^{-1} = y + y^{-1}$$

if and only if

$$(x-y)\left(1 - \frac{1}{xy}\right) = 0,$$

Substituting $x + x^{-1}$ (continued)

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, and x is such that $x + x^{-1} \in F$

$$f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Question: where should x come from to make $x + x^{-1}$ reside in F?

But first...if x and y are nonzero elements of some field K then

$$x + x^{-1} = y + y^{-1}$$

if and only if

$$(x - y)\left(1 - \frac{1}{xy}\right) = 0,$$

which is true if and only if

$$x \in \{y, y^{-1}\}.$$

Substituting $x + x^{-1}$ (continued)

char(F) odd, $f(x) = x^d$ with $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, and x is such that $x + x^{-1} \in F$

$$f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Question: where should x come from to make $x + x^{-1}$ reside in F?

But first...if x and y are nonzero elements of some field K then

$$x + x^{-1} = y + y^{-1}$$

if and only if

$$(x - y)\left(1 - \frac{1}{xy}\right) = 0,$$

which is true if and only if

$$x \in \{y, y^{-1}\}.$$

So all nonempty fibers of the map $x \mapsto x + x^{-1}$ have two points in them, except for $\{1\}$ and $\{-1\}$.

Inspiration from $\mathbb{C}$

Consider how $x \mapsto x + x^{-1}$ maps $\mathbb{C}^*$ into $\mathbb{C}$.

Inspiration from $\mathbb{C}$

Consider how $x \mapsto x + x^{-1}$ maps $\mathbb{C}^*$ into $\mathbb{C}$.

The map is surjective because $\mathbb{C}$ is algebraically closed.

Inspiration from $\mathbb{C}$

Consider how $x \mapsto x + x^{-1}$ maps $\mathbb{C}^*$ into $\mathbb{C}$.

The map is surjective because $\mathbb{C}$ is algebraically closed.

So by the previous slide, every element has two preimages under this map, except for 2 and -2, which have preimages $\{1\}$ and $\{-1\}$, respectively.

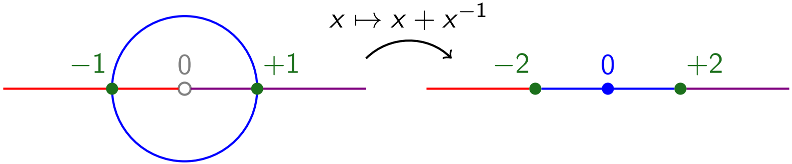
Inspiration from $\mathbb{C}$

Consider how $x \mapsto x + x^{-1}$ maps $\mathbb{C}^*$ into $\mathbb{C}$.

The map is surjective because $\mathbb{C}$ is algebraically closed.

So by the previous slide, every element has two preimages under this map, except for 2 and -2, which have preimages $\{1\}$ and $\{-1\}$, respectively.

The preimage of the real axis is the union of the punctured real axis, $\mathbb{R}^*$, and the complex unit circle $\mathbb{T}$:



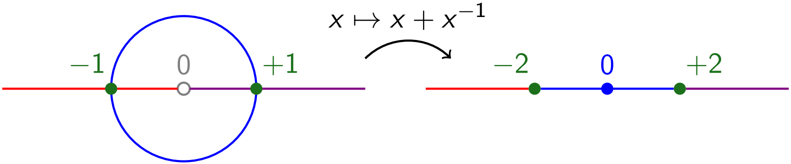
Inspiration from $\mathbb{C}$

Consider how $x \mapsto x + x^{-1}$ maps $\mathbb{C}^*$ into $\mathbb{C}$.

The map is surjective because $\mathbb{C}$ is algebraically closed.

So by the previous slide, every element has two preimages under this map, except for 2 and -2, which have preimages $\{1\}$ and $\{-1\}$, respectively.

The preimage of the real axis is the union of the punctured real axis, $\mathbb{R}^*$, and the complex unit circle $\mathbb{T}$:



The disjoint union

$$\mathbb{R}^* \sqcup \mathbb{T} = \{(r, \mathbb{R}^*) : r \in \mathbb{R}^*\} \cup \{(t, \mathbb{T}) : t \in \mathbb{T}\}$$

is mapped by $(x, S) \mapsto x + x^{-1}$ to give a double cover of $\mathbb{R}$.

A double cover of F

$E = \mathbb{F}_{q^2}$ is the quadratic extension of $F = \mathbb{F}_q$. The unit circle of E, denoted U_E, is the unique subgroup of E^* of order $q + 1$:

$$U_E = \{x \in E^* : x^{q+1} = 1\}.$$

A double cover of F

$E = \mathbb{F}_{q^2}$ is the quadratic extension of $F = \mathbb{F}_q$. The unit circle of E, denoted U_E, is the unique subgroup of E^* of order $q+1$:

$$U_E = \{x \in E^* : x^{q+1} = 1\}.$$

characteristic p	characteristic 0
F	$\mathbb{R}$
E	$\mathbb{C}$
$x \mapsto x^q$	$x \mapsto \overline{x}$
$U_E = \{x \in E^* : xx^q = 1\}$	$\mathbb{T} = \{x \in \mathbb{C}^* : x\overline{x} = 1\}$
$F^* \sqcup U_E$	$\mathbb{R}^* \sqcup \mathbb{T}$

A double cover of F

$E = \mathbb{F}_{q^2}$ is the quadratic extension of $F = \mathbb{F}_q$. The unit circle of E, denoted U_E, is the unique subgroup of E^* of order $q+1$:

$$U_E = \{x \in E^* : x^{q+1} = 1\}.$$

characteristic p	characteristic 0
F	$\mathbb{R}$
E	$\mathbb{C}$
$x \mapsto x^q$	$x \mapsto \overline{x}$
$U_E = \{x \in E^* : xx^q = 1\}$	$\mathbb{T} = \{x \in \mathbb{C}^* : x\overline{x} = 1\}$
$F^* \sqcup U_E$	$\mathbb{R}^* \sqcup \mathbb{T}$

Our disjoint union has $(q-1)+(q+1) = 2q$ elements

$$F^* \sqcup U_E = \{(a, F^*) : a \in F^*\} \cup \{(b, U_E) : b \in U_E\}.$$

A double cover of F

$E = \mathbb{F}_{q^2}$ is the quadratic extension of $F = \mathbb{F}_q$. The unit circle of E, denoted U_E, is the unique subgroup of E^* of order $q+1$:

$$U_E = \{x \in E^* : x^{q+1} = 1\}.$$

characteristic p	characteristic 0
F	$\mathbb{R}$
E	$\mathbb{C}$
$x \mapsto x^q$	$x \mapsto \overline{x}$
$U_E = \{x \in E^* : xx^q = 1\}$	$\mathbb{T} = \{x \in \mathbb{C}^* : x\overline{x} = 1\}$
$F^* \sqcup U_E$	$\mathbb{R}^* \sqcup \mathbb{T}$

Our disjoint union has $(q-1)+(q+1) = 2q$ elements

$$F^* \sqcup U_E = \{(a, F^*) : a \in F^*\} \cup \{(b, U_E) : b \in U_E\}.$$

Then the map $\lambda\colon F^* \sqcup U_E \to F$ with $\lambda(x, S) = x + x^{-1}$ is a double cover of F (i.e., λ is 2-to-1 from $F^* \sqcup U_E$ to F).

A double cover of F

$E = \mathbb{F}_{q^2}$ is the quadratic extension of $F = \mathbb{F}_q$. The unit circle of E, denoted U_E, is the unique subgroup of E^* of order $q+1$:

$$U_E = \{x \in E^* : x^{q+1} = 1\}.$$

characteristic p	characteristic 0
F	$\mathbb{R}$
E	$\mathbb{C}$
$x \mapsto x^q$	$x \mapsto \overline{x}$
$U_E = \{x \in E^* : xx^q = 1\}$	$\mathbb{T} = \{x \in \mathbb{C}^* : x\overline{x} = 1\}$
$F^* \sqcup U_E$	$\mathbb{R}^* \sqcup \mathbb{T}$

Our disjoint union has $(q-1)+(q+1) = 2q$ elements

$$F^* \sqcup U_E = \{(a, F^*) : a \in F^*\} \cup \{(b, U_E) : b \in U_E\}.$$

Then the map $\lambda \colon F^* \sqcup U_E \to F$ with $\lambda(x, S) = x + x^{-1}$ is a double cover of F (i.e., λ is 2-to-1 from $F^* \sqcup U_E$ to F).

Lemma (fiber doubling)

If $g \colon F \to F$, then $|g^{-1}(\{c\})| = \frac{|(g\circ\lambda)^{-1}(\{c\})|}{2}$ for every $c \in F$.

Applying the double cover

If $\mathrm{char}(F)$ is odd and $f(x) = x^d$ over F where $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, then the fibers of Δf are half the size of those of

$$(f_4 \circ \lambda)(x, S) = f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

Applying the double cover

If $\mathrm{char}(F)$ is odd and $f(x) = x^d$ over F where $d = d_1/d_2$ for $d_1, d_2 \in \mathbb{Z}_+$ with $\gcd(d_2, q-1) = 1$, then the fibers of Δf are half the size of those of

$$(f_4 \circ \lambda)(x, S) = f_4(x + x^{-1}) = \frac{((x+1)^{2d_1} - (x-1)^{2d_1})^{d_2}}{((x+1)^{2d_2} - (x-1)^{2d_2})^{d_1}}.$$

When $d = (3^n + 1)/(3^k + 1)$ over $F = \mathbb{F}_{3^n}$ ($n > 1$ odd, $k \geq 0$ even, $\gcd(k, n) = 1$), we have $d_1 = (3^n + 1)/2$ and $d_2 = (3^k + 1)/2$, and then you get a function that is "simple" enough to analyze:

$$(f_4 \circ \lambda)(x, S) = \frac{\left((x+1)^{2d_1} - (x-1)^{2d_1}\right)^{d_2}}{\left((x+1)^{2d_2} - (x-1)^{2d_2}\right)^{d_1}}$$

$$= \frac{\left(\left(x^{3^n+1} + x^{3^n} + x + 1\right) - \left(x^{3^n+1} - x^{3^n} - x + 1\right)\right)^{d_2}}{\left(\left(x^{3^k+1} + x^{3^k} + x + 1\right) - \left(x^{3^k+1} - x^{3^k} - x + 1\right)\right)^{d_1}} = -\frac{(x^{3^n} + x)^{d_2}}{(x^{3^k} + x)^{d_1}}$$

Our main result

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ *and let* $f\colon F \to F$ *with* $f(x) = x^{(3^n+1)/(3^k+1)}$, *where* $n > 1$ *is odd,* k *is nonnegative and even, and* $\gcd(n, k) = 1$.

Our main result

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ *and let* $f \colon F \to F$ *with* $f(x) = x^{(3^n+1)/(3^k+1)}$, *where* $n > 1$ *is odd,* k *is nonnegative and even, and* $\gcd(n, k) = 1$*. Then for every* $c \in F$*, we have*

$$\left|(\Delta f)^{-1}(\{c\})\right| = \begin{cases} 1 & \text{if } c \in \mathbb{F}_3, \\ 1 + \eta(1 - c^{3^k+1}) & \text{otherwise,} \end{cases}$$

where η *is the quadratic character for* F*: so* $\eta(1 - c^{3^k+1})$ *modulo 3 is* $(1 - c^{3^k+1})^{(q-1)/2}$.

Our main result

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ *and let* $f\colon F \to F$ *with* $f(x) = x^{(3^n+1)/(3^k+1)}$, *where* $n > 1$ *is odd,* k *is nonnegative and even, and* $\gcd(n,k) = 1$*. Then for every* $c \in F$*, we have*

$$\left|(\Delta f)^{-1}(\{c\})\right| = \begin{cases} 1 & \text{if } c \in \mathbb{F}_3, \\ 1 + \eta(1 - c^{3^k+1}) & \text{otherwise,} \end{cases}$$

where η *is the quadratic character for* F*: so* $\eta(1 - c^{3^k+1})$ *modulo* 3 *is* $(1 - c^{3^k+1})^{(q-1)/2}$.

So f *is an APN function with reduced differential spectrum*

$$\frac{3^n - 3}{2}\,[0] + 3\,[1] + \frac{3^n - 3}{2}\,[2].$$

Our main result

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ and let $f \colon F \to F$ with $f(x) = x^{(3^n+1)/(3^k+1)}$, where $n > 1$ is odd, k is nonnegative and even, and $\gcd(n,k) = 1$. Then for every $c \in F$, we have

$$\left|(\Delta f)^{-1}(\{c\})\right| = \begin{cases} 1 & \text{if } c \in \mathbb{F}_3, \\ 1 + \eta(1 - c^{3^k+1}) & \text{otherwise,} \end{cases}$$

where η is the quadratic character for F: so $\eta(1 - c^{3^k+1})$ modulo 3 is $(1 - c^{3^k+1})^{(q-1)/2}$.

So f is an APN function with reduced differential spectrum

$$\frac{3^n - 3}{2}\,[0] + 3\,[1] + \frac{3^n - 3}{2}\,[2].$$

Given any $c \in F$, there is a algorithm for determining which elements lie in $(\Delta f)^{-1}(\{c\})$ using $O(n) = O(\log q)$ operations (where an operation is either one the four field operations of F or an exponentiation of an element of F to some power).

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ and let $f\colon F \to F$ with $f(x) = x^{(3^n+1)/(3^k+1)}$, where $n > 1$ is odd, k is nonnegative and even, and $\gcd(n, k) = 1$.

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ *and let* $f\colon F \to F$ *with* $f(x) = x^{(3^n+1)/(3^k+1)}$, *where* $n > 1$ *is odd,* k *is nonnegative and even, and* $\gcd(n,k) = 1$. *Let* $\epsilon \in \mathbb{Z}_+$ *with* $\epsilon(3^k - 1)/4 \equiv 1 \pmod{(q-1)/2}$.

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ and let $f\colon F \to F$ with $f(x) = x^{(3^n+1)/(3^k+1)}$, where $n > 1$ is odd, k is nonnegative and even, and $\gcd(n,k) = 1$. Let $\epsilon \in \mathbb{Z}_+$ with $\epsilon(3^k-1)/4 \equiv 1 \pmod{(q-1)/2}$. Let

$$p_0(x) = (1 - x^{3^k+1})^{\frac{q+1}{4}} \qquad p_1(x) = (((x+1)^{q-2}+1)^{\frac{3^k+1}{2}} - 1)^{q-2}$$

$$p_2(x) = x^{q-2+\frac{(q-3)\epsilon}{4}}(p_0(x)+1)^{\frac{(3q-1)\epsilon}{4}} \qquad p_3(x) = p_2(x) + p_2(x)^{q-2}$$

$$p_4(x) = p_1(p_3(x)) \qquad p_5(x) = \prod_{j=0}^{n-1}\left((-1)^j p_0(x)^{3^{jk}} + 1\right)$$

$$p_6(x) = \left(p_5(x) - p_5(x)^{q-2}\right)\left(p_5(x) + p_5(x)^{q-2}\right)^{q-2} \qquad p_7(x) = \left(1 - p_6(x)^2\right)^{\frac{q+1}{4}}$$

$$p_8(x) = \left((x-1)^{\frac{q+1}{2}} - (x+1)^{\frac{q+1}{2}}\right)^{\frac{3^k+1}{2}}\left((x-1)^{\frac{3^k+1}{2}} - (x+1)^{\frac{3^k+1}{2}}\right)^{\frac{q-3}{2}}$$

$$p_9(x) = x^{\frac{2q-3^k-3}{2}} p_8(p_7(x)) p_7(x) \qquad p_{10}(x) = p_1(p_9(x))$$

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ and let $f\colon F \to F$ with $f(x) = x^{(3^n+1)/(3^k+1)}$, where $n > 1$ is odd, k is nonnegative and even, and $\gcd(n,k) = 1$. Let $\epsilon \in \mathbb{Z}_+$ with $\epsilon(3^k - 1)/4 \equiv 1 \pmod{(q-1)/2}$. Let

$$p_0(x) = (1 - x^{3^k+1})^{\frac{q+1}{4}} \qquad p_1(x) = (((x+1)^{q-2}+1)^{\frac{3^k+1}{2}} - 1)^{q-2}$$

$$p_2(x) = x^{q-2+\frac{(q-3)\epsilon}{4}} (p_0(x)+1)^{\frac{(3q-1)\epsilon}{4}} \qquad p_3(x) = p_2(x) + p_2(x)^{q-2}$$

$$p_4(x) = p_1(p_3(x)) \qquad p_5(x) = \prod_{j=0}^{n-1} \left((-1)^j p_0(x)^{3^{jk}} + 1\right)$$

$$p_6(x) = \left(p_5(x) - p_5(x)^{q-2}\right)\left(p_5(x) + p_5(x)^{q-2}\right)^{q-2} \qquad p_7(x) = \left(1 - p_6(x)^2\right)^{\frac{q+1}{4}}$$

$$p_8(x) = \left((x-1)^{\frac{q+1}{2}} - (x+1)^{\frac{q+1}{2}}\right)^{\frac{3^k+1}{2}} \left((x-1)^{\frac{3^k+1}{2}} - (x+1)^{\frac{3^k+1}{2}}\right)^{\frac{q-3}{2}}$$

$$p_9(x) = x^{\frac{2q-3^k-3}{2}} p_8(p_7(x)) p_7(x) \qquad p_{10}(x) = p_1(p_9(x))$$

For $c \in F$, consider the fiber $(\Delta f)^{-1}(\{c\})$ of the derivative of f.

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ and let $f\colon F \to F$ with $f(x) = x^{(3^n+1)/(3^k+1)}$, where $n > 1$ is odd, k is nonnegative and even, and $\gcd(n,k) = 1$. Let $\epsilon \in \mathbb{Z}_+$ with $\epsilon(3^k-1)/4 \equiv 1 \pmod{(q-1)/2}$. Let

$$p_0(x) = (1 - x^{3^k+1})^{\frac{q+1}{4}} \qquad p_1(x) = (((x+1)^{q-2}+1)^{\frac{3^k+1}{2}} - 1)^{q-2}$$

$$p_2(x) = x^{q-2+\frac{(q-3)\epsilon}{4}} (p_0(x)+1)^{\frac{(3q-1)\epsilon}{4}} \qquad p_3(x) = p_2(x) + p_2(x)^{q-2}$$

$$p_4(x) = p_1(p_3(x)) \qquad p_5(x) = \prod_{j=0}^{n-1} \left((-1)^j p_0(x)^{3^{jk}} + 1\right)$$

$$p_6(x) = \left(p_5(x) - p_5(x)^{q-2}\right)\left(p_5(x) + p_5(x)^{q-2}\right)^{q-2} \qquad p_7(x) = \left(1 - p_6(x)^2\right)^{\frac{q+1}{4}}$$

$$p_8(x) = \left((x-1)^{\frac{q+1}{2}} - (x+1)^{\frac{q+1}{2}}\right)^{\frac{3^k+1}{2}} \left((x-1)^{\frac{3^k+1}{2}} - (x+1)^{\frac{3^k+1}{2}}\right)^{\frac{q-3}{2}}$$

$$p_9(x) = x^{\frac{2q-3^k-3}{2}} p_8(p_7(x)) p_7(x) \qquad p_{10}(x) = p_1(p_9(x))$$

For $c \in F$, consider the fiber $(\Delta f)^{-1}(\{c\})$ of the derivative of f.

(i) If $(1 - c^{3^k+1})^{(q-1)/2} = -1$, then $(\Delta f)^{-1}(\{c\}) = \emptyset$.

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ and let $f \colon F \to F$ with $f(x) = x^{(3^n+1)/(3^k+1)}$, where $n > 1$ is odd, k is nonnegative and even, and $\gcd(n,k) = 1$. Let $\epsilon \in \mathbb{Z}_+$ with $\epsilon(3^k - 1)/4 \equiv 1 \pmod{(q-1)/2}$. Let

$$p_0(x) = (1 - x^{3^k+1})^{\frac{q+1}{4}} \qquad p_1(x) = (((x+1)^{q-2} + 1)^{\frac{3^k+1}{2}} - 1)^{q-2}$$

$$p_2(x) = x^{q-2+\frac{(q-3)\epsilon}{4}} (p_0(x) + 1)^{\frac{(3q-1)\epsilon}{4}} \qquad p_3(x) = p_2(x) + p_2(x)^{q-2}$$

$$p_4(x) = p_1(p_3(x)) \qquad p_5(x) = \prod_{j=0}^{n-1} \left((-1)^j p_0(x)^{3^{jk}} + 1\right)$$

$$p_6(x) = \left(p_5(x) - p_5(x)^{q-2}\right)\left(p_5(x) + p_5(x)^{q-2}\right)^{q-2} \qquad p_7(x) = \left(1 - p_6(x)^2\right)^{\frac{q+1}{4}}$$

$$p_8(x) = \left((x-1)^{\frac{q+1}{2}} - (x+1)^{\frac{q+1}{2}}\right)^{\frac{3^k+1}{2}} \left((x-1)^{\frac{3^k+1}{2}} - (x+1)^{\frac{3^k+1}{2}}\right)^{\frac{q-3}{2}}$$

$$p_9(x) = x^{\frac{2q-3^k-3}{2}} p_8(p_7(x)) p_7(x) \qquad p_{10}(x) = p_1(p_9(x))$$

For $c \in F$, consider the fiber $(\Delta f)^{-1}(\{c\})$ of the derivative of f.

(i) If $(1 - c^{3^k+1})^{(q-1)/2} = -1$, then $(\Delta f)^{-1}(\{c\}) = \emptyset$.

(ii) Otherwise, $(\Delta f)^{-1}(\{c\}) = \{p_4(c), p_{10}(c)\}$.

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ *and let* $f\colon F \to F$ *with* $f(x) = x^{(3^n+1)/(3^k+1)}$, *where* $n > 1$ *is odd,* k *is nonnegative and even, and* $\gcd(n,k) = 1$. *Let* $\epsilon \in \mathbb{Z}_+$ *with* $\epsilon(3^k - 1)/4 \equiv 1 \pmod{(q-1)/2}$. *Let*

$$p_0(x) = (1 - x^{3^k+1})^{\frac{q+1}{4}} \qquad p_1(x) = (((x+1)^{q-2}+1)^{\frac{3^k+1}{2}} - 1)^{q-2}$$

$$p_2(x) = x^{q-2+\frac{(q-3)\epsilon}{4}}(p_0(x)+1)^{\frac{(3q-1)\epsilon}{4}} \qquad p_3(x) = p_2(x) + p_2(x)^{q-2}$$

$$p_4(x) = p_1(p_3(x)) \qquad p_5(x) = \prod_{j=0}^{n-1}\left((-1)^j p_0(x)^{3^{jk}} + 1\right)$$

$$p_6(x) = \left(p_5(x) - p_5(x)^{q-2}\right)\left(p_5(x) + p_5(x)^{q-2}\right)^{q-2} \qquad p_7(x) = \left(1 - p_6(x)^2\right)^{\frac{q+1}{4}}$$

$$p_8(x) = \left((x-1)^{\frac{q+1}{2}} - (x+1)^{\frac{q+1}{2}}\right)^{\frac{3^k+1}{2}}\left((x-1)^{\frac{3^k+1}{2}} - (x+1)^{\frac{3^k+1}{2}}\right)^{\frac{q-3}{2}}$$

$$p_9(x) = x^{\frac{2q-3^k-3}{2}} p_8(p_7(x)) p_7(x) \qquad p_{10}(x) = p_1(p_9(x))$$

For $c \in F$, *consider the fiber* $(\Delta f)^{-1}(\{c\})$ *of the derivative of f.*

(i) *If* $(1 - c^{3^k+1})^{(q-1)/2} = -1$, *then* $(\Delta f)^{-1}(\{c\}) = \emptyset$.

(ii) *Otherwise,* $(\Delta f)^{-1}(\{c\}) = \{p_4(c), p_{10}(c)\}$. *If* $c \in \mathbb{F}_3$, *then* $p_4(c) = p_{10}(c) = 1 - c$, *but if* $c \notin \mathbb{F}_3$, *then* $p_4(c)$ *and* $p_{10}(c)$ *are distinct elements of* $F \setminus \mathbb{F}_3$.

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ and let $f\colon F \to F$ with $f(x) = x^{(3^n+1)/(3^k+1)}$, where $n > 1$ is odd, k is nonnegative and even, and $\gcd(n,k) = 1$. Let $\epsilon \in \mathbb{Z}_+$ with $\epsilon(3^k - 1)/4 \equiv 1 \pmod{(q-1)/2}$. Let

$$p_0(x) = (1 - x^{3^k+1})^{\frac{q+1}{4}} \qquad p_1(x) = (((x+1)^{q-2}+1)^{\frac{3^k+1}{2}} - 1)^{q-2}$$

$$p_2(x) = x^{q-2+\frac{(q-3)\epsilon}{4}}(p_0(x)+1)^{\frac{(3q-1)\epsilon}{4}} \qquad p_3(x) = p_2(x) + p_2(x)^{q-2}$$

$$p_4(x) = p_1(p_3(x)) \qquad p_5(x) = \prod_{j=0}^{n-1}\left((-1)^j p_0(x)^{3^{jk}} + 1\right)$$

$$p_6(x) = \left(p_5(x) - p_5(x)^{q-2}\right)\left(p_5(x) + p_5(x)^{q-2}\right)^{q-2} \qquad p_7(x) = \left(1 - p_6(x)^2\right)^{\frac{q+1}{4}}$$

$$p_8(x) = \left((x-1)^{\frac{q+1}{2}} - (x+1)^{\frac{q+1}{2}}\right)^{\frac{3^k+1}{2}}\left((x-1)^{\frac{3^k+1}{2}} - (x+1)^{\frac{3^k+1}{2}}\right)^{\frac{q-3}{2}}$$

$$p_9(x) = x^{\frac{2q-3^k-3}{2}} p_8(p_7(x))p_7(x) \qquad p_{10}(x) = p_1(p_9(x))$$

For $c \in F$, consider the fiber $(\Delta f)^{-1}(\{c\})$ of the derivative of f.

(i) If $(1 - c^{3^k+1})^{(q-1)/2} = -1$, then $(\Delta f)^{-1}(\{c\}) = \emptyset$.

(ii) Otherwise, $(\Delta f)^{-1}(\{c\}) = \{p_4(c), p_{10}(c)\}$. If $c \in \mathbb{F}_3$, then $p_4(c) = p_{10}(c) = 1 - c$, but if $c \notin \mathbb{F}_3$, then $p_4(c)$ and $p_{10}(c)$ are distinct elements of $F \setminus \mathbb{F}_3$.

The $p_4(c)$ element originates from the F^* part of our double cover and the $p_{10}(c)$ element from the U_E part.

Theorem (K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Let $F = \mathbb{F}_{3^n}$ and let $f\colon F \to F$ with $f(x) = x^{(3^n+1)/(3^k+1)}$, where $n > 1$ is odd, k is nonnegative and even, and $\gcd(n,k) = 1$. Let $\epsilon \in \mathbb{Z}_+$ with $\epsilon(3^k-1)/4 \equiv 1 \pmod{(q-1)/2}$. Let

$$p_0(x) = (1 - x^{3^k+1})^{\frac{q+1}{4}} \qquad p_1(x) = (((x+1)^{q-2}+1)^{\frac{3^k+1}{2}} - 1)^{q-2}$$

$$p_2(x) = x^{q-2+\frac{(q-3)\epsilon}{4}}(p_0(x)+1)^{\frac{(3q-1)\epsilon}{4}} \qquad p_3(x) = p_2(x) + p_2(x)^{q-2}$$

$$p_4(x) = p_1(p_3(x)) \qquad p_5(x) = \prod_{j=0}^{n-1}\left((-1)^j p_0(x)^{3^{jk}} + 1\right)$$

$$p_6(x) = \left(p_5(x) - p_5(x)^{q-2}\right)\left(p_5(x) + p_5(x)^{q-2}\right)^{q-2} \qquad p_7(x) = \left(1 - p_6(x)^2\right)^{\frac{q+1}{4}}$$

$$p_8(x) = \left((x-1)^{\frac{q+1}{2}} - (x+1)^{\frac{q+1}{2}}\right)^{\frac{3^k+1}{2}}\left((x-1)^{\frac{3^k+1}{2}} - (x+1)^{\frac{3^k+1}{2}}\right)^{\frac{q-3}{2}}$$

$$p_9(x) = x^{\frac{2q-3^k-3}{2}} p_8(p_7(x)) p_7(x) \qquad p_{10}(x) = p_1(p_9(x))$$

For $c \in F$, consider the fiber $(\Delta f)^{-1}(\{c\})$ of the derivative of f.

(i) If $(1 - c^{3^k+1})^{(q-1)/2} = -1$, then $(\Delta f)^{-1}(\{c\}) = \emptyset$.

(ii) Otherwise, $(\Delta f)^{-1}(\{c\}) = \{p_4(c), p_{10}(c)\}$. If $c \in \mathbb{F}_3$, then $p_4(c) = p_{10}(c) = 1 - c$, but if $c \notin \mathbb{F}_3$, then $p_4(c)$ and $p_{10}(c)$ are distinct elements of $F \smallsetminus \mathbb{F}_3$.

The $p_4(c)$ element originates from the F^* part of our double cover and the $p_{10}(c)$ element from the U_E part.

About p_5

Consider $p_5(x) = \prod_{j=0}^{n-1} \left((-1)^j p_0(x)^{3^{jk}} + 1 \right)$ in our algorithm.

About p_5

Consider $p_5(x) = \prod_{j=0}^{n-1} \left((-1)^j p_0(x)^{3^{jk}} + 1\right)$ in our algorithm.

When investigating the fibers of $f_4 \circ \lambda$, if $(f_4 \circ \lambda)(y, U_E) = b$ for some $b \in F$, then (with some easily handled exceptions)

$$y^{3^k} = \frac{sy + 1}{y - s}$$

where s is a square root of $b^2 - 1$, and the right-hand side has a Möbius transformation with matrix $\begin{pmatrix} s & 1 \\ 1 & -s \end{pmatrix}$.

About p_5

Consider $p_5(x) = \prod_{j=0}^{n-1} \left((-1)^j p_0(x)^{3^{jk}} + 1\right)$ in our algorithm.

When investigating the fibers of $f_4 \circ \lambda$, if $(f_4 \circ \lambda)(y, U_E) = b$ for some $b \in F$, then (with some easily handled exceptions)

$$y^{3^k} = \frac{sy+1}{y-s}$$

where s is a square root of $b^2 - 1$, and the right-hand side has a Möbius transformation with matrix $\begin{pmatrix} s & 1 \\ 1 & -s \end{pmatrix}$.

One then iterates this n times to get $y^{3^{nk}} = y$ (recall that $y \in U_E \subseteq E = \mathbb{F}_{3^{2n}}$ and k is even) on the left-hand side and a composition of n Möbius transformations with matrices $\begin{pmatrix} s^{3^{(n-1)k}} & 1 \\ 1 & -s^{3^{(n-1)k}} \end{pmatrix}, \ldots, \begin{pmatrix} s & 1 \\ 1 & -s \end{pmatrix}$ on the right-hand side.

About p_5

Consider $p_5(x) = \prod_{j=0}^{n-1} \left((-1)^j p_0(x)^{3^{jk}} + 1\right)$ in our algorithm.

When investigating the fibers of $f_4 \circ \lambda$, if $(f_4 \circ \lambda)(y, U_E) = b$ for some $b \in F$, then (with some easily handled exceptions)

$$y^{3^k} = \frac{sy + 1}{y - s}$$

where s is a square root of $b^2 - 1$, and the right-hand side has a Möbius transformation with matrix $\begin{pmatrix} s & 1 \\ 1 & -s \end{pmatrix}$.

One then iterates this n times to get $y^{3^{nk}} = y$ (recall that $y \in U_E \subseteq E = \mathbb{F}_{3^{2n}}$ and k is even) on the left-hand side and a composition of n Möbius transformations with matrices $\begin{pmatrix} s^{3^{(n-1)k}} & 1 \\ 1 & -s^{3^{(n-1)k}} \end{pmatrix}, \ldots, \begin{pmatrix} s & 1 \\ 1 & -s \end{pmatrix}$ on the right-hand side.

Further algebra with these matrices gives a solution for y that involves the product $\prod_{j=0}^{n-1} \left((-1)^j s^{3^{jk}} + 1\right)$.

Reflection on analysis of differential properties

Arrange differential analyses of a power function $f(x) = x^d$ over F into increasing levels of specificity. For various levels, we indicate where the result was achieved for the family of exponents of our main result.

Reflection on analysis of differential properties

Arrange differential analyses of a power function $f(x) = x^d$ over F into increasing levels of specificity. For various levels, we indicate where the result was achieved for the family of exponents of our main result.

(1) A bound on the differential uniformity: finding a B such that $|(\Delta f)^{-1}(\{c\})| \leq B$ for all $c \in F$

Reflection on analysis of differential properties

Arrange differential analyses of a power function $f(x) = x^d$ over F into increasing levels of specificity. For various levels, we indicate where the result was achieved for the family of exponents of our main result.

(1) A bound on the differential uniformity: finding a B such that $|(\Delta f)^{-1}(\{c\})| \leq B$ for all $c \in F$

(2) Differential uniformity: $\max_{c \in F} |(\Delta f)^{-1}(\{c\})|$

Reflection on analysis of differential properties

Arrange differential analyses of a power function $f(x) = x^d$ over F into increasing levels of specificity. For various levels, we indicate where the result was achieved for the family of exponents of our main result.

(1) A bound on the differential uniformity: finding a B such that $|(\Delta f)^{-1}(\{c\})| \leq B$ for all $c \in F$

(2) Differential uniformity: $\max_{c \in F} |(\Delta f)^{-1}(\{c\})|$

(3) Set of differential multiplicities: $\{|(\Delta f)^{-1}(\{c\})| : c \in F\}$
(Zha–Wang, 2010)

Reflection on analysis of differential properties

Arrange differential analyses of a power function $f(x) = x^d$ over F into increasing levels of specificity. For various levels, we indicate where the result was achieved for the family of exponents of our main result.

(1) A bound on the differential uniformity: finding a B such that $|(\Delta f)^{-1}(\{c\})| \leq B$ for all $c \in F$

(2) Differential uniformity: $\max_{c \in F} |(\Delta f)^{-1}(\{c\})|$

(3) Set of differential multiplicities: $\{|(\Delta f)^{-1}(\{c\})| : c \in F\}$ (Zha–Wang, 2010)

(4) Differential spectrum: $[\![|(\Delta f)^{-1}(\{c\})| : c \in F]\!]$ (Tian–Chen, 2017)

Reflection on analysis of differential properties

Arrange differential analyses of a power function $f(x) = x^d$ over F into increasing levels of specificity. For various levels, we indicate where the result was achieved for the family of exponents of our main result.

(1) A bound on the differential uniformity: finding a B such that $|(\Delta f)^{-1}(\{c\})| \leq B$ for all $c \in F$

(2) Differential uniformity: $\max_{c \in F} |(\Delta f)^{-1}(\{c\})|$

(3) Set of differential multiplicities: $\{|(\Delta f)^{-1}(\{c\})| : c \in F\}$
(Zha–Wang, 2010)

(4) Differential spectrum: $[\![|(\Delta f)^{-1}(\{c\})| : c \in F]\!]$
(Tian–Chen, 2017)

(5) Individual fiber sizes: an algorithm for finding $|(\Delta f)^{-1}(\{c\})|$ for arbitrary c
(K.–O'Connor–Pacheco–Sapozhnikov, 2024)

Reflection on analysis of differential properties

Arrange differential analyses of a power function $f(x) = x^d$ over F into increasing levels of specificity. For various levels, we indicate where the result was achieved for the family of exponents of our main result.

(1) A bound on the differential uniformity: finding a B such that $|(\Delta f)^{-1}(\{c\})| \leq B$ for all $c \in F$

(2) Differential uniformity: $\max_{c \in F} |(\Delta f)^{-1}(\{c\})|$

(3) Set of differential multiplicities: $\{|(\Delta f)^{-1}(\{c\})| : c \in F\}$
(Zha–Wang, 2010)

(4) Differential spectrum: $[\![|(\Delta f)^{-1}(\{c\})| : c \in F]\!]$
(Tian–Chen, 2017)

(5) Individual fiber sizes: an algorithm for finding $|(\Delta f)^{-1}(\{c\})|$ for arbitrary c
(K.–O'Connor–Pacheco–Sapozhnikov, 2024)

(6) Individual fibers: an algorithm for finding $(\Delta f)^{-1}(\{c\})$ for arbitrary c
(K.–O'Connor–Pacheco–Sapozhnikov, 2024)